BAB I

PENDAHULUAN

1.1 Latar Belakang

Tingginya angka kriminalitas, khususnya pencurian dan pembobolan rumah, merupakan masalah serius yang dipicu oleh kelemahan mendasar pada sistem kunci konvensional[1], [2], [3], [4]. Hal ini tercermin dari data kriminalitas tahun 2023 yang menunjukkan bahwa Pencurian dengan Pemberatan (Curat) masih mendominasi tindak kejahatan terhadap properti, dengan jumlah kasus mencapai 62.961 kejadian atau sekitar 16,85% dari total tindak kriminal yang tercatat, sehingga menegaskan tingginya risiko keamanan pada hunian masyarakat[5]. Kunci tradisional dinilai kurang aman karena mudah hilang dan dapat diduplikasi, serta rentan terhadap perusakan pintu, yang memungkinkan tindakan pencurian[6], [7]. Kelemahan struktural ini menyebabkan minimnya kontrol akses dan pengawasan efektif, sebab sistem konvensional tidak dapat mencatat siapa saja yang masuk atau keluar properti. Tuntutan akan perlindungan aset usaha mendorong kebutuhan modernisasi sistem keamanan yang mampu menyediakan autentikasi terintegrasi, pemantauan jarak jauh, dan manajemen akses terpusat, khususnya bagi pelaku usaha kecil seperti pedagang kios yang tidak dapat sepenuhnya mengawasi tempat usahanya secara langsung [3], [8], [9]. Kebutuhan akan solusi yang secara mendasar mengatasi kerentanan ini belum sepenuhnya terpenuhi oleh produk komersial yang tersedia, terutama dalam

hal sistem pengawasan akses berbasis web yang terintegrasi dengan *aktivitas real-time*[10].

Adopsi *smart lock door* memang mengatasi kerentanan fisik kunci konvensional, namun solusi komersial yang beredar saat ini memiliki batasan signifikan dalam kapabilitas pengawasan akses yang komprehensif[11]. Meskipun telah terjadi pergeseran teknologi, sebagian besar sistem yang tersedia masih mengandalkan notifikasi *push* sederhana dan terjebak dalam ekosistem aplikasi *mobile* [12], [13], [14]. Ketergantungan pada aplikasi *mobile* ini seringkali gagal menyediakan *platform surveillance* yang terpusat, skalabel, dan *real-time* berbasis web[15][16]. Secara akademis, defisit kritis terletak pada minimnya dukungan untuk manajemen dan audit data historis melalui antarmuka *web-based* yang stabil[17][18]. Produk yang ada seringkali tidak menawarkan log aktivitas akses yang komprehensif dan mudah diaudit, yang merupakan data fundamental untuk pengawasan keamanan properti [19]. Celah inilah yang menciptakan kebutuhan mendesak untuk mengembangkan solusi yang mengalihkan fokus dari perangkat keras ke *platform web-based*, yang mampu menyajikan visibilitas penuh, kontrol akses, dan log aktivitas *real-time* dalam satu *dashboard* terpusat untuk tujuan forensik dan keamanan proaktif[20] [21]. Selain itu, sebagian besar *smart lock* komersial tidak mendukung manajemen pengguna berbasis peran[22], pembatasan akses berbasis geolokasi[23], maupun pengelolaan autentikasi biometrik melalui antarmuka web[24], sehingga tidak mampu memenuhi kebutuhan pengawasan properti yang menyeluruh dan terpusat.

Perkembangan teknologi *Internet of Things* (IoT) mendorong transformasi sistem keamanan dari perangkat fisik yang berdiri sendiri menjadi ekosistem terhubung yang mampu dikontrol dan dipantau melalui *platform* berbasis web secara *real-time*[25]. Integrasi ini memungkinkan setiap aktivitas akses pada perangkat keamanan pintu untuk secara otomatis tercatat, diteruskan ke *server* melalui protokol MQTT, dan disinkronisasi ke basis data berbasis *cloud* sehingga dapat ditampilkan pada antarmuka web secara langsung[26][27]. Data yang dikirim melalui *MQTT* selanjutnya disimpan dan disinkronisasi menggunakan Firebase Realtime Database, sehingga setiap perubahan status perangkat dapat langsung tercermin pada *dashboard web* tanpa memerlukan proses *polling* yang berulang [28].Kemampuan inilah yang menjadikan arsitektur berbasis IoT sebagai fondasi ideal bagi pengembangan sistem pengawasan akses berbasis web, karena data dari perangkat fisik dapat dikelola, divisualisasikan, dan diaudit secara terpusat melalui *dashboard* yang dapat diakses dari mana saja[29].

