

BAB 1

USULAN GAGASAN

1.1 Latar Belakang Masalah

Seiring berjalannya waktu, Internet of Things (IoT) telah digunakan secara luas dan mengalami perkembangan pesat. Hal ini memungkinkan akses informasi yang lebih luas dari berbagai sumber[1]. IoT merupakan konsep di mana benda atau objek tertentu ditanamkan dengan teknologi seperti sensor dan perangkat lunak untuk berkomunikasi, mengendalikan, menghubungkan, dan bertukar data melalui perangkat lain selama terhubung ke internet[1]. Konsep ini erat kaitannya dengan istilah machine-to-machine (M2M), di mana semua alat dengan kemampuan komunikasi M2M disebut perangkat cerdas atau smart devices[1].

Dalam lingkungan IoT terjadi pertukaran, transfer, dan penyimpanan data. Namun, ada potensi akses dan validasi data oleh pihak yang tidak bertanggung jawab, yang dapat mengakibatkan kerugian[1]. Oleh karena itu, kami merancang sistem autentikasi berbasis QR Code dengan menggunakan protokol Message Queueing Telemetry Transport (MQTT) pada perangkat IoT. Sistem ini bertujuan untuk mencegah tindakan pencurian data dan memvalidasi klaim terhadap informasi dokumen dan data yang dikirimkan[2][3][4][5][6][7].

Protokol MQTT adalah protokol konektivitas M2M yang dirancang untuk mengirimkan data kecil dalam bentuk byte array dengan menggunakan arsitektur SSL[4]. MQTT memiliki beberapa keunggulan dibandingkan dengan HTTP atau protokol lainnya, antara lain kemampuan untuk mengirimkan data dengan bandwidth yang efisien, pengiriman yang cepat karena ukuran data yang kecil, penggunaan energi yang rendah, serta konektivitas dan *latency* yang tinggi[4]. Data yang dikirimkan melalui protokol MQTT berupa QR Code, sehingga pengguna dapat memvalidasi data yang terkandung dalam QR Code tersebut[3][6]. QR Code merupakan kode matriks dua dimensi yang dapat menyimpan ribuan karakter alfanumerik[6]. QR Code terdiri dari titik-titik dan spasi yang membentuk kotak, dan setiap elemennya memiliki arti masing-masing[6]. Hal ini membuat QR Code mudah digunakan. Pengguna dapat menggunakan smartphone atau perangkat cerdas lainnya untuk memindai QR Code[6]. Dengan demikian, sistem autentikasi berbasis QR Code dengan protokol MQTT pada perangkat IoT dapat mencegah tindakan pencurian data, melindungi integritas informasi, dan memberikan metode validasi yang efisien[2][3][4][5][7]. Penggunaan QR

Code memungkinkan penyimpanan informasi yang luas dalam bentuk yang mudah diakses, sementara protokol MQTT memastikan pengiriman data yang efisien dan aman dalam lingkungan IoT[3][4].

1.2 Informasi Pendukung Masalah

Dari penelitian Naeem yang membuat model serangan brute force untuk memperoleh informasi client dan memberikannya kepada penyerang, sehingga penyerang dapat melakukan subscribe atau publish secara tidak sah[4]. Model ancaman yang dirancang dengan menggunakan serangan DDoS dan brute force langsung menuju kepada broker dan jika penyerang berhasil mendapatkan password maka penyerang bisa masuk dengan cara menyamar menjadi pengguna yang sah, dan penyerang dapat melakukan publish maupun subscribe sehingga mengakibatkan kebocoran informasi pengguna[20]. Oleh karena itu, dapat kita ambil bahwa protokol MQTT sangat rentan terhadap serangan brute force maupun serangan yang terkait autentikasi oleh karena itu dibutuhkan sistem keamanan yang lain pada protokol MQTT. Kemudian ada juga penelitian yang dilakukan oleh Azwar mereka menggunakan 2FA sebagai pengamanan protokol MQTT yaitu dengan menggunakan username dan password juga One Time Password (OTP)[5]. Pengamanan 2FA dengan menggunakan OTP ini berhasil membuat protokol MQTT terhindar dari serangan brute force. Karena OTP dikirim ke pengguna dengan batas waktu tertentu, jadi jika waktu OTP sudah habis maka OTP tidak bisa digunakan lagi. Akan tetapi, akan tetap ada celah terhadap serangan karena selama batas waktu OTP masih berlaku maka OTP tersebut masih bisa digunakan oleh penyerang sehingga penyerang dapat mencoba masuk kedalam sistem dan melakukan penyerangan selama waktu OTP masih ada. Oleh karena itu dibutuhkan sistem pengamanan yang lebih dapat diandalkan untuk mengamankan MQTT.

