

Rancang Bangun Sistem Smart Door Lock Berbasis ESP32 Dengan Verifikasi Biometrik dan Cloud Logging

Mahendra [1*], Mochammad Ilham Aziz [2], Saifulloh Azhar[3]
Program Studi Informatika, Institut Teknologi Al Mahrusiyah, Kota Kediri, Indonesia
Email: mahendra284des@gmail.com[1], il.ilham95@gmail.com[2], azharnian@gmail.com[3]

Abstrak

Perkembangan *Internet of Things (IoT)* mendorong lahirnya sistem keamanan yang lebih cerdas dan terintegrasi, di CV. Indah Pratama, penggunaan kunci manual masih menimbulkan kendala berupa rendahnya efisiensi akses, risiko kehilangan atau penyalahgunaan kunci, serta tidak adanya pencatatan aktivitas keluar-masuk secara sistematis. Penelitian ini mengembangkan sistem *Smart Door Lock* berbasis ESP32 yang mengintegrasikan autentikasi sidik jari dengan pencatatan aktivitas secara *real-time* menggunakan Google Sheets. Metode yang digunakan adalah *Research and Development (R&D)* dengan model *Waterfall* yang meliputi analisis kebutuhan, perancangan, implementasi, pengujian, dan penerapan. Komunikasi data antara ESP32 dan Google Sheets dilakukan melalui Google Apps Script. Pengujian sistem menggunakan *Black Box Testing* dan pengujian *latency* untuk mengukur waktu pengiriman data ke *cloud*. Hasil penelitian menunjukkan sistem berfungsi sesuai rancangan, mampu melakukan autentikasi sidik jari, membuka kunci pintu secara otomatis, serta mencatat aktivitas akses secara *real-time*. Fitur *fail-safe buffering* memastikan data tetap tersimpan ketika koneksi internet terputus. Berdasarkan hasil pengujian, sistem mencapai tingkat keberhasilan 100% dengan rata-rata latency 1.980 ms sehingga mampu meningkatkan efisiensi akses sekaligus menyediakan pencatatan aktivitas yang transparan dan terstruktur.

Kata Kunci: *Biometrik, Cloud Logging;* ESP32*; Internet Of Things; Smart Door Lock*

ABSTRACT

The rapid advancement of the Internet of Things (IoT) has driven the development of smarter and more integrated security systems. At CV. Indah Pratama, the continued use of conventional mechanical keys presents several challenges, including inefficient access management, the risk of lost or unauthorized use of keys, and the absence of a systematic access logging mechanism. This study developed an ESP32 -based Smart Door Lock system that integrates fingerprint authentication with real-time activity logging using Google Sheets. The research employed the Research and Development (R&D) method with the Waterfall development model, consisting of requirements analysis, system design, implementation, testing, and deployment. Data communication between the ESP32 and Google Sheets was established through Google Apps Script. System evaluation was conducted using Black Box Testing and latency testing to measure data transmission time to the cloud. The results demonstrate that the proposed system operates as intended by providing reliable fingerprint authentication, automatically unlocking the door, and recording access activities in real time. In addition, the fail-safe buffering feature ensures that data are securely stored during internet connectivity interruptions. Based on the testing results, the system achieved a 100% success rate with an average latency of 1.980 ms, demonstrating its effectiveness in improving access efficiency while providing transparent and well-structured access activity records.

Keywords: *Biometrics; Cloud Logging; ESP32; Internet of Things; Smart Door Lock*

1. PENDAHULUAN

Perkembangan teknologi *Internet of Things (IoT)* telah mengubah sistem keamanan fisik dari yang sebelumnya bersifat pasif menjadi lebih cerdas, otomatis, dan terhubung. Dalam sistem kontrol akses, pemanfaatan *IoT* kini menjadi salah satu kebutuhan untuk meningkatkan keamanan sekaligus memudahkan pengelolaan akses. Meskipun demikian, masih banyak institusi yang menggunakan kunci manual sebagai sistem pengaman utama. Penggunaan kunci manual memiliki sejumlah kelemahan, seperti proses akses yang kurang efisien, risiko kehilangan atau penyalahgunaan kunci, serta tidak tersedianya pencatatan aktivitas keluar-masuk secara sistematis. Akibatnya, pemilik usaha tidak memiliki data yang dapat digunakan untuk melakukan pengawasan maupun evaluasi terhadap aktivitas akses.

Permasalahan tersebut juga dialami oleh CV. Indah Pratama, yang menjadi objek penelitian ini. Perusahaan ini memiliki karakteristik khusus karena area produksi berada dalam satu lingkungan dengan rumah tinggal pemilik. Kondisi tersebut menyebabkan pintu digunakan oleh dua kelompok pengguna dengan kebutuhan akses yang berbeda, yaitu karyawan yang memiliki jam kerja tetap dan anggota keluarga yang memerlukan akses secara fleksibel. Karena masih menggunakan kunci manual, seluruh aktivitas akses tidak terdokumentasi dengan baik sehingga menyulitkan proses pengawasan, meningkatkan risiko keamanan, dan mengurangi efisiensi operasional sehari-hari.