Kebutuhan akan sistem pengawasan akses berbasis web lebih jauh mencakup aspek manajemen risiko dan audit forensik digital yang tidak dapat dipenuhi oleh aplikasi *mobile* konvensional[30]. Tidak seperti aplikasi *mobile* yang hanya bersifat transaksional, *platform* web mampu memvisualisasikan data historis secara terpusat dan intuitif [31]. Kapabilitas ini mencakup fitur kritis seperti penyaringan log berdasarkan pengguna, waktu, dan status insiden, serta kemampuan ekspor data untuk keperluan analisis dan investigasi lebih lanjut[24]. Fleksibilitas pengembangan web juga

memungkinkan perancangan antarmuka yang lebih kaya dan adaptif, sehingga status keamanan properti dapat disajikan secara menyeluruh dalam satu tampilan terpadu[32]. Pengembangan *dashboard* berbasis web merupakan langkah strategis yang mengubah sistem keamanan pintu dari sekadar perangkat fisik menjadi sistem informasi manajemen keamanan yang komprehensif dan berorientasi pada pengambilan keputusan[33].

Meskipun log aktivitas *real-time* telah menyediakan rekaman data akses secara kronologis, volume data yang besar justru menyulitkan administrator dalam mengidentifikasi pola anomali secara manual[34]. Keterbatasan ini mendorong kebutuhan akan integrasi kecerdasan buatan dalam sistem pengawasan akses, yang mampu menganalisis pola data log secara otomatis dan kontekstual untuk mendeteksi aktivitas mencurigakan lebih awal[35]. Pemanfaatan *Large Language Model* (LLM) melalui antarmuka berbasis API, seperti yang disediakan oleh *platform* Groq, memungkinkan sistem untuk memberikan interpretasi cerdas terhadap data keamanan sehingga administrator dapat mengambil keputusan yang lebih tepat dan proaktif[36].

Sistem yang dikembangkan dalam penelitian ini dirancang dengan arsitektur berlapis yang mengintegrasikan antarmuka publik, manajemen perangkat berbasis IoT, dan kontrol akses berbasis peran pengguna. Pendekatan ini memungkinkan diferensiasi hak akses antara administrator dan pengguna akhir, di mana setiap peran memperoleh kapabilitas pemantauan dan pengendalian yang sesuai dengan tanggung jawabnya[37].

Untuk memperkuat keamanan operasional, sistem menerapkan pembatasan kontrol berbasis geolokasi[38] serta autentikasi biometrik sidik jari yang dilindungi oleh mekanisme verifikasi identitas berlapis [39][40]. Keseluruhan fitur ini disajikan dalam satu *platform* web terpadu yang mengubah sistem keamanan pintu dari sekadar perangkat fisik menjadi solusi manajemen akses yang komprehensif, teraudit, dan responsif secara *real-tim*e[41].

Berdasarkan analisis terhadap kelemahan sistem konvensional dan keterbatasan fitur pada *Smart Lock* komersial, terdapat kebutuhan mendesak untuk mengembangkan *platform* pengawasan akses berbasis web yang terpadu dan proaktif. Penelitian ini mengusulkan pengembangan sistem *smart lock door* berbasis IoT dengan fokus pada perancangan *dashboard* web yang menyediakan pemantauan *real*-time, manajemen akses berbasis peran, serta log aktivitas yang dapat diaudit. Sistem yang dikembangkan juga mengintegrasikan keamanan berlapis dan pembatasan akses berbasis lokasi untuk mendukung pengambilan keputusan pengguna secara kontekstual. Dengan demikian, kontribusi utama penelitian ini adalah menghadirkan solusi keamanan berbasis web yang memberikan visibilitas penuh, kontrol jarak jauh, dan respons otomatis dalam satu *platform* terpusat yang komprehensif.

