



Rancang Bangun Sistem Keamanan Kotak Persembahan Gereja Berbasis Internet of Things (IoT) Menggunakan Metode Research and Development (R&D)

Design and Development of an IoT-Based Security System for Church Offering Boxes Using the Research and Development (R&D) Approach

Kasianus Yosef Yoel*, Ahmad Fajri, Kusnandar

Program Studi Teknik Informatika, STMIK Widya Cipta Dharma, Samarinda, Indonesia

Email: ¹*2143038@wicida.ac.id, ²ahmadfajri@wicida.ac.id, ³kusnandar@wicida.ac.id

Email Penulis Korespondensi: 2143038@wicida.ac.id

Received: 30/09/2026, Revised: 15/10/2026, Accepted: 16/10/2026, Published: 16/10/2026

Abstrak—Keamanan kotak persembahan gereja perlu diperhatikan untuk mencegah akses tanpa izin dan mendukung pemantauan kondisi kotak secara lebih efektif. Penelitian ini bertujuan untuk merancang dan membangun sistem keamanan kotak persembahan gereja berbasis Internet of Things (IoT) yang mampu melakukan autentikasi pengguna, mengendalikan akses kunci, mendeteksi kondisi pembukaan kotak, serta mengirimkan informasi keamanan secara real-time. Metode yang digunakan adalah Research and Development (R&D) yang diterapkan melalui tahapan analisis kebutuhan, perancangan, pengembangan, implementasi, dan pengujian terhadap prototipe. Sistem dibangun menggunakan NodeMCU ESP8266 sebagai mikrokontroler, sensor fingerprint AS608 sebagai autentikasi, solenoid lock sebagai pengunci, magnetic door switch sebagai pendeteksi pembukaan, OLED sebagai media informasi, serta Telegram sebagai media notifikasi. Pengujian fungsional dilakukan menggunakan metode black-box pada enam skenario. Hasil pengujian menunjukkan bahwa seluruh tiga percobaan menggunakan sidik jari yang telah terdaftar berhasil memberikan akses, sedangkan dua percobaan menggunakan sidik jari yang tidak terdaftar berhasil ditolak. Sistem juga berhasil mengirimkan notifikasi Telegram pada seluruh lima jenis notifikasi dengan waktu respons 0,9–1,3 detik. Selain itu, mekanisme lockdown aktif setelah lima kali kegagalan autentikasi berturut-turut selama tiga menit, deteksi pembukaan paksa berhasil dijalankan, dan fungsi keamanan lokal tetap bekerja ketika koneksi Wi-Fi terputus. Kebaruan penelitian ini terletak pada integrasi autentikasi sidik jari, deteksi pembukaan paksa, mekanisme lockdown, kendali Telegram, dan pengujian fungsi keamanan lokal saat Wi-Fi terputus dalam satu purwarupa untuk kotak persembahan gereja, dengan firmware non-blocking yang memprioritaskan proses lokal (hardware-first). Kontribusi penelitian berupa rancangan purwarupa, arsitektur firmware tersebut, dan data pengujian fungsional yang dapat menjadi acuan pengembangan sistem serupa.

Kata Kunci: ESP8266; Sensor Sidik Jari AS608; Sistem Keamanan; IoT; Telegram

Abstract—The security of church offering boxes needs to be addressed to prevent unauthorized access and support more effective monitoring of the box condition. This study aims to design and develop an Internet of Things (IoT)-based security system for church offering boxes that can perform user authentication, control access to the lock, detect box opening conditions, and send security information in real time. The Research and Development (R&D) method was applied through the stages of requirements analysis, design, development, implementation, and prototype testing. The system combines a NodeMCU ESP8266, an AS608 fingerprint sensor, a solenoid lock, a magnetic door switch, an OLED display, and Telegram notification. The results showed that all three trials using registered fingerprints successfully granted access, while two trials using unregistered fingerprints were successfully rejected. The system also successfully delivered Telegram notifications in all five notification types, with response times ranging from 0.9 to 1.3 seconds. The lockdown mechanism was activated after five consecutive authentication failures for three minutes, forced opening detection operated successfully, and local security functions remained operational when the Wi-Fi connection was unavailable. The novelty of this study lies in integrating fingerprint authentication, forced-opening detection, a lockdown mechanism, Telegram-based control, and testing of local security functions under Wi-Fi loss in a single prototype for church offering boxes, using non-blocking firmware that prioritizes local processing (hardware-first). The contribution is the prototype design, this firmware architecture, and functional test data that can serve as a reference for developing similar systems.