1.3 Analisis Umum

Analisis umum yang kami ambil ada dua yaitu berdasarkan aspek manufakturabilitas dan aspek keberlanjutan.

1.3.1 Aspek Manufakturabilitas

Aspek manufakturabilitas yang relevan dalam implementasi "MQTT- Based QR Code Authentication on IoT Devices" meliputi:

- 1) Desain dan produksi QR code

Dalam tahap manufaktur, penting untuk mempertimbangkan desain QR code yang optimal agar

dapat dicetak dengan jelas dan akurat pada perangkat IoT. Desain harus mempertimbangkan ukuran, kontras, dan kejelasan QR code agar dapat dengan mudah dipindai oleh perangkat pemindai.

2) Integrasi protokol MQTT

Perangkat IoT harus didesain dan diproduksi dengan dukungan untuk protokol MQTT. Ini memerlukan pemilihan komponen dan perangkat keras yang sesuai, termasuk mikrokontroler atau modul IoT yang mendukung koneksi MQTT. Keberhasilan implementasi MQTT pada perangkat IoT mempengaruhi manufakturabilitas dan kualitas keseluruhan perangkat.

3) Keamanan dan validasi QR code

Dalam konteks manufaktur, perlu mempertimbangkan keamanan dan validasi QR code yang terkait dengan autentikasi. Sistem manufaktur harus mengimplementasikan langkah-langkah yang tepat untuk menghasilkan QR code dengan keamanan yang baik dan mencegah duplikasi atau manipulasi oleh pihak yang tidak berwenang.

4) Uji coba dan evaluasi

Sebelum perangkat IoT diproduksi secara massal, tahap uji coba dan evaluasi harus dilakukan untuk memastikan kinerja dan keandalan sistem autentikasi QR code berbasis MQTT. Aspek manufakturabilitas melibatkan proses pengujian perangkat, verifikasi keamanan, serta pemantauan dan pengelolaan perangkat dalam skenario yang realistis.

5) Efisiensi produksi

Aspek manufakturabilitas juga mencakup efisiensi produksi perangkat IoT dengan sistem autentikasi QR code. Perlu dipertimbangkan faktor-faktor seperti biaya bahan, kecepatan produksi, ketersediaan komponen, dan proses perakitan yang dapat mempengaruhi kemampuan produksi massal dengan kualitas yang konsisten.

Dalam keseluruhan, aspek manufakturabilitas ini penting untuk memastikan implementasi yang berhasil dari sistem autentikasi QR code berbasis MQTT pada perangkat IoT. Dengan memperhatikan aspek-aspek ini, manufaktur dapat menghasilkan perangkat yang handal, aman, dan efisien dalam menjaga keamanan data dan autentikasi pada lingkungan IoT.

1.3.2 Aspek Keberlanjutan

Aspek keberlanjutan yang relevan dalam implementasi "MQTT- Based QR Code Authentication on IoT Devices" meliputi:

1) Penggunaan sumber daya yang efisien

Dalam merancang dan memproduksi perangkat IoT dengan sistem autentikasi QR code berbasis MQTT, perlu memperhatikan penggunaan sumber daya yang efisien. Hal ini mencakup penggunaan energi yang hemat, penggunaan bahan yang ramah lingkungan, dan pemilihan komponen yang memiliki masa pakai yang panjang.

2) Perpanjangan masa pakai perangkat

Salah satu aspek keberlanjutan adalah memperpanjang masa pakai perangkat IoT. Ini dapat dicapai

melalui perancangan yang baik, penggunaan komponen berkualitas tinggi, dan perawatan yang tepat. Dengan demikian, pengguna dapat memanfaatkan perangkat IoT untuk jangka waktu yang lebih lama sebelum perlu menggantinya, mengurangi limbah elektronik.