Berbagai penelitian mengenai *Smart Door Lock* telah dilakukan, namun masih memiliki beberapa keterbatasan. Penelitian terdahulu telah mengembangkan sistem berbasis *Arduino* yang bekerja secara *standalone* tanpa koneksi internet, sehingga tidak mampu melakukan pemantauan atau pengiriman data secara jarak jauh (Alfonsius et al., 2024; Maulana et al., 2023; Zain et al., 2024). Penelitian terdahulu juga telah memanfaatkan konsep *IoT*, tetapi autentikasinya masih menggunakan *Radio Frequency Identification (RFID)*(Amalia & Muhammad, 2024). Pendekatan ini bergantung pada kartu fisik yang berisiko hilang, tertinggal, atau digunakan oleh pihak yang tidak berwenang.

Sementara itu, penelitian lain dengan menggunakan *Telegram* sebagai media pelaporan aktivitas akses (Ardiansah et al., 2024; Suci Br Kembaren et al., 2023). Meskipun mampu memberikan notifikasi secara langsung, riwayat akses hanya tersimpan dalam bentuk percakapan sehingga kurang efektif sebagai media dokumentasi jangka panjang. Data yang tersimpan juga sulit direkap dan dianalisis untuk kebutuhan pelaporan maupun audit.

Berdasarkan kondisi tersebut, penelitian ini mengembangkan sistem *Smart Door Lock* berbasis ESP32 yang mengintegrasikan autentikasi sidik jari dan *cloud logging* menggunakan

Google Sheets. Sensor sidik jari AS608 dipilih karena sidik jari merupakan identitas biometrik yang unik, permanen, sulit dipalsukan, dan tidak dapat dipindahtangankan seperti kartu RFID (Ega Satrya & Servanda, 2024; Putra et al., 2023). ESP32 digunakan sebagai pusat kendali karena memiliki kemampuan pemrosesan yang baik serta modul Wi-Fi bawaan sehingga mampu mengirimkan data secara langsung ke layanan *cloud* tanpa perangkat tambahan.

Penggunaan database konvensional (seperti MySQL, PostgreSQL, atau Firebase) dalam skala usaha kecil menengah (UMKM) sering kali menimbulkan kendala finansial dan teknis, seperti perlunya biaya lisensi atau penyewaan *cloud server* berbayar, konfigurasi *backend API* yang kompleks, pemeliharaan berkala oleh *database administrator*, hingga pembuatan dashboard admin khusus atau kueri *SQL* untuk kebutuhan audit. Hal ini kurang efisien bagi pemilik UMKM yang umumnya tidak memiliki latar belakang IT. Sebagai solusinya, Google Sheets digunakan sebagai media penyimpanan data akses karena mudah diintegrasikan melalui Google Apps Script, dapat diakses secara *real-time* dari berbagai perangkat, tidak memerlukan biaya lisensi, serta menyajikan data dalam bentuk tabel yang terstruktur sehingga memudahkan proses pemantauan, pelaporan, dan evaluasi aktivitas akses (Pratama et al., 2023).

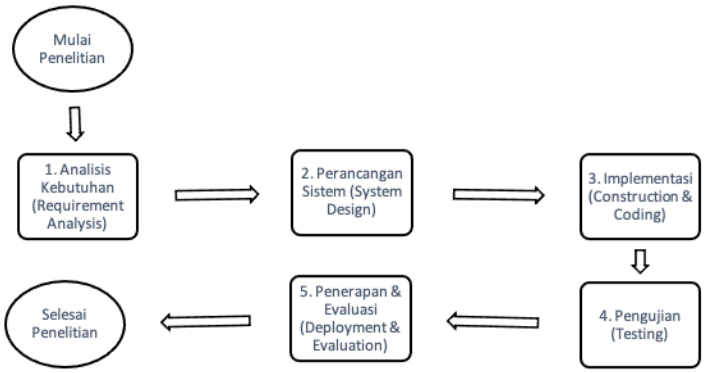
Kombinasi antara ESP32, autentikasi biometrik, dan penyimpanan data berbasis *cloud* menjadi kebaruan dalam penelitian ini. Sistem yang dikembangkan tidak hanya meningkatkan keamanan akses pintu, tetapi juga menyediakan pencatatan aktivitas yang transparan dan berkelanjutan sehingga mendukung pengawasan serta pertanggungjawaban data.

Berdasarkan latar belakang tersebut, penelitian ini bertujuan merancang dan membangun sistem *Smart Door Lock* berbasis ESP32 dengan autentikasi sidik jari, mengimplementasikan pencatatan aktivitas akses secara real-time ke Google Sheets, serta mengevaluasi kinerja sistem melalui *Black Box Testing* dan pengujian latency pada lingkungan operasional CV. Indah Pratama.

2. METODE

Penelitian ini menggunakan metode *Research and Development (R&D)* yang bertujuan untuk mengembangkan produk teknologi sekaligus menguji efektivitasnya pada lingkungan operasional nyata (Waruwu, 2024). Proses pengembangan sistem menerapkan model *Waterfall* karena memiliki tahapan yang terstruktur, berurutan, dan terdokumentasi dengan baik sehingga sesuai untuk pengembangan sistem yang mengintegrasikan perangkat keras dan perangkat lunak (Anis et al., 2023). Tahapan penelitian meliputi lima fase, yaitu: (1) Analisis Kebutuhan (*Requirement Analysis*), (2) Perancangan Sistem (*System Design*), (3) Implementasi (*Construction and Coding*), (4) Pengujian (*Testing*), dan (5) Penerapan (*Deployment*).

