

BAB I

PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi digital di era revolusi industri 4.0 telah mendorong berbagai aspek kehidupan untuk bertransformasi menuju sistem yang lebih cerdas dan efisien. Salah satu penerapan teknologi tersebut adalah melalui Internet of Things (IoT) yang memungkinkan perangkat fisik terhubung dengan internet sehingga dapat dikendalikan dan dipantau secara otomatis (Khang et al., 2024). Penerapan IoT ini menjadi kunci dalam mewujudkan sistem cerdas di berbagai sektor.

Di lingkungan perguruan tinggi, khususnya pada fasilitas perpustakaan, kebutuhan akan sistem penyimpanan barang yang aman dan praktis menjadi hal penting. Selama ini, penggunaan *Locker* konvensional yang masih mengandalkan kunci fisik sering menimbulkan berbagai permasalahan, seperti hilangnya kunci, risiko duplikasi kunci, serta keterbatasan dalam pengelolaan *Locker* oleh pihak pengelola perpustakaan. Kondisi tersebut dapat mengurangi kenyamanan dan efisiensi pelayanan kepada mahasiswa (Akbar et al., 2023). Permasalahan ini menunjukkan perlunya peningkatan sistem keamanan dan manajemen aset yang ada.

Untuk mengatasi permasalahan tersebut, diperlukan sistem penyimpanan modern yang lebih aman, praktis, dan efisien. Salah satu solusinya adalah merancang *Smart Locker* berbasis IoT dengan memanfaatkan mikrokontroler *ESP32* sebagai pusat kendali sistem. *ESP32* dipilih karena memiliki keunggulan berupa dukungan Wi-Fi dan kemampuan komputasi yang cukup baik untuk aplikasi IoT, menjadikannya pilihan ideal untuk kontrol sistem *real-time* (Ramschie et al., 2021)

Sebagai metode autentikasi, sistem *Smart Locker* ini menggunakan *QR Code* (Quick Response Code) dan *RFID* (Radio Frequency Identification) sebagai kunci akses pengguna. *QR Code* dipilih karena bersifat unik, mudah dibuat, sulit dipalsukan, serta lebih efisien dibandingkan kunci fisik maupun PIN statis (Agus & Candra, 2023). Sementara itu, *RFID* digunakan sebagai alternatif autentikasi berbasis kartu, di mana pengguna cukup menempelkan kartu *RFID* pada pembaca untuk melakukan akses. Kombinasi kedua metode ini memungkinkan fleksibilitas dalam penggunaan, baik melalui smartphone maupun kartu identitas, serta meminimalkan risiko kehilangan kunci fisik dan duplikasi akses oleh pihak yang tidak berwenang.

Dengan penerapan autentikasi *QR Code* dan *RFID* yang terintegrasi dalam sistem IoT, pengguna dapat membuka dan menutup *Locker* secara otomatis, sedangkan status *Locker* dapat dipantau secara *real-time* melalui aplikasi mobile. Hal ini meningkatkan keamanan penyimpanan barang, memudahkan proses peminjaman maupun pengembalian *Locker*, serta mendukung efisiensi pengelolaan

fasilitas di perpustakaan. Dengan demikian, *Smart Locker* berbasis IoT ini diharapkan mampu memberikan solusi penyimpanan yang lebih aman, modern, dan sesuai dengan kebutuhan layanan mahasiswa di lingkungan kampus.

1.2 Rumusan Masalah

Penelitian ini berfokus pada perancangan dan implementasi sistem *Smart Locker* berbasis *Internet of Things* (IoT) dengan autentikasi ganda menggunakan *QR Code* dan *RFID* untuk menyediakan akses penyimpanan barang yang aman, serta memungkinkan pemantauan status loker secara *real-time*.

1.3 Batasan Masalah

1. Sistem *Smart Locker* yang dirancang hanya terdiri dari 3 unit *Locker* sebagai prototipe pengujian, dan belum ditujukan untuk implementasi skala besar.
2. Metode autentikasi yang digunakan terbatas pada *QR Code* dan *RFID* sebagai akses pengguna. Metode biometrik atau autentikasi berbasis wajah tidak dibahas dalam penelitian ini.
3. Mikrokontroler yang digunakan adalah *ESP32*, sehingga pembahasan tidak mencakup mikrokontroler atau platform IoT lain seperti Raspberry Pi atau ESP8266.
4. Pemantauan kondisi *Locker* dilakukan menggunakan Sensor *Ultrasonik*, yang hanya mendeteksi ada atau tidaknya barang, bukan jenis atau berat barang yang disimpan.

5. Komunikasi data menggunakan jaringan Wi-Fi, sehingga penelitian tidak membahas konektivitas melalui jaringan seluler (LTE, GSM) atau LoRa.
6. Aplikasi mobile hanya digunakan untuk proses registrasi, pemindaian *QR Code*, dan monitoring status *Locker*, tanpa melibatkan sistem pembayaran atau manajemen pengguna lanjutan.
7. Sistem keamanan fisik *Locker* (material, kekuatan mekanik, atau anti pencurian fisik) tidak dievaluasi secara mendalam, fokus penelitian hanya pada sistem kontrol dan autentikasi berbasis IoT.

1.4 Tujuan Dan Manfaat

1.4.1 Tujuan

Tujuan penelitian ini adalah merancang dan mengimplementasikan sistem *Smart Locker* berbasis *Internet of Things* (IoT) dengan autentikasi ganda menggunakan *QR Code* dan *RFID* guna menyediakan sistem penyimpanan barang yang aman, otomatis, serta mampu menampilkan status loker secara *real-time* melalui aplikasi monitoring.

1.4.2 Manfaat

1. Memberikan kemudahan bagi pengguna dalam mengakses *Locker* tanpa kunci fisik.
2. Meningkatkan keamanan penyimpanan barang melalui autentikasi yang terkontrol dan tercatat.

3. Mempermudah petugas perpustakaan dalam memantau dan mengelola *Locker* secara otomatis.
4. Mendukung penerapan konsep Smart Campus di lingkungan kampus.

1.5 Sistematika Penulisan

1. BAB I Pendahuluan

Membahas latar belakang penelitian, rumusan masalah, batasan masalah, tujuan dan manfaat penelitian, serta sistematika penulisan laporan.

2. BAB II Tinjauan Pustaka dan Landasan Teori

Berisi kajian teori yang relevan dengan penelitian, penelitian terdahulu sebagai dasar penyusunan sistem, serta konsep-konsep pendukung seperti IoT, autentikasi *QR Code*, *RFID*, Sensor *Ultrasonik*, dan mikrokontroler *ESP32*.

3. BAB III Metodologi Penelitian

Menjelaskan metode yang digunakan dalam perancangan sistem, mulai dari perancangan perangkat keras, perangkat lunak, arsitektur sistem, hingga alur kerja sistem *Smart Locker*.

4. BAB IV Perancangan dan Implementasi Sistem

Menguraikan proses pembuatan prototipe *Smart Locker*, implementasi autentikasi *QR Code* dan *RFID*, integrasi sensor serta *ESP32*, pengujian sistem, dan analisis hasil.

5. BAB V Kesimpulan dan Saran

Menyajikan kesimpulan yang diperoleh dari hasil penelitian serta memberikan saran untuk pengembangan sistem lebih lanjut.