3) Pembaruan perangkat lunak dan keamanan

Dalam konteks IoT, penting untuk mempertimbangkan aspek keberlanjutan dalam pembaruan perangkat lunak dan keamanan. Melalui pembaruan perangkat lunak, perangkat IoT dapat memperoleh fitur baru, peningkatan kinerja, dan perbaikan keamanan yang relevan. Dengan demikian, perangkat IoT tetap relevan dan dapat melindungi pengguna dari ancaman keamanan yang baru.

4) Daur ulang dan pengolahan limbah

Dalam proses manufaktur dan pemilihan bahan, perlu mempertimbangkan cara yang tepat untuk daur ulang dan memproses limbah yang dihasilkan. Ini mencakup pemilihan bahan yang dapat didaur ulang, metode pengolahan limbah elektronik yang ramah lingkungan, serta kebijakan pengelolaan limbah yang berkelanjutan.

5) Kompatibilitas dan interoperabilitas

Aspek keberlanjutan juga mencakup kemampuan perangkat IoT untuk berintegrasi dan berinteroperabilitas dengan sistem lain. Dengan adopsi standar komunikasi dan protokol yang terbuka, perangkat IoT dapat bekerja dengan sistem yang lebih luas, mengurangi kebutuhan untuk penggantian perangkat ketika ada perubahan atau peningkatan di lingkungan IoT.

Dalam keseluruhan, memperhatikan aspek keberlanjutan dalam implementasi "MQTT-Based QR Code Authentication on IoT Devices" penting untuk menciptakan solusi yang lebih ramah lingkungan, hemat sumber daya, dan memiliki dampak jangka panjang. Dengan mengadopsi praktik-praktik keberlanjutan ini, dapat menciptakan lingkungan IoT yang lebih berkelanjutan, yang mendukung inovasi teknologi tanpa mengorbankan keberlanjutan lingkungan dan sosial[25].

1.4 Kebutuhan yang Harus Dipenuhi

Berikut beberapa kebutuhan komponen yang harus dipenuhi :

Tabel 1. 1 Alat dan Bahan

No	Alat dan Bahan	Jumlah	Fungsi
1	ESP32 DevKit Support Bluetooth dan Wifi	1	Modul pengembangan berbasis mikrokontroler yang menggabungkan <i>Wifi</i> dan <i>Bluetooth</i> . Fungsi utama DevKit ESP32 adalah bertindak sebagai platform pengembangan untuk membangun berbagai proyek IoT (Internet of Things). Modul ini dapat digunakan untuk menghubungkan dan mengontrol berbagai perangkat elektronik melalui WiFi atau Bluetooth

2	LCD 16x2 with i2c	1	Modul tampilan karakter dengan antarmuka I2C. Fungsi utama LCD 16x2 I2C adalah untuk menampilkan teks atau informasi kepada pengguna. Modul ini dapat digunakan untuk menampilkan data, pesan atau status sistem elektronik yang ingin ditampilkan
3	LED 5mm WARNA WARNI - Merah	4	Dioda pemancar cahaya kecil dengan diameter 3 milimeter. Fungsi utama LED 3MM adalah sebagai indikator visual yang dapat memberikan informasi tentang keadaan atau status sistem. LED 3mm banyak digunakan dalam proyek elektronik sebagai indikator daya, indikator status atau untuk membuat efek pencahayaan
4	Battery Lithium - Polymer 1s 3.7v 2000mAH	1	Baterai isi ulang dengan tegangan output 3,7 volt dan berkapasitas 2000 mAh. Fungsi utama baterai ini adalah menyediakan sumber daya portabel untuk perangkat elektronik. Baterai Li-po banyak digunakan di berbagai proyek elektronik seperti ponsel, tablet, drone, dan gadget
5	Module Battery Level Lithium 1S	1	Modul elektronik untuk mengukur atau memantau level daya atau kapasitas baterai. Tugas utama dari Battery Level Module adalah memberikan informasi status baterai yang tersisa dalam bentuk tegangan atau persentase. Modul ini berguna untuk sistem yang menggunakan baterai untuk memantau tingkat daya yang tersisa atau untuk membunyikan alarm saat baterai perlu diisi
6	Kabel Pelangi Pita 10 pin per meter	4	Media penghubung antar pin pada perangkat
7	Push Button Kecil	1	Komponen elektronik yang berfungsi sebagai saklar sesaat. Saat tombol ditekan, sirkuit dihidupkan, dan saat tombol dilepas, sirkuit kembali rusak. Fungsi utama push button adalah memungkinkan pengguna untuk mengontrol atau memicu fungsi tertentu dalam sistem elektronik, seperti menghidupkan atau mematikan perangkat
8	3D Printing Case	1	Sebagai proteksi fisik untuk komponen elektronik, memberikan kustomisasi sesuai desain dan ukuran perangkat, meningkatkan estetika, membantu penyusunan komponen, serta digunakan sebagai prototipe untuk pengujian dan pengembangan perangkat IoT

