

BAB 1 PENDAHULUAN

1.1 Latar Belakang

Internet of Things (IoT), merupakan konsep dimana “semua” benda yang mampu memuat alokasi penyimpanan dan kemampuan komputasi antar perangkat yang saling terhubung dalam sebuah jaringan serta saling berkolaborasi dalam bentuk apapun, kapanpun dan dimanapun. Perkembangan IoT yang semakin meningkat saat ini membuat dapat diterapkan pada berbagai macam area seperti lingkungan industri, lingkungan rumah tangga, lingkungan kesehatan dan lain-lain dengan menghubungkan sensor untuk memonitor parameter tertentu dari berbagai aktivitas secara *real-time* untuk menyediakan informasi bagi pengguna (Aziz, B., 2015).

Pada umumnya perangkat yang digunakan pada IoT memiliki keterbatasan dalam bentuk spesifikasi contohnya penyimpanan memori yang kecil dan daya yang rendah. Agar perangkat-perangkat yang terbatas ini dapat berkomunikasi satu sama lain dengan baik, sebuah protokol standar komunikasi dan perangkat untuk menghubungkan objek-objek tersebut sangat diperlukan (Niruntasukrat, dkk., 2016). Protokol MQTT merupakan protokol komunikasi *Internet of Things* (IoT) berbasis mekanisme *topic-based publish/subscribe* yang bersifat ringan, desain sederhana, terbuka dan mudah diimplementasi. Karakteristik tersebut membuat MQTT cocok diimplementasikan pada lingkungan yang terbatas seperti lingkungan IoT dimana jaringan mahal, memiliki *bandwidth* rendah dan jaringan tak stabil, untuk berjalan di perangkat yang memiliki *prosesor*, memori dan daya terbatas (Sengupta, S., & Ghosh, D., 2013). Selain protokol komunikasi, dibutuhkan pula sebuah perangkat yang menjembatani kemampuan objek tersebut untuk melakukan kegiatan tersebut dan pengguna yang ingin mengaksesnya. Disamping kemampuan untuk saling berbicara, perangkat tersebut membutuhkan ukuran yang kecil untuk dapat diletakkan pada sebuah objek tanpa mengganggu fungsi dasar dari objek tersebut. Perangkat nodeMCU merupakan mikrokontroler yang memiliki integrasi modul esp8266 untuk berkomunikasi dengan internet. NodeMCU juga dijuluki sebagai perangkat masa depan IoT (Jaffe, S., 2016).

Salah satu permasalahan yang terdapat dalam setiap sistem, termasuk IoT, adalah keamanan. Kebanyakan perangkat IoT mengumpulkan data yang bersifat personal seperti aktivitas sehari-hari, *home-automation*, informasi kesehatan dsb. Karena itu akses terhadap data tersebut atau kemampuan untuk memanipulasi data tersebut dapat menyalahi konsep privasi (Aziz, B., 2015). Menurut Andress, J. (2011), untuk meningkatkan keamanan dalam sistem dapat dicapai melalui beberapa langkah yang dimulai dari identifikasi yang merupakan proses klaim identitas dimana kita menuntut identitas pihak tertentu (bisa berupa seseorang atau sesuatu), autentikasi yang merupakan sarana atau metode validasi terhadap klaim identitas pihak tersebut apakah benar atau tidak, dan otorisasi yang memungkinkan kita untuk menentukan kegiatan pihak tersebut di dalam sistem apakah dibolehkan atau dilarang.

Mekanisme autentikasi pada MQTT dapat dilakukan melalui penggunaan *username* dan *password* yang masih sederhana, dan dibutuhkan sebuah mekanisme otorisasi pada MQTT yang dapat digunakan untuk mengatur akses kontrol dan manajemen identitas klien (Niruntasukrat, dkk., 2016). Sedangkan mekanisme otorisasi pada MQTT dapat dilakukan dengan menggunakan *Access Control List (ACL)* yang diterapkan pada sisi broker MQTT, metode yang dilakukan adalah untuk mengatur pengguna sistem tertentu untuk mengakses topik tertentu pada aktivitas tertentu (*publish/subscribe*). Penggunaan metode ini sangat penting karena melindungi keamanan data yang diakses terhadap pengguna yang tidak bertanggung jawab, melalui penerapan ACL pada IoT ini aktivitas pengguna terkait hak akses terhadap sumberdaya dapat terkontrol dengan baik dalam MQTT (Upadhyay, dkk., 2016). ACL memiliki tujuan untuk memastikan pengguna yang memiliki hak akses mendapatkan data sesuai keinginan dan pengguna yang tak memiliki hak akses untuk tidak mengakses data tersebut.

Berdasarkan pada uraian permasalahan diatas, maka dibuatlah sebuah penelitian untuk mengimplementasikan mekanisme otorisasi pada protokol MQTT menggunakan sebuah model ACL yang akan diterapkan pada broker MQTT, untuk mengatur dan melakukan manajemen hak akses klien MQTT. NodeMCU akan digunakan sebagai mikrokontroler yang akan mengatur aktivitas sensor dan aktuator dalam sistem dan berperan sebagai node klien yang melakukan *publish/subscribe*. Model ACL akan diatur menggunakan pengaturan berdasarkan peran klien dan daftar perizinan hak akses akan didasarkan pada topik yang dapat diakses dan jenis akses topik tersebut. Pengaturan ini bertujuan untuk memastikan bahwa hanya pengguna yang telah terotorisasi yang dapat mengakses data dan memastikan data tersebut berasal dari sumber yang benar, serta pengguna yang tidak terotorisasi tidak dapat mengakses data tersebut.