Alur kegiatan penelitian dilaksanakan secara bertahap mengikuti lima fase model Waterfall seperti pada Gambar 1, diawali dengan tahap analisis kebutuhan (*requirement analysis*) melalui observasi lapangan di CV. Indah Pratama dan studi literatur untuk mengidentifikasi permasalahan kunci manual serta memetakan spesifikasi teknis komponen. Selanjutnya tahap kedua, dilakukan perancangan sistem (*system design*) yang mencakup penyusunan diagram blok arsitektur, skema pengkabelan *hardware*, *flowchart* program *mikrokontroler*, diagram alur komunikasi *IoT*, dan struktur tabel Google Sheets. Tahap ketiga adalah implementasi (*construction and coding*), dilakukan perakitan komponen fisik, pembuatan casing *3D print*, pemrograman *firmware* ESP32, konfigurasi Google Apps Script, serta pembuatan algoritma *fail-safe buffering*. Tahap keempat adalah pengujian (*testing*) prototipe tersebut kemudian diuji melalui *Black Box Testing* untuk validasi fungsionalitas serta pengujian kinerja non-fungsional untuk mengukur tingkat akurasi biometrik (*success rate*) dan waktu tunda pengiriman data (*latency*). Pada tahap kelima adalah penerapan dan evaluasi (*deployment & evaluation*), sistem dipasang secara langsung pada pintu akses fisik CV. Indah Pratama untuk menguji keandalan operasional di lingkungan nyata serta mengevaluasi peningkatan efisiensi waktu akses dan administrasi data dibandingkan sistem kunci manual.



Gambar 1. Diagram Alur Penelitian

Instrumen penelitian terdiri atas perangkat keras (*hardware*) dan perangkat lunak (*software*). Perangkat keras yang digunakan meliputi ESP32 *DevKitC V4* sebagai pengendali utama sekaligus modul komunikasi *Wi-Fi*, sensor sidik jari AS608, *relay* 1 *channel*, *solenoid door lock 12V, LCD I2C 16×2, buzzer*, lima buah push button untuk navigasi menu dan pembuka pintu dari dalam, modul *LM2596 step-down*, serta *power supply 12V*. Peralatan pendukung meliputi laptop, *multimeter digital*, kabel mikro *USB*, solder, timah, *PCB*, dan casing hasil cetak *3D printer*. Sementara itu, perangkat lunak yang digunakan adalah *Arduino*

IDE untuk pengembangan program, Google Chrome, Google Apps Script sebagai penghubung komunikasi data, serta Google Sheets sebagai basis data *cloud*. Beberapa pustaka yang digunakan antara lain Adafruit Fingerprint, LiquidCrystal_I2C, HTTPClient, dan ArduinoJson.

Pengumpulan data dilakukan melalui empat teknik, yaitu observasi, pengujian sistem, pencatatan log otomatis, dan studi dokumentasi. Observasi digunakan untuk mengamati kinerja perangkat, interaksi pengguna, serta respons sistem terhadap berbagai kondisi. Pengujian sistem dilakukan untuk memperoleh data mengenai fungsionalitas dan performa sistem. Pencatatan log dilakukan secara otomatis oleh ESP32 ke Google Sheets setiap kali terjadi aktivitas akses pintu. Selain itu, studi dokumentasi dilakukan dengan mempelajari datasheet komponen, dokumentasi pustaka, dan berbagai literatur yang relevan.

Analisis data dilakukan untuk mengevaluasi kelayakan teknis dan kinerja sistem. Pengujian fungsional menggunakan *Black Box Testing* untuk memverifikasi setiap fitur, meliputi autentikasi sidik jari, tombol darurat, tombol pembuka pintu, tampilan *LCD, buzzer,* mekanisme *fail-safe buffering* saat koneksi internet terputus, serta kesesuaian antara aktivitas fisik dan data yang tersimpan pada Google Sheets. Pada mekanisme *fail-safe buffering*, ketika jaringan Wi-Fi terputus saat terjadi aktivitas akses, mikrokontroler ESP32 secara otomatis menyimpan paket data aktivitas berformat JSON ke dalam memori penampung (*buffer*) lokal perangkat, sehingga fungsi operasional pintu tetap berjalan normal. Selanjutnya, begitu koneksi internet kembali pulih (*online*), sistem secara otomatis melakukan sinkronisasi dengan mentransmisikan seluruh data yang tersimpan di memori lokal secara kronologis ke Google Sheets melalui Google Apps Script, sehingga integritas data (*data integrity*) tetap terjamin dan risiko kehilangan data (*data loss*) dapat dicegah.

Kinerja sistem dianalisis menggunakan statistik deskriptif berdasarkan dua parameter, yaitu persentase keberhasilan (*Success Rate*) dan *latency* pengiriman data. Persentase Keberhasilan (*Success Rate*) dihitung menggunakan Persamaan(1). Sementara itu, *latency* pengiriman data dari ESP32 ke Google Sheets dihitung menggunakan Persamaan (2) .

$$SR = \frac{P_{berhasil}}{P_{total}} X\ 100\% \quad (1)$$

Keterangan:

(SR) = persentase keberhasilan (%)

(P_{berhasil}) = jumlah percobaan yang berhasil dikenali

(P_{total}) = jumlah seluruh percobaan

$$L = n\,T_{rx} - T_{tx} \quad (2)$$

Keterangan:

(L) = rata-rata latency (ms)

(T_{rx}) = waktu data diterima dan tercatat pada Google Sheets (server *timestamp*)

(T_{tx}) = waktu data dikirim oleh ESP32 (*device timestamp*)