Keywords: ESP8266; AS608 Fingerprint Sensor; Security System; IoT; Telegram

1. PENDAHULUAN

Kotak persembahan gereja merupakan tempat penyimpanan uang persembahan jemaat yang perlu memiliki sistem keamanan untuk mencegah akses oleh pihak yang tidak berwenang. Uang yang terkumpul perlu dijaga keamanannya karena kotak persembahan menjadi tempat penyimpanan sementara sebelum dilakukan pengambilan dan pengelolaan oleh pihak yang berwenang. Penggunaan kunci konvensional pada kotak penyimpanan memiliki keterbatasan karena belum dapat melakukan autentikasi pengguna dan memberikan informasi mengenai kondisi kotak secara langsung. Kondisi tersebut dapat menyulitkan pihak yang berwenang dalam mengetahui aktivitas akses dan perubahan kondisi pintu tanpa melakukan pemeriksaan secara langsung.

Penelitian terdahulu mengenai sistem keamanan kotak amal juga telah menunjukkan penggunaan komponen elektronik dan teknologi *Internet of Things* (IoT) untuk meningkatkan keamanan serta memungkinkan kondisi perangkat dipantau melalui jaringan internet. Berdasarkan permasalahan tersebut, penelitian ini merancang sistem keamanan kotak persembahan gereja dengan menggunakan sensor sidik jari AS608 sebagai autentikasi pengguna, ESP8266 sebagai pusat pengendali, *magnetic door switch* untuk mendeteksi kondisi pintu, buzzer sebagai indikator peringatan, serta Telegram





sebagai media notifikasi dan pengendalian. Salah satu penerapannya adalah sistem keamanan pada tempat penyimpanan benda atau uang yang memiliki nilai, seperti kotak uang, kotak amal, dan brankas. Penggunaan teknologi pada sistem penyimpanan tersebut bertujuan untuk meningkatkan keamanan, memberikan kemudahan dalam proses akses, serta mengurangi ketergantungan terhadap sistem pengamanan konvensional. Penelitian mengenai pengamanan kotak amal menunjukkan bahwa penggunaan komponen elektronik dapat menjadi alternatif untuk meningkatkan keamanan terhadap risiko pencurian [1], [2]. Selain itu, pengembangan sistem keamanan pada kotak amal juga telah memanfaatkan *teknologi Internet of Things* (IoT) sehingga kondisi perangkat dapat dipantau melalui jaringan internet [3].

Pada kenyataannya, sistem keamanan pada tempat penyimpanan masih banyak menggunakan kunci fisik atau gembok manual. Sistem tersebut memiliki keterbatasan karena kunci dapat hilang, rusak, diduplikasi, atau digunakan oleh pihak yang tidak memiliki hak akses. Permasalahan serupa juga ditemukan pada sistem pengamanan brankas yang masih menggunakan mekanisme konvensional, sehingga diperlukan metode autentikasi yang lebih terkontrol [4]. Penelitian mengenai brankas menunjukkan bahwa penggunaan kunci elektronik berbasis mikrokontroler dan solenoid dapat digunakan untuk mengotomatisasi proses penguncian dan pembukaan [5]. Penelitian lain mengembangkan purwarupa sistem pengamanan dan pelacak brankas yang menggabungkan sensor sidik jari dengan modul GPS berbasis IoT sehingga kondisi maupun lokasi perangkat dapat dipantau dari jarak jauh [6]. Penelitian mengenai keamanan brankas berbasis sensor sidik jari lainnya menunjukkan bahwa autentikasi biometrik dapat digunakan sebagai metode pengganti kunci konvensional [7].

Salah satu teknologi yang dapat digunakan sebagai metode autentikasi adalah sensor sidik jari. Sidik jari memiliki karakteristik yang berbeda pada setiap individu sehingga dapat digunakan sebagai identitas biometrik dalam proses verifikasi pengguna. Penelitian mengenai pengamanan pintu menggunakan sensor sidik jari menunjukkan bahwa akses dapat diberikan kepada pengguna yang telah terdaftar, sedangkan pengguna yang tidak dikenali dapat ditolak dan sistem dapat memberikan peringatan [8]. Penerapan *fingerprint* pada sistem keamanan brankas juga telah dikembangkan dengan kombinasi sensor lain untuk meningkatkan keamanan akses [9]. Selain itu, penelitian mengenai sistem keamanan sepeda motor menunjukkan bahwa *fingerprint* dapat digunakan sebagai pengendali akses yang terintegrasi dengan mikrokontroler dan sistem IoT [10].

Perkembangan *Internet of Things* memungkinkan perangkat keamanan terhubung dengan jaringan internet sehingga informasi dari sistem dapat dikirimkan kepada pengguna. Salah satu penelitian mengembangkan sistem penguncian pintu berbasis NodeMCU ESP8266 dengan *fingerprint* yang terhubung dengan konsep IoT [11]. Penelitian lain mengembangkan akses kunci pintu berbasis ESP32 dan sensor *fingerprint* AS608 yang terhubung dengan Telegram, sehingga pintu dapat dikendalikan dari jarak jauh dan pemilik memperoleh notifikasi ketika sidik jari tidak cocok atau pintu dibuka secara paksa [12]. Telegram juga dimanfaatkan sebagai antarmuka kendali pada kotak amal masjid berbasis ESP32 yang pintunya dapat dibuka melalui kartu RFID atau bot Telegram [13].

