BAB I
PENDAHULUAN

1.1. Latar Belakang

Perkembangan teknologi Internet of Things (IoT) telah memberikan dampak signifikan dalam berbagai sektor. IoT memungkinkan perangkat pintar untuk saling terhubung dan berkomunikasi, sehingga meningkatkan efisiensi operasional serta kualitas layanan di berbagai bidang, seperti otomasi rumah, sistem transportasi cerdas, dan pengawasan industri berbasis sensor. Salah satu perangkat yang sering digunakan dalam implementasi IoT adalah mikrokontroler ESP32. Perangkat ini memiliki keunggulan dalam efisiensi daya, konektivitas Wi-Fi dan Bluetooth, serta kemampuan menjalankan aplikasi dengan konsumsi daya rendah [1]. Oleh karena itu, ESP32 banyak digunakan dalam berbagai aplikasi, termasuk perangkat wearable, sistem pemantauan cerdas, dan perangkat sensor industri.

Peningkatan jumlah perangkat IoT yang terhubung memerlukan pemeliharaan dan pembaruan firmware secara berkala untuk menjaga kinerja dan keamanan sistem. Pembaruan firmware diperlukan untuk meningkatkan performa, memperbaiki kesalahan perangkat lunak, serta mengatasi celah keamanan yang dapat dimanfaatkan oleh pihak yang tidak bertanggung jawab. Pembaruan manual masih banyak digunakan dengan cara menghubungkan perangkat secara fisik menggunakan kabel atau perangkat keras tambahan. Metode ini memiliki keterbatasan dalam hal efisiensi waktu dan skalabilitas. Kendala ini semakin terasa pada perangkat yang tersebar di lokasi terpencil. Selain itu, pembaruan manual meningkatkan risiko kesalahan teknis, terutama dalam pengelolaan perangkat dalam jumlah besar [2]. Oleh karena itu, diperlukan metode yang lebih efisien dan fleksibel, seperti pembaruan Over-the-Air (OTA). Metode ini memungkinkan pembaruan firmware dilakukan secara jarak jauh tanpa memerlukan intervensi langsung dari pengguna.

Pembaruan OTA memiliki beberapa keunggulan, di antaranya adalah mengurangi waktu henti perangkat dan memungkinkan sistem tetap beroperasi selama proses pembaruan berlangsung [3]. Namun, agar proses ini berjalan dengan aman dan efisien, diperlukan protokol komunikasi yang sesuai. Salah satu protokol yang sering digunakan dalam sistem IoT adalah Message Queuing Telemetry Transport (MQTT). MQTT dirancang untuk komunikasi dalam jaringan dengan keterbatasan bandwidth

dan sumber daya. Protokol ini memiliki keunggulan dalam efisiensi penggunaan data, konsumsi daya rendah, serta keandalan dalam kondisi jaringan yang tidak stabil. Oleh karena itu, MQTT menjadi pilihan utama dalam implementasi sistem berbasis IoT. Selain itu, MQTT mendukung mekanisme Access Control List (ACL) yang berfungsi untuk mengelola hak akses terhadap topik komunikasi, sehingga meningkatkan keamanan dalam proses pengiriman data [4].

Dalam implementasi pembaruan firmware OTA, MQTT sering digunakan sebagai protokol untuk mengirim file pembaruan. Namun, protokol ini memiliki keterbatasan pada ukuran payload yang dapat dikirim dalam satu kali transmisi. Batasan ini menjadi kendala ketika ukuran firmware lebih besar dari kapasitas payload yang didukung oleh MQTT. Konsekuensinya, proses pengiriman dapat mengalami kegagalan atau data yang diterima tidak lengkap. Kendala ini berdampak pada keberhasilan pembaruan OTA serta menurunkan keandalan sistem secara keseluruhan [5].

Sebagai alternatif, Hypertext Transfer Protocol (HTTP) lebih sesuai untuk mentransfer file berukuran besar karena lebih stabil dan andal dalam mengelola proses transfer data. HTTP memungkinkan pengunduhan firmware secara lebih efektif, terutama untuk file dengan ukuran besar [6]. Namun, dalam implementasi umum, metode ini sering kali mengharuskan ESP32 berfungsi sebagai server yang menyediakan file firmware. Pendekatan ini memiliki sejumlah keterbatasan, terutama dari sisi performa dan fleksibilitas. Protokol HTTP tergolong cukup berat untuk dijalankan pada perangkat seperti ESP32 yang memiliki sumber daya terbatas. Jika menggunakan HTTPS, beban kerja perangkat akan semakin meningkat karena proses enkripsi dan dekripsi yang memerlukan komputasi tambahan. Selain itu, ketika ESP32 difungsikan sebagai web server, alamat IP-nya hanya dapat diakses dari jaringan lokal. Hal ini membatasi fleksibilitas sistem, terutama jika dibutuhkan akses dari luar jaringan. Oleh karena itu, meskipun HTTP mudah diimplementasikan, pendekatan ini kurang ideal untuk skenario yang membutuhkan efisiensi tinggi dan akses jarak jauh [7].