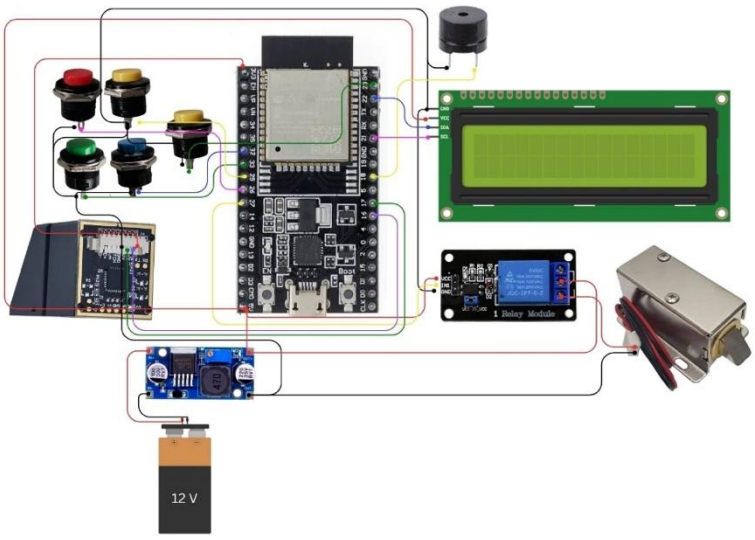
(n) = jumlah sampel pengujian.

3. HASIL DAN PEMBAHASAN

3.1. Implementasi Integrasi Sistem

Implementasi sistem smart door lock berbasis mikrokontroler ESP32 ini merupakan tahapan untuk menghasilkan sistem pengunci pintu otomatis. Proses integrasi ini mencakup tiga bagian utama, yaitu konfigurasi unit pemroses ESP32 dan integrasi sensor biometrik sidik jari AS608 beserta layar LCD. Selain itu, dilakukan pembuatan jalur komunikasi data berbasis cloud menggunakan Google Sheets.

Pada bagian pertama, ESP32 dikonfigurasi melalui Arduino IDE. Konfigurasi ini bertujuan untuk mengelola alokasi pin masukan atau keluaran, mengaktifkan modul Wi-Fi internal, serta mengendalikan saklar elektronik modul relay untuk memutus atau menyambung arus 12V menuju *solenoid door lock.* Gambar 2 menunjukkan skema rangkaian elektronika pada sistem *smart door lock*.



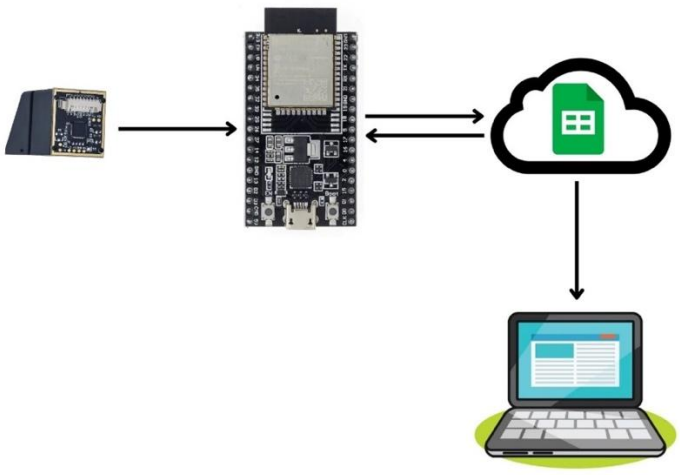
Gambar 2. Skema Rangkaian Elektornika Sistem *Smart Door Lock*

Detail pemetaan koneksi pin (*pin mapping*) antara Unit Pengendali Pusat (ESP32) dan komponen penyusun sistem dijelaskan secara rinci pada Tabel 1.

Tabel 1. Detail Koneksi Pin ESP32 dengan Komponen Sistem

No	Komponen	Pin ESP32 (GPIO)	Fungsi
1.	Sensor Sidik Jari (RX)	GPIO 17 (TX2)	Mengirim data/perintah ke sensor
2.	Sensor Sidik Jari (TX)	GPIO 16 (RX2)	Menerima data serial dari sensor
3.	Tombol Mode	GPIO 32	Memilih mode
4.	Tombol OK	GPIO 33	Konfirmasi pilihan
5.	Tombol UP	GPIO 25	Navigasi ke atas/Pendaftaran
6.	Tombol DOWN	GPIO 26	Navigasi ke bawah/Penghapusan
7.	Tombol Rilis (*Exit Button*)	GPIO 23	Membuka kunci dari dalam
8.	*Relay* (IN)	GPIO 27	Sinyal aktivasi *Solenoid*
9.	LCD I2C (SDA)	GPIO 21	Jalur *Data Serial Display*
10.	LCD I2C (SCL)	GPIO 22	Jalur *Clock Serial Display*
11.	*Buzzer*	GPIO 18	Indikator suara/*feedback*

Pada bagian kedua, sensor sidik jari AS608 diintegrasikan untuk memvalidasi identitas pengguna berdasarkan basis data lokal pada memori sensor, sementara *LCD* 16x2 difungsikan untuk menampilkan status operasional dan instruksi interaktif secara *real-time* kepada pengguna di lokasi pintu. Pada bagian ketiga, Google Sheets direalisasikan sebagai basis data penyimpanan *log* aktivitas jarak jauh. Komunikasi data ini dijembatani oleh Google Apps Script yang menerima data enkripsi HTTPS POST dari ESP32, memproses parameter masukan, dan menuliskan rekam riwayat tersebut langsung ke dalam baris tabel spreadsheet secara otomatis, detail seperti pada Gambar 3.