Telegram dapat digunakan sebagai media komunikasi antara sistem keamanan dengan pengguna. Penelitian pada sistem keamanan brankas berbasis NodeMCU ESP8266 dan *fingerprint* memanfaatkan Telegram untuk memberikan notifikasi kepada pemilik [5]. Penelitian pada sistem keamanan brankas menggunakan NodeMCU dan *fingerprint* juga memanfaatkan Telegram untuk memberikan notifikasi kepada pemilik apabila terjadi kesalahan autentikasi atau kondisi tertentu [4]. Penelitian lainnya menerapkan verifikasi *password* dan sidik jari pada brankas berbasis IoT serta menggunakan Telegram untuk mengirimkan notifikasi ketika terjadi percobaan akses yang tidak sesuai [14].

Penerapan *fingerprint* dan Telegram juga telah dikembangkan pada sistem keamanan kotak amal menggunakan ESP32-CAM. Sistem tersebut menggunakan *fingerprint* untuk akses pembukaan kotak dan Telegram untuk mengirimkan foto apabila terjadi percobaan pembukaan tanpa sidik jari terdaftar [3]. Pada objek kotak amal masjid, pengamanan juga dilakukan melalui jaringan sensor nirkabel dan SMS gateway untuk menyampaikan informasi kepada pengurus [1]. Penelitian lain menerapkan kombinasi *fingerprint* dan alarm dengan notifikasi Telegram berbasis IoT pada sistem keamanan pintu pagar untuk mencegah akses oleh pihak yang tidak berwenang [15], serta *fingerprint* pada *security door lock* berbasis mikrokontroler [16]. Hal tersebut menunjukkan bahwa integrasi autentikasi biometrik dan komunikasi berbasis internet dapat digunakan untuk memberikan perlindungan sekaligus informasi kepada pengguna.

Mikrokontroler ESP8266 dipilih dalam penelitian ini karena memiliki kemampuan pemrosesan dan konektivitas Wi-Fi yang sesuai untuk pengembangan sistem berbasis IoT. Mikrokontroler keluarga ESP, yaitu ESP8266 dan ESP32, telah digunakan pada berbagai penelitian yang mengintegrasikan sensor *fingerprint* atau Telegram dengan sistem berbasis internet [10], [11], [12], [13]. Penggunaan mikrokontroler tersebut memungkinkan proses pembacaan sensor, pengolahan data autentikasi, pengendalian mekanisme pengunci, serta pengiriman informasi kepada pengguna dilakukan dalam satu sistem. Pengembangan sistem penyimpanan yang memadukan *fingerprint* dan *face recognition* telah dilakukan pada *smart locker* untuk memberikan autentikasi pengguna pada loker penyimpanan [17]. Penerapan sensor sidik jari AS608 pada ESP32 juga dilaporkan pada sistem keamanan kendaraan roda dua yang memadukan autentikasi sidik jari, pelacakan lokasi menggunakan GPS, dan antarmuka Telegram untuk kontrol serta notifikasi, dengan rata-rata waktu respons pengenalan sidik jari 1,8 detik [18].

Meskipun teknologi *fingerprint*, mikrokontroler, solenoid, dan IoT telah banyak diterapkan pada sistem keamanan pintu, brankas, kotak amal, dan tempat penyimpanan, penelitian-penelitian tersebut memiliki beberapa keterbatasan bila diterapkan pada kotak persembahan gereja. Pertama, sistem pada [3], [4], [5], dan [15] memanfaatkan *fingerprint* dan notifikasi Telegram, tetapi tidak melaporkan mekanisme pembatasan percobaan akses berulang maupun deteksi pembukaan pintu tanpa otorisasi. Kedua, deteksi pembukaan paksa dilaporkan pada [12] menggunakan sensor getar untuk pintu rumah, sedangkan kendali melalui Telegram pada kotak amal [13] menggunakan RFID tanpa autentikasi biometrik.



Ketiga, tidak satu pun penelitian yang dikaji melaporkan pengujian apakah fungsi pengamanan tetap berjalan saat koneksi Wi-Fi terputus, padahal seluruh sistem tersebut bergantung pada jaringan untuk notifikasi. Keempat, objek penelitian terdahulu adalah kotak amal masjid, brankas, dan pintu, sedangkan kotak persembahan gereja belum menjadi objek. Perbandingan fitur penelitian terkait dengan penelitian ini disajikan pada Tabel 1.