1.2 Rumusan Masalah

Berdasarkan analisis latar belakang, penilitian ini bertujuan untuk menjawab dua masalah utama :

1. Bagaimana merancang arsitektur sistem smart door lock berbasis IoT yang terintegrasi dengan *platform web-based access surveillance* menggunakan protokol MQTT dan Firebase Realtime Database untuk mendukung pemantauan akses secara *real-time*?
2. Bagaimana membangun *dashboard* berbasis web dengan manajemen akses berbasis peran (*role-based*) yang mampu menampilkan log aktivitas historis, status perangkat, dan lokasi perangkat secara terpusat?
3. Bagaimana merancang sistem autentikasi biometrik sidik jari yang aman dengan mekanisme verifikasi berlapis melalui konfirmasi *email* untuk mencegah pendaftaran akses yang tidak sah?
4. Bagaimana menerapkan pembatasan kontrol akses pintu berbasis geolokasi sehingga fitur buka pintu hanya dapat diaktifkan oleh pengguna yang berada dalam radius tertentu dari perangkat?

1.3 Batasan Masalah

Agar penelitian ini memiliki fokus yang jelas dan dapat diukur, ruang lingkup perancangan sistem dibatasi sebagai berikut:

1. Komunikasi data antara perangkat ESP32 dan *server* menggunakan protokol MQTT melalui *broker mosquitto* yang dijalankan pada VPS, tanpa melakukan perbandingan dengan protokol IoT lainnya.
2. Sistem yang dikembangkan berupa *smart door lock* berbasis IoT menggunakan mikrokontroler ESP32 sebagai perangkat utama dengan penyimpanan data pada Firebase Realtime Database.

3. Sistem autentikasi dibatasi pada sidik jari dengan verifikasi *email*, tanpa mencakup metode autentikasi lain seperti face recognition atau OTP berbasis SMS.
4. Pembatasan kontrol akses berbasis geolokasi hanya diterapkan pada fitur buka pintu jarak jauh sebagai mekanisme keamanan kontekstual untuk mencegah aktivasi kontrol dari lokasi yang tidak sah.

1.4 Tujuan dan Manfaat

1.4.1. Tujuan

Penelitian ini bertujuan untuk merancang dan mengimplementasikan sistem *smart lock door* berbasis IoT dengan fokus pengembangan *platform* pengawasan akses berbasis web,secara spesifik sebagai berikut:

1. Merancang sistem *smart lock door* berbasis IoT yang terintegrasi dengan *dashboard* web untuk pemantauan akses secara *real-time*.
2. Membangun *dashboard* web dengan manajemen akses berbasis peran yang menampilkan log aktivitas, status perangkat, dan lokasi secara terpusat.
3. Menerapkan autentikasi biometric sidik jari dengan verifikasi *email* berlapis guna mencegah pendaftaran akses yang tidak sah.
4. Mengintegrasikan analisis kecerdasan buatan berbasis Groq untuk memberikan rekomendasi keamanan secara kontekstual kepada pengguna.

1.4.2. Manfaat

Hasil penelitian ini diharapkan memberikan manfaat bagi beberapa pihak:

1. Bagi Pengguna: Memudahkan pemantauan dan pengendalian akses pintu dari jarak jauh melalui antarmuka web yang dapat diakses kapan saja dan dapat meningkatkan keamanan properti melalui sistem autentikasi berlapis dan notifikasi otomatis secara *real-time*
2. Bagi Pelaku: Usaha Membantu pedagangkios mengawasi keamanan tempat usaha harus berada di lokasi secara langsung,jadi dapat mengurangi resiko kerugian akibat pencurian melaluipemantauan dan log aktivitas yang teraudit
3. Bagi Akademik: Memberikan kontribusi ilmiah berupa rancangan integrasi IoT dan platformweb sebagai referensi penelitian serupa