Gambar 3. Diagram Alur Komunikasi Data Esp32 ke Spreedsheet

Sinergi fungsional antar komponen ini memastikan kontrol akses fisik berjalan selaras dengan pencatatan digital. Ketika pemindaian sidik jari berhasil divalidasi oleh ESP32,

mikrokontroler akan mengirim sinyal pemicu ke modul *relay* untuk membuka *solenoid*. Pada saat yang sama, paket data aktivitas berformat JSON dikirimkan ke *cloud.* Google Apps Script bertindak sebagai *middleware* yang menerima data tersebut, secara otomatis menentukan waktu (*timestamp*) server, melakukan pencarian (*lookup*) ID pengguna pada sheet referensi, dan menyinkronkan data lengkap ke dalam *sheet* rekam akses.

3.2. Implementasi Antarmuka Lokal dan Cloud

Visualisasi dari hasil perakitan fisik perangkat keras dan dashboard pemantauan *cloud* disajikan untuk memberikan gambaran operasional sistem yang sesungguhnya di lapangan. Tampilan data pengguna dan riwayat log akses pada layanan *cloud* Google Sheets ditunjukkan pada Gambar 4 dan Gambar 5.

Waktu	ID	Nama Pengguna	Metode	Status
08/01/2026 6:18:34	2	Jiati	Fingerprint	Berhasil
08/01/2026 6:19:21	1	Fredy	Fingerprint	Berhasil
08/01/2026 6:19:28	0	Jari Tidak Dikenal	Fingerprint	Gagal
08/01/2026 6:19:34	3	Fram	Fingerprint	Berhasil
08/01/2026 6:19:39	0	Jari Tidak Dikenal	Fingerprint	Gagal
08/01/2026 6:19:50	2	Jiati	Fingerprint	Berhasil
12/01/2026 22:18:36	4	Lim	Fingerprint	Berhasil
12/01/2026 22:18:44	2	Jiati	Fingerprint	Berhasil
12/01/2026 22:20:17	2	Jiati	Fingerprint	Berhasil

Gambar 4. Desain Tabel Log Aktivitas

ID	Nama Pengguna
1	Fredy
2	Jiati
3	Fram
4	Lim
5	Andri
6	Indah
7	Indra
8	Adam
9	Azam
10	Mbah

Gambar 5. Tampilan Sheet Data User

Berdasarkan Gambar 5, tabel referensi menyimpan data identitas nama lengkap pengguna yang disinkronkan dengan ID unik sidik jari. Sementara itu, Gambar 3 membuktikan bahwa data log aktivitas telah berhasil direkam secara terstruktur dan kronologis, memuat parameter Waktu (*timestamp*), ID, Nama Pengguna, Metode, dan Status Akses. Selain

antarmuka cloud, pengguna di lokasi alat berinteraksi langsung melalui antarmuka visual LCD 16x2 yang menyajikan panduan sistem interaktif. Variasi tampilan layar LCD dalam berbagai kondisi operasional ditunjukkan pada Gambar 6-9.



Gambar 6. Antarmuka Layar LCD 16x2 dalam Berbagai Mode Operasional: (a) Mode Siaga

Tampilan mode siaga pada Gambar 6, menunjukkan kondisi awal sistem ketika berada dalam keadaan standby. Pada antarmuka LCD 16x2, layar menyajikan status konektivitas jaringan serta instruksi visual bagi pengguna untuk menempelkan jari pada modul sensor AS608. Tampilan ini menandakan bahwa mikrokontroler ESP32 berada dalam posisi siap untuk merespons masukan biometrik maupun pemicu tombol navigasi secara *real time.*



Gambar 7 Antarmuka Layar LCD 16x2 dalam Berbagai Mode Operasional: (b) Mode Admin

Tampilan mode admin pada Gambar 7, menyajikan antarmuka navigasi interaktif untuk pengelolaan hak akses pengguna yang diakses dengan menahan tombol "Mode" selama 3 detik. Layar LCD memberikan panduan langkah demi langkah bagi administrator, dimulai dari permintaan verifikasi sidik jari Admin (ID 1) hingga navigasi pilihan menu utama pendaftaran (*Enroll*) ID baru atau penghapusan (*Delete*) ID pengguna terdaftar menggunakan tombol *Up*, *Down*, dan OK.



Gambar 8. Antarmuka Layar LCD 16x2 dalam Berbagai Mode Operasional: (c) Mode Manual

Gambar 8 tampilan mode manual menampilkan indikasi visual saat prosedur akses darurat (*emergency access mode*) diaktifkan, yaitu melalui kombinasi penekanan tombol Mode selama 3 detik dilanjutkan tombol OK ketika sensor mengalami kendala fungsi. Layar LCD menyajikan keterangan bahwa *solenoid door lock* sedang dipicu aktif untuk membuka kunci pintu secara bypass tanpa melalui proses verifikasi biometrik.



Gambar 9. Antarmuka Layar LCD 16x2 dalam Berbagai Mode Operasional: (d) Hasil Verifikasi

Tampilan umpan balik akses (hasil verifikasi) ditampilkan pada Gambar 9 yang menyajikan umpan balik visual (*visual feedback*) seketika setelah pengguna melakukan pemindaian sidik jari. Apabila verifikasi biometrik cocok, layar LCD menampilkan pesan "Akses Berhasil" beserta nomor ID pengguna yang teridentifikasi. Sebaliknya, jika sidik jari yang ditempelkan tidak terdaftar dalam memori sensor, LCD menampilkan pesan "Akses Gagal" sebagai petunjuk visual bahwa hak akses ditolak.