Tabel 1. Perbandingan Fitur Penelitian Terkait dengan Penelitian yang Dilakukan

Referensi	Objek	<i>Fingerprint</i>	Deteksi pembukaan paksa	<i>Lockdown</i>	Kendali Telegram	Uji fungsi lokal saat <i>offline</i>
[1]	Kotak amal masjid	–	–	–	–	–
[3]	Kotak amal	√	–	–	–	–
[4]	Brankas	√	–	–	–	–
[5]	Brankas	√	–	–	–	–
[15]	Pintu pagar	√	–	–	–	–
[12]	Pintu rumah	√	√	–	√	–
[13]	Kotak amal masjid	–	–	–	√	–
Penelitian ini	Kotak persembahan gereja	√	√	√	√	√

Keterangan: √ = dilaporkan; – = tidak dilaporkan dalam artikel tersebut.

Berdasarkan Tabel 1, belum ditemukan penelitian yang mengintegrasikan keempat lapis pengamanan berikut dalam satu purwarupa untuk kotak persembahan gereja: (1) pencegahan melalui autentikasi sidik jari; (2) pembatasan melalui *lockdown* setelah kegagalan autentikasi berulang; (3) pendeteksian pembukaan tanpa otorisasi melalui *magnetic door switch* disertai alarm lokal dan notifikasi Telegram; serta (4) keandalan melalui fungsi keamanan lokal yang tetap berjalan saat Wi-Fi terputus. Celah (*gap*) inilah yang dijawab oleh penelitian ini.

Dibandingkan [12], sistem ini menambahkan *lockdown* dan pengujian operasi *offline*, serta mendeteksi perubahan posisi pintu secara langsung melalui *magnetic door switch*. Dibandingkan [3], [4], [5], dan [15], sistem ini menambahkan deteksi pembukaan paksa, pembatasan percobaan akses, dan kendali jarak jauh. Dibandingkan [13], sistem ini menambahkan autentikasi biometrik sehingga akses tidak bergantung pada kartu atau akun pengguna. Keunggulan tersebut bersifat kualitatif, yaitu pada kelengkapan lapisan pengamanan. Kebaruan penelitian ini terletak pada integrasi lapisan-lapisan tersebut dalam satu arsitektur *firmware non-blocking* yang memprioritaskan proses lokal (*hardware-first asynchronous polling*) dan diverifikasi melalui pengujian *black-box* pada kotak persembahan gereja.

Rumusan masalah penelitian ini adalah bagaimana merancang dan membangun sistem keamanan kotak persembahan gereja berbasis IoT yang mampu mengautentikasi pengguna, mengendalikan akses kunci, mendeteksi kondisi pintu, dan menyampaikan informasi keamanan secara *real-time*, serta bagaimana kinerja fungsionalnya. Tujuan penelitian ini adalah merancang, membangun, dan menguji purwarupa sistem keamanan kotak persembahan gereja berbasis IoT yang mengintegrasikan autentikasi sidik jari, *lockdown*, deteksi pembukaan paksa, serta notifikasi dan kendali Telegram, dengan fungsi keamanan lokal yang tetap berjalan saat Wi-Fi terputus.

Kontribusi penelitian ini adalah: (1) rancangan purwarupa pengamanan berlapis untuk kotak persembahan gereja; (2) arsitektur *firmware finite state machine non-blocking* dengan *hardware-first asynchronous polling* dan *Safe Rollback* yang dirancang agar keputusan akses lokal diproses lebih dahulu daripada komunikasi jaringan (waktu respons autentikasi rata-rata 0,96 detik pada pengujian) dan konektivitas dapat dipulihkan otomatis; serta (3) data pengujian fungsional *black-box* pada enam skenario yang dapat menjadi acuan pengembangan sistem serupa.

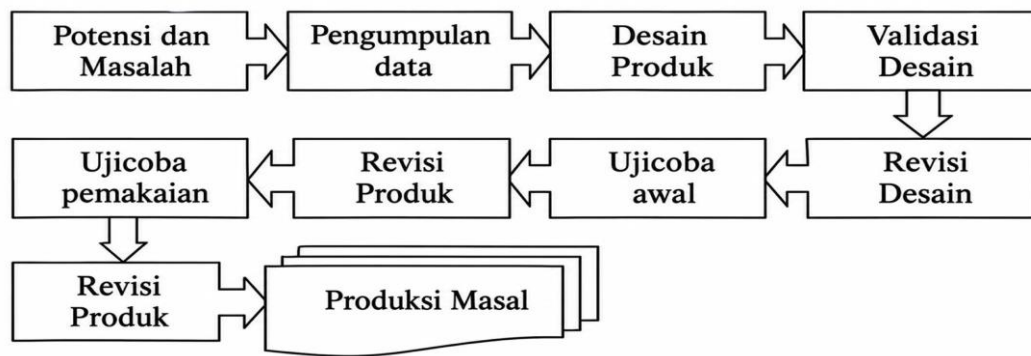
2. METODOLOGI PENELITIAN

2.1 Tahapan Penelitian

Penelitian ini menggunakan metode *Research and Development* (R&D), yaitu metode penelitian untuk menghasilkan produk tertentu dan menguji keefektifan produk tersebut [19]. Metode ini dipilih karena penelitian tidak hanya menghasilkan purwarupa sistem keamanan kotak persembahan, tetapi juga mengujinya untuk mengetahui kinerja setiap fungsinya.