9	Relay 5v close Arduino	1	Relay berperan dalam menerapkan sistem otorisasi akses. Pengaktifan relay hanya akan terjadi apabila QR code yang dipindai telah dianggap sah dan diverifikasi oleh server MQTT. Hal ini bertujuan untuk memastikan bahwa hanya pihak yang memiliki otorisasi yang tepat yang dapat mengendalikan perangkat yang terhubung ke relay tersebut.
10	PCB Lubang ic Kecil	1	Untuk menjamin kualitas dan kehandalan total rangkaian, penting bagi kita untuk melakukan penempatan lubang PCB kecil secara tepat. Hal ini akan membantu memelihara tata letak yang teratur dan meningkatkan efisiensi keseluruhan dari desain rangkaian elektronik.
11	USB cable to DC	1	Dengan memanfaatkan USB <i>cable to DC</i> , proyek dapat menggunakan daya dari berbagai sumber USB yang banyak tersedia dan mengubahnya menjadi tegangan yang sesuai untuk mendukung operasi perangkat elektronik atau rangkaian yang terhubung.
12	Jack DC Female	1	Fungsi utama Jack DC Female sebagai tempat untuk menerima daya listrik dari sumber eksternal. Hal ini memberikan kemudahan dan fleksibilitas dalam menyediakan daya yang dibutuhkan oleh perangkat atau rangkaian elektronik yang terhubung.
13	Modul Charger Lithium j5019 + Step Up In 3-9V to 4-24V 2A DC to DC	1	Modul Charger Lithium J5019 + Step Up In 3-9V to 4-24V 2A DC to DC berfungsi untuk secara aman dan efisien mengisi daya baterai Lithium, sambil menyediakan tegangan yang sesuai untuk berbagai perangkat atau rangkaian yang memerlukan daya listrik dengan kebutuhan tegangan yang beragam.

1.5 Solusi-Solusi Sistem yang Ditawarkan

Adapun perancangan QR Code menggunakan protokol MQTT dan modul Esp8266 dengan kriptografi AES-256, berikut beberapa solusi yang ditawarkan :

1.5.1 Identifikasi Kebutuhan

Tahap awal yang perlu diidentifikasi terlebih dahulu adalah kebutuhan dan tujuan dari perancangan QR Code.

1.5.2 Protokol dan Modul

Pada perancangan QR Code ini menggunakan protokol MQTT, modul Esp8266 dengan kriptografi AES-256 yang bertujuan untuk menjalankan proses komunikasi pertukaran data dari awal hingga akhir.

1.5.3 Integrasi Sistem

Sesudah memilih protokol dan modul yang akan digunakan, tahap selanjutnya mengintegrasikan semua sistem dengan melakukan konfigurasi.

1.5.4 Kontrol dan Pemantauan

Setelah integrasi sistem selanjutnya dapat melakukan pengontrolan dan pemantauan dengan menyediakan software atau perangkat lunak.

1.5.5 Pengujian dan Validasi

Selanjutnya, apabila seluruh proses telah dilakukan tahap pengujian dan validasi dengan tujuan mengetahui sistem yang sudah dirancang berjalan sesuai yang direncanakan.

1.6 Karakteristik Produk

Pada penelitian ini membutuhkan produk pembanding yang dapat menjadi acuan dari produk yang kami rancang. Produk A merupakan sistem yang penulis rancang dan produk B merupakan sistem untuk perbandingan. Berikut perbandingan fitur-fitur dari kedua produk :

1.6.1 Karakteristik Produk A

Adapun perancangan QR-Code yang dibangun pada produk A menggunakan protokol MQTT dengan memiliki karakteristik sebagai berikut :

1) Fitur Utama

Sebagai tempat proses terjadinya pertukaran data dan penerimaan data dari publisher hingga ke subscriber dengan dimunculkan topik tertentu.