Untuk mengatasi tantangan yang dihadapi dalam pembaruan firmware OTA, penelitian ini mengusulkan integrasi MQTT dan HTTP sebagai solusi. MQTT digunakan sebagai mekanisme autentikasi, sedangkan HTTP digunakan untuk mengunduh file firmware dari cloud storage. Dalam pendekatan ini, ESP32 tidak lagi berfungsi sebagai server, melainkan sebagai klien yang mengunduh firmware dari

cloud storage. Hal ini memastikan bahwa hanya perangkat yang memiliki izin yang dapat mengakses dan mengunduh file pembaruan. Pendekatan ini menggabungkan keunggulan MQTT dalam komunikasi yang ringan dan aman dengan keandalan HTTP dalam transfer file berukuran besar.

Selain aspek keamanan dan keandalan, sistem yang dikembangkan dirancang untuk mempermudah proses penggunaan pembaruan firmware OTA. Banyak sistem pembaruan firmware yang ada saat ini masih memerlukan konfigurasi manual yang kompleks, seperti pengaturan server khusus atau pengelolaan sertifikat keamanan yang rumit. Pendekatan dalam penelitian ini menekankan pada pembuatan mekanisme yang sederhana dan langsung dapat digunakan, dengan meminimalkan kebutuhan konfigurasi manual yang berlebihan. Dengan demikian, sistem ini bertujuan menyediakan solusi pembaruan firmware yang efisien, aman, andal, serta mudah dioperasikan pada perangkat IoT berbasis ESP32.

1.2. Rumusan Masalah

Berdasarkan latar belakang, terdapat beberapa permasalahan utama dalam pembaruan firmware OTA untuk ESP32 dengan integrasi MQTT dan HTTP, yaitu:

1. Bagaimana merancang dan mengembangkan sistem pendukung proses pembaruan firmware Over-The-Air (OTA) pada perangkat IoT berbasis ESP32?
2. Bagaimana merancang dan mengembangkan sebuah library untuk ESP32 yang mampu mendukung proses pembaruan firmware secara Over-The-Air (OTA) dengan integrasi protokol MQTT dan HTTP?
3. Bagaimana menguji dan mengevaluasi efektivitas, efisiensi, dan keandalan proses pembaruan firmware OTA yang dikembangkan pada perangkat ESP32?

1.3. Tujuan Penelitian

Penelitian ini bertujuan untuk merancang dan mengembangkan sistem pembaruan firmware Over-The-Air (OTA) pada perangkat Internet of Things (IoT) berbasis mikrokontroler ESP32, dengan mengintegrasikan protokol Message Queuing Telemetry Transport (MQTT) sebagai mekanisme autentikasi serta protokol Hypertext Transfer Protocol (HTTP) sebagai media distribusi firmware. Perancangan sistem ini ditujukan untuk menghasilkan metode pembaruan firmware yang dapat beroperasi

secara optimal, mengatasi berbagai kendala teknis yang umum terjadi dalam proses pembaruan, serta meminimalkan intervensi konfigurasi secara manual dari pengguna.

1.4. Manfaat Penelitian

Penelitian ini memberikan kontribusi dalam pengembangan sistem pembaruan firmware Over-The-Air (OTA) pada perangkat IoT berbasis ESP32 dengan integrasi protokol MQTT dan HTTP, yang memungkinkan proses pembaruan dilakukan secara jarak jauh dan terstruktur. Sistem yang dikembangkan diharapkan mampu mengatasi kendala teknis, seperti keterbatasan ukuran payload, serta mengurangi ketergantungan terhadap intervensi manual dalam pemeliharaan perangkat. Selain itu, penelitian ini juga memberikan landasan untuk mengevaluasi kinerja sistem pembaruan dalam kondisi operasional nyata, sehingga hasilnya dapat digunakan sebagai acuan dalam penerapan mekanisme pembaruan firmware yang sesuai dengan kebutuhan perangkat IoT di berbagai lingkungan penggunaan.

1.5. Batasan Masalah

Dalam penelitian ini, beberapa batasan masalah yang perlu diperhatikan adalah:

1. Sistem yang dikembangkan diuji hanya pada perangkat ESP32 dengan tipe *ESP-WROOM-32*. Pengujian tidak mencakup perangkat IoT lain dengan spesifikasi perangkat keras atau sistem operasi yang berbeda.
2. Kode library didesain dengan sintaks yang sederhana agar mudah digunakan. Tidak ada evaluasi lebih lanjut terhadap pengalaman pengguna atau kemudahan sintaks tersebut dari sudut pandang developer.
3. Penelitian ini berfokus pada aspek keamanan dalam proses pembaruan firmware OTA, yang diwujudkan melalui mekanisme autentikasi perangkat, kontrol akses berbasis ACL, dan enkripsi data (TLS/SSL) dengan sertifikat digital. Ruang lingkup penelitian ini tidak mencakup analisis mendalam terhadap berbagai bentuk serangan siber maupun pengembangan sistem keamanan tambahan di luar protokol OTA yang diimplementasikan.