Tahapan R&D mengacu pada sepuluh langkah menurut Sugiyono [19] sebagaimana ditunjukkan pada Gambar 1, yaitu potensi dan masalah, pengumpulan data, desain produk, validasi desain, revisi desain, uji coba produk, revisi produk, uji coba pemakaian, revisi produk, dan produksi massal. Setiap Langkah pada Gambar 1 menghasilkan keluaran yang menjadi masukan bagi Langkah berikutnya dan dapat diulang apabila ditemukan kekurangan.

Penelitian ini, keluaran tahapan awal berupa kebutuhan sistem keamanan kotak persembahan, dilanjutkan rancangan perangkat keras, perangkat lunak, dan alur kerja sehingga purwarupa beserta data pengujiannya, sehingga hasil penelitian dapat ditelusuri dari masalah yang diidentifikasi sampai produk yang diuji. Penjelasan tiap tahapan diuraikan berikut.



Gambar 1. Langkah-langkah Penggunaan *Metode Research and Development (R&D)*

Penelitian diawali dengan mengidentifikasi masalah pada keamanan kotak persembahan yang masih memiliki keterbatasan dalam autentikasi pengguna dan pemantauan kondisi kotak. Kondisi tersebut menjadi dasar untuk mengembangkan sistem keamanan berbasis teknologi mikrokontroler dan *Internet of Things (IoT)*.

Pengumpulan data dilakukan dengan mengumpulkan informasi melalui studi literatur dari jurnal, buku, dan sumber relevan mengenai sistem keamanan, ESP8266, sensor sidik jari AS608, IoT, Telegram, *solenoid door lock*, *magnetic door switch*, OLED, dan buzzer. Informasi tersebut digunakan sebagai dasar dalam menentukan kebutuhan sistem. Pada tahap ini dibuat rancangan perangkat keras dan perangkat lunak sistem. ESP8266 berfungsi sebagai mikrokontroler, AS608 sebagai autentikasi sidik jari, relay dan *solenoid door lock* sebagai mekanisme penguncian, *magnetic door switch* sebagai pendeteksi pintu, OLED dan buzzer sebagai media informasi/peringatan, serta Telegram sebagai media notifikasi dan kendali sistem.

Rancangan yang telah dibuat diperiksa untuk mengetahui kesesuaiannya dengan kebutuhan sistem. Validasi meliputi rancangan perangkat keras, perangkat lunak, hubungan antar komponen, serta alur kerja sistem sebelum direalisasikan menjadi prototype. Apabila ditemukan kekurangan pada hasil validasi, dilakukan perbaikan terhadap rancangan, baik pada rangkaian komponen maupun alur kerja program, sehingga desain siap digunakan pada tahap pembuatan produk. Desain yang telah diperbaiki kemudian direalisasikan menjadi prototipe sistem keamanan kotak persembahan dengan mengintegrasikan ESP8266, AS608, relay, *solenoid door lock*, *magnetic door switch*, OLED, buzzer, dan Telegram.

Prototipe diuji untuk mengetahui fungsi masing-masing komponen dan sistem, meliputi pembacaan sidik jari, autentikasi pengguna, pembukaan dan penguncian *solenoid*, pendeteksian kondisi pintu, buzzer, OLED, serta komunikasi melalui Telegram. Setelah fungsi sistem berhasil diuji, dilakukan uji coba pemakaian melalui simulasi penggunaan dalam kondisi yang menyerupai keadaan sebenarnya. Pengujian dilakukan untuk mengetahui kinerja sistem secara keseluruhan dan menemukan kemungkinan kekurangan saat digunakan. Jika ditemukan kekurangan selama uji coba pemakaian, dilakukan penyempurnaan pada perangkat keras maupun perangkat lunak. Revisi dilakukan agar prototipe dapat bekerja sesuai dengan fungsi dan kebutuhan yang telah ditentukan.

Produksi massal merupakan tahap akhir dalam model R&D setelah produk dinyatakan layak. Pada penelitian ini, tahap produksi massal tidak dilaksanakan karena penelitian dibatasi pada pengembangan dan pengujian satu prototipe sistem keamanan kotak persembahan.

2.2 Perancangan Perangkat Keras

Perancangan perangkat keras diawali dengan menentukan komponen elektronik yang dibutuhkan beserta fungsinya dalam sistem, sebagaimana ditunjukkan pada Tabel 2.