2) Fitur Dasar

Mendukung model publikasi di mana subscriber dapat bertukar data dan menerima data dengan dimunculkan topik tertentu.

3) Fitur Tambahan

Memiliki perlindungan data dengan AES-256

4) Solusi yang diharapkan

- Diinstal dan dioperasikan dengan mudah
- Aplikasi dapat beroperasi dengan lebih efisien

1.6.2 Karakteristik Produk B

Adapun perancangan QR-Code dibangun pada produk B memiliki karakteristik sebagai

berikut :

1) Fitur Utama

Sebagai tempat proses terjadi nya pertukaran data dan penerimaan data dari server hingga ke klien.

2) Fitur Dasar

Mendukung model server dimana *client* dapat bertukar data dan menerima data.

3) Fitur tambahan

Memiliki perlindungan data dengan SSL.

4) Solusi yang diharapkan

- Diinstal dan dioperasi dengan mudah
- Data yang dikirimkan benar dan tepat waktu.

1.7 Skenario Penggunaan

Skenario penggunaan dibutuhkan sebagai acuan perbandingan untuk memilih produk yang akan digunakan.

1.7.1 Karakteristik Produk A

MQTT merupakan protokol komunikasi yang melakukan pengiriman dan menerima data yang terjadi pada publisher hingga ke subscriber dengan topic yang sama. adapun berikut skenario dari produk A :

- 1) Mengaktifkan mobile app QR Code.
- 2) Arahkan kamera handphone ke QR Code yang ada di perangkat iot.
- 3) Masukkan username dan password.
- 4) Apabila benar akan ditampilkan alamat atau data yang dituju.
- 5) Produk ini menggunakan protokol MQTT yang membantu proses berjalannya pengiriman data dan penerima data.

1.7.2 Karakteristik Produk B

HTTP merupakan protokol komunikasi yang digunakan mengirim dan menerima informasi dari sebuah server, sehingga pengguna dapat mengaksesnya seperti halnya perancangan QR-Code ini.adapun berikut skenario dari produk B :

- 1) Mengaktifkan mobile app QR Code
- 2) Arahkan kamera handphone ke QR Code yang ada di perangkat iot

- 3) Masukkan username dan password
- 4) Apabila benar akan ditampilkan alamat atau data yang dituju
- 5) Produk ini menggunakan protokol HTTP yang membantu proses berjalannya pengiriman data dan penerima data.

1.8 Kesimpulan dan Ringkasan CD-1

Dalam era Internet of Things (IoT), pertukaran data semakin meluas, tetapi ini juga membawa potensi risiko ketika data dapat diakses oleh pihak yang tidak berwenang [1]. Oleh karena itu, penting untuk mengimplementasikan autentikasi melalui protokol Message Queuing Telemetry Transport (MQTT) dengan memanfaatkan teknologi *Quick Response* (QR) Code, agar keamanan data dapat dijaga dengan baik [1]. Ancaman-ancaman yang mungkin timbul melibatkan serangan Denial of Service (DoS) dan upaya brute force, yang berpotensi merusak sistem broker dan mengakibatkan potensi risiko keamanan yang serius [15]. Dalam mengatasi hal ini, solusi yang diusulkan adalah pemanfaatan QR Code dengan protokol MQTT, serta penggunaan modul Esp32 dengan kriptografi *Advanced Encryption Standard* (AES)-256, guna memastikan tingkat autentikasi yang kuat dan perlindungan data yang lebih baik. Dengan menggunakan QR Code dalam protokol MQTT, banyak keunggulan yang dapat diperoleh, termasuk kemudahan penggunaan, efisiensi dalam proses otorisasi, serta keandalan dalam pertukaran data.

Dalam implementasi produk A, penggunaan QR Code melalui protokol MQTT dipadukan dengan perlindungan data AES-256, yang bertujuan untuk memberikan pengalaman pengguna yang efisien dan aman. Di sisi lain, produk B mengandalkan protokol komunikasi HTTP dengan memanfaatkan QR Code untuk memberikan akses ke informasi, dengan autentikasi melalui username dan password.