Secara fisik pada Gambar 10, seluruh komponen elektronik utama (ESP32, sensor AS608, layar *LCD*, tombol navigasi, dan *buzzer*) diwadahi di dalam sebuah wadah (*casing*) kokoh hasil cetakan *3D Printer* untuk melindungi sistem dari kerusakan fisik luar tanpa menghambat akses pengguna. Penempatan aktuator mekanis (*solenoid door lock*), tombol keluar (*exit button*), dan unit kendali dirancang secara efisien pada area pintu CV. Indah Pratama.



Gambar 10. Perangkat Keras Smart Door Lock

3.3. Hasil Pengujian Fungsional (*Black Box Testing*)

Pengujian fungsional sistem dilakukan menggunakan metode *Black Box Testing* untuk memvalidasi respons masukan dan keluaran setiap fitur fisik serta logika program tanpa melihat kode program internal. Hasil pengujian menyeluruh terhadap skenario operasional sistem disajikan pada Tabel 2. Hasil pengujian menegaskan bahwa seluruh fitur fisik, logika perlindungan darurat (*fail-safe manual mode*), tombol rilis dalam (*exit button*), konektivitas Wi-Fi, hingga fitur penyimpanan sementara (*fail-safe buffering*) ketika internet terputus telah bekerja dengan sukses 100% sesuai spesifikasi rancangan.

Tabel 2. Hasil Pengujian Fungsionalitas Sistem

No	Fitur Uji	Skenario	Kriteria Keberhasilan	Hasil
1.	Verifikasi Biometrik	Menempelkan jari yang terdaftar	*Solenoid* terbuka, *Buzzer* bunyi pendek, LCD menampilkan "Akses Berhasil".	Berhasil
2.	Verifikasi Biometrik	Menempelkan jari yang tidak terdaftar	*Solenoid* tetap terkunci, *Buzzer* bunyi panjang, LCD menampilkan "Akses Gagal".	Berhasil
3.	Akses Menu Admin	Menahan tombol "Mode" selama 3 detik	Sistem meminta verifikasi Admin sebelum masuk ke tampilan Menu Admin.	Berhasil
4.	Navigasi Menu Admin	Menekan tombol Up, Down, dan OK	Indikator pilihan bergerak sesuai input dan masuk ke sub-menu yang dipilih.	Berhasil
5.	Pendaftaran *User* (*Enroll*)	Masuk menu admin "Pendaftaran", scan jari 2x	Data ID tersimpan di memori, LCD menampilkan "ID Terdaftar".	Berhasil
6.	Penghapusan *User* (*Delete*)	Masuk menu admin "Hapus ID", pilih ID	Data ID terhapus dari memori, LCD menampilkan "ID Dihapus".	Berhasil
7.	Mode Manual (*Emergency*)	Menahan tombol Mode 5 detik, lalu tekan OK	*Solenoid* terbuka, LCD menampilkan "Akses Berhasil".	Berhasil
8.	Tombol Keluar (*Exit Button*)	Menekan tombol rilis dari sisi dalam rumah	*Solenoid* terbuka, LCD menampilkan "Akses Berhasil".	Berhasil
9.	Koneksi *Wi-Fi*	Menghidupkan alat di area *hotspot*	LCD menampilkan "*Wi-Fi* connect".	Berhasil
10.	*Cloud Logging* (Integrasi)	Melakukan akses saat *Wi-Fi* terhubung	Data Waktu, ID, Nama, Metode, dan Status muncul secara akurat di Google Sheets.	Berhasil

No	Fitur Uji	Skenario	Kriteria Keberhasilan	Hasil
11.	Kemampuan Sistem (*Buffering*)	Mematikan internet, scan jari, lalu nyalakan kembali	Saat offline data tersimpan di memori lokal, saat online data otomatis terkirim susulan.	Berhasil

3.4. Pengujian Kinerja Performa Sistem

Pengujian performa sistem difokuskan pada analisis kuantitatif terhadap dua parameter utama, yaitu tingkat akurasi verifikasi sensor sidik jari (*Success Rate*) dan kecepatan transmisi data (*Latency*) menuju *cloud database*.

3.4.1. Pengujian Akurasi Verifikasi Sidik Jari

Pengukuran tingkat akurasi verifikasi sensor biometrik AS608 dihitung berdasarkan persentase keberhasilan (*Success Rate*) menggunakan Persamaan (1). Pengujian dilakukan melalui 10 percobaan penempelan sidik jari terdaftar untuk melihat kemampuan deteksi sensor. Rekapitulasi data uji akurasi sidik jari disajikan pada Tabel 3.

Tabel 3. Pengujian Akurasi Akses Sensor Sidik Jari

No.	Percobaan Ke-	Status (Berhasil/Gagal)
1.	1	Berhasil
2.	2	Berhasil
3.	3	Berhasil
4.	4	Berhasil
5.	5	Berhasil
6.	6	Berhasil
7.	7	Berhasil
8.	8	Berhasil
9.	9	Berhasil
10.	10	Berhasil
Total		**SR = 100%**

Berdasarkan Persamaan (1) dan data Tabel 3, hasil kalkulasi menunjukkan:

$SR = \frac{10}{10}\ X\ 100\% = 100\%.$

Sistem terbukti memiliki tingkat akurasi 100% dalam mengenali pengguna terdaftar dan menolak sidik jari yang tidak terdaftar secara presisi. Hal ini meminimalkan risiko kesalahan deteksi biometrik dalam membatasi akses ruangan di CV. Indah Pratama.