Tabel 2. Kebutuhan Perangkat Keras

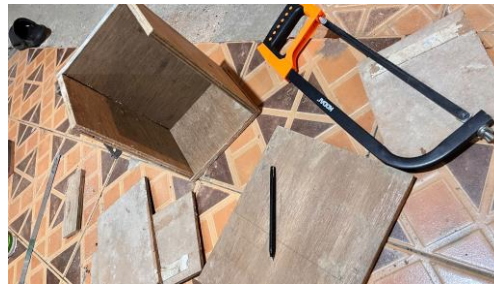
No	Komponen	Fungsi
1	NodeMCU ESP8266	Pusat pengendali sistem dan konektivitas Wi-Fi
2	Sensor Fingerprint AS608	Media autentikasi biometrik pengguna
3	Modul Relay 1 Channel (Solenoid)	Mengendalikan aktuator solenoid door lock
4	Modul Relay 1 Channel (Buzzer)	Mengendalikan active buzzer sebagai alarm
5	OLED 0.91" I2C (SSD1306)	Menampilkan status sistem secara fisik
6	Magnetic Door Switch (NC)	Mendeteksi kondisi buka/tutup pintu
7	Solenoid Door Lock	Aktuator penahan/pengunci pintu kotak uang
8	Modul Power Supply 12V	Sumber daya rangkaian relay dan solenoid

Konfigurasi jalur GPIO antara setiap komponen dengan NodeMCU ESP8266 ditunjukkan pada Tabel 3. Pemilihan pin disesuaikan dengan kebutuhan komunikasi masing-masing modul, seperti komunikasi *SoftwareSerial* untuk sensor sidik jari dan komunikasi I2C untuk layar OLED.

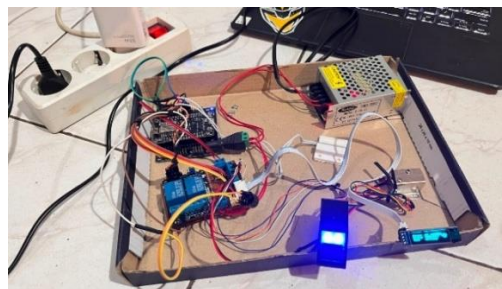
Tabel 3. Konfigurasi Pin GPIO NodeMCU ESP8266

Komponen	Pin Silkscreen	GPIO
Fingerprint AS608 (TX/RX)	D5 / D6	GPIO 14 / GPIO 12
OLED SDA / SCL	D2 / D1	GPIO 4 / GPIO 5
Magnetic Door Switch	D7	GPIO 13 (INPUT_PULLUP)
Relay Solenoid Door Lock	D0	GPIO 16
Relay Active Buzzer	D3	GPIO 0

Setelah komponen dan konfigurasi pin ditentukan, tahap selanjutnya adalah pembuatan bodi kotak yang menggunakan bahan papan kayu (multiplek) yang dipotong dan dirangkai sesuai ukuran rancangan, sebagaimana ditunjukkan pada Gambar 2.

**Gambar 2.** Proses Pemotongan dan Perakitan Bodi Kotak

Tahapan berikutnya dilanjutkan dengan penataan seluruh komponen elektronik yang akan dipasang pada bodi kotak. Sebelum pemasangan, komponen akan diuji terlebih dahulu agar sistem antarperangkat dapat bekerja dengan baik, sebagaimana terlihat pada Gambar 3.

**Gambar 3.** Penataan Komponen Elektronik Sebelum Pemasangan

Sensor sidik jari AS608 dan layar OLED dipasang pada bagian pintu kotak agar mudah diakses oleh pengguna, sedangkan NodeMCU ESP8266, modul relay, dan *solenoid door lock* dipasang pada bagian dalam kotak dan dihubungkan menggunakan kabel jumper sesuai dengan konfigurasi pin pada Tabel 3. Hasil pengkabelan internal sistem ditunjukkan pada Gambar 4.