1.2 Rumusan Masalah

Berdasarkan pada latar belakang yang telah dijelaskan diatas, maka beberapa permasalahan yang ingin penulis bahas dalam penelitian ini adalah sebagai berikut:

1. Bagaimana menerapkan mekanisme otorisasi pada protokol MQTT dengan menggunakan *access control list*?
2. Bagaimana merancang model *access control list* sebagai mekanisme otorisasi untuk mengatur hak akses pengguna pada protokol MQTT?
3. Bagaimana pengaruh penerapan mekanisme otorisasi dengan *access control list* terhadap keamanan dan performa sistem IoT berbasis protokol MQTT yang menggunakan perangkat nodeMCU?

1.3 Tujuan

Berdasarkan pada rumusan masalah yang telah diuraikan diatas, maka tujuan yang ingin didapatkan dalam penelitian ini adalah sebagai berikut:

1. Dapat menerapkan *access control list* sebagai mekanisme otorisasi pada protokol MQTT sebagai cara untuk mengatur hak akses pengguna dalam lingkungan IoT yang menggunakan perangkat nodeMCU.
2. Dapat merancang sebuah model *access control list* yang digunakan sebagai mekanisme otorisasi untuk mengatur dan melakukan manajemen hak akses pengguna pada protokol MQTT.
3. Dapat meningkatkan keamanan pada sisi privasi pengguna terhadap hak akses data yang dapat diakses dalam sistem IoT berbasis protokol MQTT yang menggunakan perangkat nodeMCU tanpa mengurangi performa dari broker untuk menangani klien.

1.4 Manfaat

Manfaat yang diharapkan bisa didapatkan melalui penelitian ini adalah sebagai berikut:

1. Penelitian ini diharapkan dapat menjadi acuan untuk membangun sebuah sistem IoT yang menggunakan protokol komunikasi MQTT serta membuat sistem tersebut lebih aman, khususnya mengenai bagaimana menerapkan *Access Control List* (ACL) sebagai mekanisme otorisasi untuk membatasi dan mengatur hak akses pengguna dan penggunaan nodeMCU sebagai perangkat yang digunakan dalam sistem tersebut.
2. Penelitian ini diharapkan dapat menjadi referensi untuk melakukan penelitian lebih lanjut mengenai permasalahan yang memiliki keterkaitan dengan penelitian ini, untuk membuat analisa perbandingan atau pengembangan pada penelitian selanjutnya.

1.5 Batasan Masalah

Agar penelitian ini terfokus pada permasalahan yang telah dikemukakan dan tidak keluar dari latar belakang yang telah dijabarkan, maka pada penelitian ini ditentukan beberapa batasan meliputi:

1. Protokol komunikasi yang digunakan menggunakan MQTT.
2. NodeMCU digunakan sebagai sensor dan aktuator klien pada MQTT.
3. Payload data yang dikirimkan tanpa menggunakan enkripsi.
4. Keamanan difokuskan pada layer aplikasi, sedangkan layer transport digunakan secara sederhana.
5. Mekanisme autentikasi akan dilakukan secara sederhana, tanpa *sessions/cookies* dan tanpa *expiration*.
6. Mekanisme otorisasi menggunakan ACL berbasiskan pada peran.
7. Perizinan ACL akan dirancang berdasarkan pada topik dan jenis topik tersebut (*publish/subscribe*).

1.6 Sistematika Pembahasan

Sistematika pembahasan merupakan uraian struktur penulisan untuk memberikan pemahaman singkat terkait sistematika dari penyusunan skripsi secara garis besar yang meliputi beberapa bab, yaitu :

BAB I : Pendahuluan

Menguraikan permasalahan yang akan dijadikan sebagai subjek dalam penelitian ini serta sedikit pembahasan mengenai penelitian yang akan dilakukan. Bab ini terdiri dari latar belakang, rumusan masalah, tujuan penelitian, manfaat penelitian, batasan masalah dan sistematika pembahasan.

BAB II : Landasan Kepustakaan

Menguraikan tentang penelitian yang telah dilakukan sebelumnya serta dasar teori penggunaan teknologi yang diteliti dalam skripsi ini dengan menggunakan referensi yang terkait mengenai *access control list* (ACL), MQTT, nodeMCU dan aspek lain yang mendukung dalam penelitian yang akan dilakukan.

BAB III : Metodologi

Menjelaskan mengenai jenis penelitian yang dilakukan, metode dan langkah-langkah yang akan dilakukan dalam melakukan penelitian skripsi ini sesuai dengan jenis penelitian ini yaitu dimulai dari studi literatur, rekayasa kebutuhan, perancangan, implementasi, pengujian dan analisis serta pengambilan kesimpulan dan saran.

BAB IV : Rekayasa Kebutuhan dan Perancangan

Rekayasa kebutuhan menjelaskan mengenai kebutuhan sistem yang akan dibuat, seperti kebutuhan perangkat keras, kebutuhan perangkat lunak, kebutuhan fungsional, kebutuhan non-fungsional dan batasan dari implementasi yang akan dilakukan. Sementara Perancangan menguraikan proses perancangan sistem yang akan dibuat berdasarkan pada rekayasa kebutuhan.

BAB V : Implementasi

Menguraikan proses implementasi sistem yang dibuat dari hasil perancangan sistem berdasarkan kebutuhan yang dibutuhkan yaitu dengan menerapkan *access control list* (ACL) pada perangkat nodeMCU yang menggunakan protokol MQTT.

BAB VI : Pengujian dan Analisis

Menjelaskan mengenai hasil dari implementasi yang telah selesai dilakukan yang kemudian dilakukan pengujian untuk mengetahui kinerja sistem dalam menerapkan solusi dari permasalahan yang ada.

BAB VII : Penutup

Menjelaskan tentang kesimpulan yang telah diperoleh dari hasil pengujian dan analisis sistem serta saran untuk penelitian dan pengembangan lebih lanjut.