3.4.2. Pengujian *Latensi Transmisi Data (Logging)*

Pengujian latensi bertujuan untuk mengukur durasi waktu tunda (*delay*) pengiriman log data dari ESP32 hingga tercatat secara utuh di Google Sheets. Perhitungan rata-rata latensi menggunakan Persamaan (2).

Pengujian dilakukan sebanyak 10 kali sampel pengiriman data log aktivitas. Hasil pengukuran latensi transmisi disajikan pada Tabel 4.

Tabel 4. Hasil Pengukuran Latency Transmisi Data

No.	Percobaan Ke-	Waktu Kirim	Waktu Terima	*Latency* (*ms*)
1.	1	08:30:10.100	08:30:12.050	1.950
2.	2	08:35:15.250	08:35:17.200	1.950
3.	3	08:40:20.050	08:40:22.050	2.000
4.	4	08:45:05.150	08:45:07.250	2.100
5.	5	08:50:12.300	08:50:14.250	1.950
6.	6	08:55:10.400	08:55:12.380	1.980
7.	7	09:00:15.100	09:00:17.050	1.950
8.	8	09:05:20.350	09:05:22.370	2.020
9.	9	09:10:25.200	09:10:27.150	1.950
10.	10	09:15:30.450	09:15:32.400	1.950
Rata-rata				**1.980 ms**

Berdasarkan Persamaan (2) dan data Tabel 4, diperoleh nilai rata-rata latensi pengiriman data (L) sebesar 1.980 ms. Nilai latensi yang stabil di kisaran kurang dari dua detik ini menunjukkan performa komunikasi data IoT sangat responsif dan aman untuk pemantauan akses *real-time*.

3.5. Uji Coba Keseluruhan dan Analisis Stabilitas

Pengujian keseluruhan dilakukan untuk menganalisis kemampuan sistem dalam kondisi nyata. Pengujian stabilitas jaringan nirkabel diuji dengan memvariasikan jarak alat terhadap *gateway* internet untuk mengukur pengaruh kekuatan sinyal terhadap waktu tunda (*latency*), sebagaimana disajikan pada Tabel 5.

Tabel 5. Pengujian Stabilitas Jaringan terhadap Kecepatan Latensi

No.	Kondisi Sinyal	Jarak ke Gateway	Status Koneksi	Latency Rerata
1	Sangat Kuat	1 - 4 Meter	Stabil	< 2.000 ms
2	Cukup Kuat	5 - 9 Meter	Stabil	2.000 - 3.000 ms
3	Lemah	> 10 Meter	Terputus-putus	> 5.000 ms

Data Tabel 5 menunjukkan bahwa untuk menjaga performa optimal pencatatan data ke Google Sheets di bawah durasi 2 detik, posisi peletakan alat disarankan berada dalam radius sinyal stabil (di bawah 9 meter).

3.6. Analisis Efisiensi Sistem Baru Terhadap Sistem Lama

Tujuan utama peningkatan efisiensi akses telah terbukti tercapai melalui perbandingan operasional sistem baru (smart door lock) terhadap metode kunci manual lama. Evaluasi perbandingan durasi waktu akses pintu disajikan pada Tabel 6.

Tabel 6. Perbandingan Durasi Akses Pintu

No.	Metode Akses	Aktivitas Utama	Rata-rata Waktu	Keterangan
1	Kunci Manual	Mencari kunci, memasukkan, memutar kunci secara manual	10 - 15 Detik	Kurang Efisien
2	*Smart Door Lock*	Menempelkan sidik jari pada sensor biometrik	1 - 2 Detik	Sangat Efisien

Berdasarkan Tabel 6, implementasi teknologi kontrol akses berbasis biometrik sidik jari mampu memangkas durasi waktu akses hingga mencapai 85%. Untuk meninjau secara komprehensif, evaluasi perbandingan seluruh aspek manajemen operasional sistem lama dan sistem baru disajikan pada Tabel 7.

Tabel 7. Perbandingan Operasional Sistem Lama dan Baru

No	Aspek Evaluasi	Sistem Lama (Kunci Manual)	Sistem Baru (Smart Door Lock)
1.	Waktu Akses	10 - 15 Detik (Mencari & memutar kunci fisik)	1 - 2 Detik (Proses pemindaian biometrik)
2.	Pemantauan Data Akses	Tidak tersedia riwayat penggunaan pintu	Terpantau secara *real-time* lewat Google Sheets
3.	Keamanan Akses	Risiko kunci fisik hilang, tertinggal, atau diduplikasi secara ilegal	Otoritas akses personal melekat pada identitas biometrik
4.	Manajemen Pengguna	Perlu duplikat anak kunci fisik untuk menambah akses	Penambahan/penghapusan hak akses secara digital via Mode Admin
5.	Kondisi Darurat	Pintu terkunci total jika anak kunci fisik hilang	Tersedia Mode Manual darurat apabila modul sensor bermasalah

Secara keseluruhan, hasil analisis hasil dan pembahasan ini membuktikan bahwa transformasi sistem dari kunci manual ke *smart door lock* berbasis biometrik sidik jari dengan integrasi *cloud logging* di CV. Indah Pratama tidak hanya mengotomatisasi aspek fisik keamanan, tetapi juga memberikan solusi cerdas, cepat, transparan, serta berkelanjutan dalam administrasi data akses.