**Gambar 4.** Hasil Pengkabelan Komponen di Dalam Kotak

2.3 Perancangan Perangkat Lunak

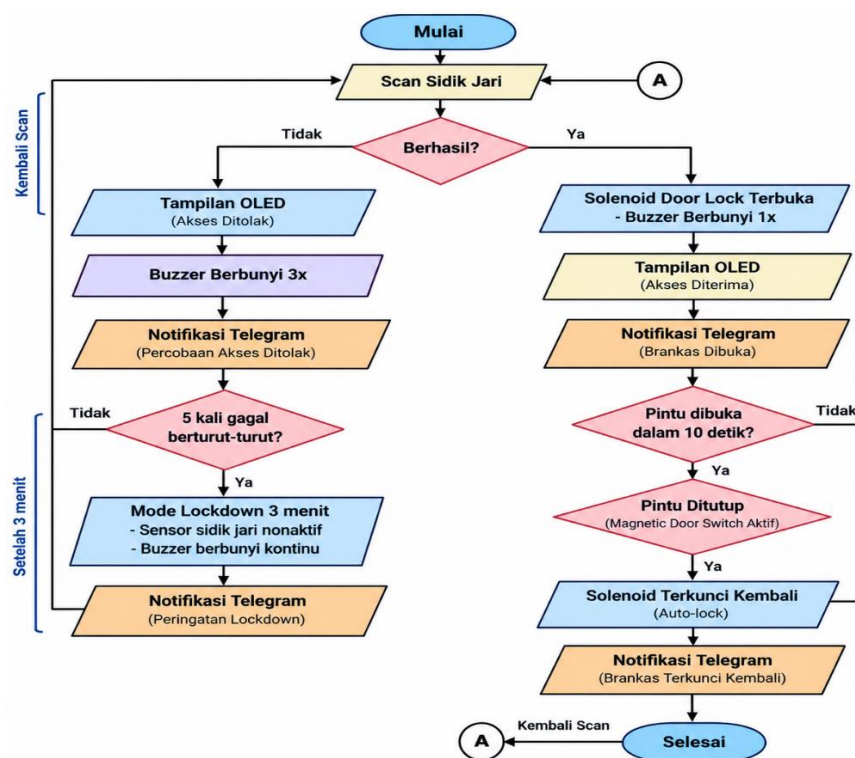
Perangkat lunak (firmware) dikembangkan menggunakan Arduino IDE dengan bahasa C/C++ dan dikompilasi untuk papan NodeMCU 1.0 (ESP-12E Module) dengan pembagian memori flash 4 MB (1 MB dialokasikan untuk LittleFS). Program utama dirancang dengan struktur *finite state machine* (FSM) non-blocking pada fungsi loop() sehingga pembacaan sensor sidik jari, sensor pintu, dan polling Telegram dapat berjalan hampir bersamaan tanpa menggunakan fungsi delay() yang dapat menghambat respons sistem.

Beberapa mekanisme utama yang diterapkan pada perangkat lunak antara lain: (1) *hardware-first asynchronous* Telegram polling dengan interval 4 detik yang otomatis dibatalkan ketika terdapat aktivitas sensor lokal, sehingga proses autentikasi sidik jari tetap responsif; (2) penyimpanan log audit dalam format teks polos (history.txt) untuk menjaga ketersediaan memori (free heap) tetap di atas 28 KB agar proses *enkripsi* TLS/SSL pada komunikasi Telegram tetap berjalan lancar; (3) fitur pengaturan Wi-Fi dinamis (/setwifi) dengan mekanisme *Safe Rollback*, yaitu pengujian koneksi ke jaringan baru selama 15 detik sebelum diterapkan secara permanen, dan pengembalian otomatis ke jaringan sebelumnya apabila pengujian gagal; (4) mekanisme *lockdown* yang menonaktifkan sensor sidik jari selama 3 menit apabila terjadi 5 kali kegagalan autentikasi berturut-turut; serta (5) mekanisme *auto-lock* yang mengunci kembali *solenoid* secara otomatis apabila pintu tidak dibuka dalam 10 detik setelah perintah buka diterima, atau ketika sensor *magnetic switch* mendeteksi pintu telah dirapatkan kembali.

Media komunikasi jarak jauh menggunakan aplikasi Telegram yang dihubungkan melalui Bot API, sejalan dengan penelitian pemanfaatan Telegram Bot pada mikrokontroler NodeMCU ESP8266 yang menunjukkan bahwa mekanisme tersebut efektif digunakan sebagai media notifikasi maupun kendali jarak jauh pada sistem berbasis IoT [20]. Pembuatan bot dilakukan melalui akun @BotFather untuk memperoleh token API, kemudian Chat ID pengguna diperoleh melalui bot @userinfobot. Token dan Chat ID tersebut selanjutnya digunakan pada program agar notifikasi dan perintah kendali hanya dapat diakses oleh pengguna yang telah terdaftar pada *whitelist.json*.

2.4 Alur Kerja Sistem

Alur kerja sistem dirancang untuk menggambarkan proses kerja sistem keamanan kotak persembahan secara keseluruhan, mulai dari autentikasi pengguna hingga sistem memberikan akses dan memantau kondisi pintu, sebagaimana ditunjukkan pada Gambar 5. Alur tersebut menjadi dasar dalam proses implementasi sistem sehingga setiap komponen dapat bekerja sesuai dengan fungsi yang telah dirancang.



