

BAB 1. PENDAHULUAN

1.1 Latar Belakang

Keamanan ruang operasional merupakan salah satu aspek penting dalam menjaga keberlangsungan layanan (*business continuity*) perusahaan, khususnya pada infrastruktur kritikal seperti Ruang *Fiber Termination Management* (FTM) milik PT Telkom Akses di Malang. Ruang FTM berfungsi sebagai pusat manajemen jaringan serat optik yang menampung berbagai perangkat strategis pendukung konektivitas digital. Gangguan keamanan pada area ini, baik akibat akses ilegal, maupun kelalaian manusia, dapat menyebabkan terganggunya layanan jaringan secara luas serta menimbulkan kerugian operasional dan finansial yang signifikan (Zeluyvenca Avista dan Oldy Fahlovi, 2024).

Namun, sistem keamanan yang diterapkan pada Ruang FTM saat ini masih menggunakan kunci konvensional yang memiliki berbagai keterbatasan. Sistem tersebut belum mampu melakukan identifikasi maupun pencatatan identitas pengguna yang mengakses ruangan. Penggunaan kunci manual juga memiliki risiko tinggi terhadap kehilangan, penggandaan kunci, hingga penyalahgunaan akses oleh pihak yang tidak berwenang (Ardiansah dkk., 2024). Akibatnya, proses penelusuran pelaku menjadi sulit dilakukan ketika terjadi insiden keamanan karena tidak tersedia validasi identitas maupun riwayat akses yang jelas.

Kerentanan penggunaan kunci fisik terbukti secara empiris pada kasus pencurian perangkat telekomunikasi di Jawa Timur pada 6 Agustus 2024. Pelaku berhasil membobol sejumlah tower BTS menggunakan kunci master tanpa menimbulkan kerusakan fisik pada pintu. Dalam kasus tersebut, satu unit UBBP G2 dan satu unit UMPT G2 hasil curian dijual seharga Rp1.650.000 kepada penadah. Aksi pencurian ini menyebabkan kerugian yang diperkirakan mencapai puluhan juta rupiah akibat hilangnya perangkat telekomunikasi dan terganggunya operasional jaringan. Insiden tersebut menunjukkan bahwa sistem kunci manual tidak mampu memverifikasi identitas pengguna, sehingga Ruang FTM memiliki

risiko tinggi terhadap akses ilegal yang sulit terdeteksi tanpa adanya penerapan autentikasi biometrik (Putra dan Effendi, 2023).

Sebagai solusi, penerapan teknologi biometrik berbasis *Internet of Things* (IoT) dapat menjadi alternatif yang lebih aman dan efektif. Teknologi *fingerprint* memiliki karakteristik autentikasi unik pada setiap individu sehingga tidak dapat dipindahtangankan seperti kunci fisik konvensional (Zaenaldi dkk., 2024).

Kebaruan pada tugas akhir ini terletak pada integrasi sistem *fingerprint* dengan *website monitoring* sebagai pusat pengendalian akses pintu Ruang FTM secara *real-time*. Fitur ini memungkinkan admin mengelola verifikasi secara terpusat, serta menyediakan riwayat akses otomatis untuk menjamin keamanan fisik yang transparan dan akuntabel bagi kebutuhan audit.

1.2 Rumusan Masalah

Berdasarkan dari uraian masalah yang dijelaskan pada latar belakang di atas, maka penulis mendapatkan pokok permasalahan sebagai berikut :

- a. Bagaimana merancang sistem kontrol akses pintu ruang FTM berbasis *fingerprint* yang mampu meningkatkan keamanan akses ruangan ?
- b. Bagaimana membangun integrasi antara perangkat kontrol akses berbasis *fingerprint* dengan *website monitoring* sehingga aktivitas akses pintu dapat dipantau secara *real-time* dan tercatat dalam *database* ?
- c. Bagaimana merancang fitur pengelolaan hak akses pengguna melalui *website* agar proses penambahan, perubahan, dan penghapusan akses dapat dilakukan secara terpusat dan terdokumentasi dengan baik ?

1.3 Tujuan

Berdasarkan rumusan masalah yang telah di paparkan di atas, tujuan dari tugas akhir ini adalah :

- a. Merancang dan mengimplementasikan sistem kontrol akses pintu ruang FTM PT. Telkom Akses Malang berbasis *fingerprint*.

- b. Mengintegrasikan antara perangkat kontrol akses *fingerprint* dan *website monitoring*
- c. Menghasilkan fitur pengelolaan hak akses pengguna melalui *website* yang memungkinkan proses penambahan, perubahan, dan penghapusan hak akses dilakukan secara terpusat dan tercatat dengan baik.

1.4 Batasan Masalah

Berdasarkan tujuan yang telah dipaparkan di atas, maka batasan masalah dari tugas akhir ini sebagai berikut:

- a. Sistem menggunakan Mikrokontroler ESP32 dan sensor *fingerprint* untuk pembacaan sidik jari serta komunikasi IoT pada kontrol akses pintu.
- b. Integrasi sistem dilakukan antara perangkat kontrol akses *fingerprint* berbasis ESP32 dengan *website monitoring* berbasis PHP dan *database* MySQL.
- c. *Website monitoring* difokuskan pada pengelolaan hak akses pengguna, meliputi proses penambahan pengguna melalui mekanisme *pending* dan persetujuan admin, perubahan hak akses, penghapusan hak akses, serta pencatatan aktivitas pengguna ruangan.

1.5 Manfaat

Adapun manfaat yang diharapkan dari pembuatan laporan ini adalah sebagai berikut :

- a. Dapat membantu admin dalam memantau kondisi akses pintu Ruang FTM secara *real-time* melalui *website monitoring*,
- b. Dapat mempermudah administrator dalam mengelola data pengguna serta hak akses ruangan secara lebih efektif dan terpusat.
- c. Menyediakan riwayat aktivitas akses pengguna yang tersimpan secara otomatis pada *database* sebagai bentuk dokumentasi keamanan.