4. PENUTUP

Simpulan dan Saran

Sistem *smart door lock* berbasis mikrokontroler ESP32 dan sensor biometrik AS608 yang terintegrasi dengan layanan *cloud* Google Sheets telah berhasil dirancang, dibangun, dan diimplementasikan secara stabil di CV. Indah Pratama. Penerapan teknologi kontrol akses biometrik ini terbukti memberikan efisiensi operasional yang sangat signifikan dengan memangkas durasi waktu akses masuk dari rata-rata 10–15 detik menggunakan kunci fisik manual menjadi hanya 1–2 detik, yang setara dengan peningkatan kecepatan akses sebesar 85%. Keamanan dan pertanggungjawaban data juga terpenuhi secara transparan melalui fitur *logging* otomatis ke Google Sheets yang mencatat parameter waktu (*timestamp*), ID pengguna, nama pengguna, metode, dan status akses secara presisi, didukung oleh tingkat akurasi verifikasi biometrik sensor sebesar 100% serta ketersediaan fungsi tombol mode manual sebagai sistem cadangan darurat yang handal apabila sensor mengalami kendala fungsi. Untuk pengembangan sistem ini di masa mendatang, disarankan adanya penambahan sistem penyuplai daya cadangan seperti baterai atau power bank tambahan agar perangkat tetap dapat beroperasi optimal saat terjadi pemadaman listrik PLN, peningkatan fitur keamanan aktif berupa notifikasi pesan instan kepada pemilik serta peringatan khusus apabila terjadi upaya akses gagal yang berulang oleh pengguna tidak terdaftar, serta penguatan kualitas jaringan *Wi-Fi* di area pemasangan guna memastikan waktu tunda (*latency*) pengiriman data ke basis data cloud tetap stabil di bawah 2.000 ms dalam jangka waktu panjang.

DAFTAR PUSTAKA

Alfonsius, E., Ruitan, A. S., & Liuw, D. (2024). Pengembangan Sistem Keamanan Pintu Menggunakan Metode Prototype Berbasis RFID dan Keypad 4x4 dengan Arduino Nano. *Jurnal Ilmiah Informatika Dan Ilmu Komputer (JIMA-ILKOM)*, *3*(2), 110–123. https://doi.org/10.58602/jima-ilkom.v3i2.33

Anis, Y., Mukti, A. B., & Rosyid, A. N. (2023). KLIK: Kajian Ilmiah Informatika dan Komputer Penerapan Model Waterfall Dalam Pengembangan Sistem Informasi Aset Destinasi Wisata Berbasis Website. *Media Online)*, *4*(2), 1134–1142. https://doi.org/10.30865/klik.v4i2.1287

Ardiansah, A., Nuraeni, M., & Ridwang[3], A. (2024). Rancang Bangun Akses Kunci Pintu Otomatis menggunakan Fingerprint Berbasis Internet of Things (IoT). *VERTEX ELEKTRO*.

Amalia, N., & Muhammad. (2024). *Rancang Bangun Sistem Keamanan Pintu Menggunakan Modul RFID Berbasis IoT*. *1*(2).

https://jurnal.komputasi.org/index.php/jst/article/view/20/

Ega Satrya, M., & Servanda, Y. (2024). *Penggunaan Teknologi Biometrik Fingerprint Untuk Meningkatkan Aplikasi Kimia Farma Use Of Fingerprint Biometric Technology To Improve Kimia Farma Applications*. https://doi.org/10.47002/seminastika.v5i1.816

Maulana, I., Azriadi, E., & Musrido, J. (2023). Rancang Bangun Sistem Smart Door Lock Menggunakan Mikrokontroler Esp32 Berbasis Internet Of Things (Iot) dan Smartphone Android. *Jurnal Teknik Industri Terintegrasi*, *6*(1), 195–208. https://doi.org/10.31004/jutin.v6i1.15123

Pratama, R. A., Pratikto, P., & Arman, M. (2023). Sistem Akuisisi Data Temperatur Showcase Berbasis IoT Menggunakan ESP32 dengan Sensor Termokopel dan Logging ke Google Spreadsheets. *Prosiding Industrial Research Workshop and National Seminar*, *14*(1), 252–257. https://doi.org/10.35313/irwns.v14i1.5395

Putra, G. R., Situmorang, B. H., & Hidayatullah, S. (2023). Identifikasi Biometrika Menggunakan Ekstraksi Minutiae Pada Citra Sidik Jari. *Jurnal Teknoinfo*, *17*(1), 289. https://doi.org/10.33365/jti.v17i1.2376

Suci Br Kembaren, Elsadora Haroannauli Patricia Br Gurning, & Any Kurniawaty Yapie. (2023). IOT Pada Purwarupa Sistem Keamanan Pintu Kantor Dengan Sensor RFID dan PIR Berbasis Telegram. *Jurnal Teknik Mesin, Elektro Dan Ilmu Komputer*, *3*(3), 84–97. https://doi.org/10.55606/teknik.v3i3.2510

Waruwu, M. (2024). Metode Penelitian dan Pengembangan (R&D): Konsep, Jenis, Tahapan dan Kelebihan. *Jurnal Ilmiah Profesi Pendidikan*, *9*(2), 1220–1230. https://doi.org/10.29303/jipp.v9i2.2141

Zain, A., Amar, M. I., Resky, A., Putriani, A. I., & Imansyah, N. (2024). Safe Lock Security Prototype Using Fingerprint And Pin. *INTEK: Jurnal Penelitian*, *11*(1), 31–36. https://doi.org/10.31963/intek.v11i1.4780