Gambar 5. Flowchart Cara Kerja Sistem Keamanan Kotak Persembahan Gereja

Flowchart pada Gambar 5 menjelaskan alur kerja sistem keamanan kotak persembahan gereja berbasis *Internet of Things* (IoT), yang dimulai dengan pemindaian sidik jari menggunakan sensor AS608. Sistem memverifikasi sidik jari untuk menentukan apakah pengguna memiliki akses. Jika sidik jari tidak sesuai, OLED menampilkan status akses ditolak, buzzer berbunyi tiga kali, dan Telegram mengirimkan notifikasi percobaan akses yang ditolak. Apabila terjadi lima kali kegagalan secara berturut-turut, sistem mengaktifkan mode *lockdown* selama tiga menit, menonaktifkan sensor sidik jari sementara, serta membunyikan buzzer secara kontinu dan mengirimkan notifikasi peringatan melalui Telegram. Setelah waktu lockdown berakhir, sistem kembali ke proses pemindaian sidik jari. Sebaliknya, jika sidik jari berhasil diverifikasi, *solenoid door lock* terbuka dan buzzer berbunyi satu kali sebagai tanda akses diterima. OLED menampilkan status akses diterima dan Telegram mengirimkan notifikasi bahwa kotak telah dibuka. Sistem kemudian memantau kondisi pintu; apabila pintu tidak dibuka dalam waktu sepuluh detik, solenoid dikunci kembali. Jika pintu dibuka, sistem menunggu hingga pintu ditutup dan kondisi tersebut terdeteksi oleh *magnetic door switch*. Selanjutnya, solenoid mengunci pintu

secara otomatis dan Telegram mengirimkan notifikasi bahwa kotak telah terkunci kembali. Setelah proses selesai, sistem kembali siap digunakan untuk pemindaian sidik jari berikutnya.

2.5 Batasan Penelitian

Penelitian dibatasi pada: (1) purwarupa kotak persembahan untuk lingkungan gereja dengan fokus pada keamanan akses; (2) autentikasi menggunakan sensor sidik jari AS608; (3) ESP8266 sebagai pengendali dan konektivitas Wi-Fi; (4) Telegram sebagai media notifikasi dan pengendalian; (5) *magnetic door switch* untuk mendeteksi kondisi buka dan tutup pintu; serta (6) pengujian fungsional pada purwarupa sesuai skenario yang telah ditentukan. Penghitungan nominal uang dan sistem akuntansi gereja tidak dibahas.

2.6 Metode Pengujian dan Parameter Evaluasi

Pengujian sistem menggunakan metode *black-box*, yaitu pengujian yang menilai kesesuaian antara masukan dan keluaran sistem tanpa meninjau struktur kode program. Pengujian dilakukan pada enam skenario, yaitu autentikasi sidik jari, notifikasi Telegram, mode *lockdown*, deteksi pembukaan paksa, *Safe Rollback* Wi-Fi, dan simulasi kondisi *offline*. Jumlah pengulangan disesuaikan dengan jenis skenario: autentikasi sidik jari diuji dengan lima percobaan (Tabel 5), notifikasi Telegram pada lima jenis pemicu (Tabel 6), dan simulasi *offline* pada lima kondisi (Tabel 7), sedangkan *lockdown*, deteksi pembukaan paksa, dan *Safe Rollback* dinilai dari kesesuaian perilaku sistem dengan rancangan tanpa merinci jumlah pengulangan. Parameter evaluasi dihitung sebagai berikut. Akurasi keputusan akses = $(\text{jumlah keputusan sesuai} \div \text{jumlah seluruh percobaan}) \times 100\%$, dengan keputusan sesuai berarti akses diterima untuk sidik jari terdaftar dan ditolak untuk sidik jari tidak terdaftar. Tingkat kesalahan penerimaan (*False Acceptance Rate*, FAR) = $(\text{jumlah sidik jari tidak terdaftar yang diterima} \div \text{jumlah percobaan sidik jari tidak terdaftar}) \times 100\%$. Tingkat kesalahan penolakan (*False Rejection Rate*, FRR) = $(\text{jumlah sidik jari terdaftar yang ditolak} \div \text{jumlah percobaan sidik jari terdaftar}) \times 100\%$. Tingkat keberhasilan notifikasi = $(\text{jumlah notifikasi terkirim} \div \text{jumlah pemicu yang diuji}) \times 100\%$. Waktu respons rata-rata = $\text{jumlah waktu respons seluruh percobaan} \div \text{jumlah percobaan}$. Waktu respons autentikasi diukur sejak jari ditempelkan pada sensor hingga keputusan akses tampil pada OLED, dan waktu notifikasi diukur sejak pemicu terjadi hingga pesan terkirim ke Telegram. Penerapan rumus tersebut pada data pengujian disajikan pada Subbab 3.3.

3. HASIL DAN PEMBAHASAN

Bagian ini menguraikan hasil implementasi perangkat keras dan perangkat lunak, hasil pengujian fungsional, serta pembahasan terhadap hasil yang diperoleh.

3.1 Implementasi Perangkat Keras

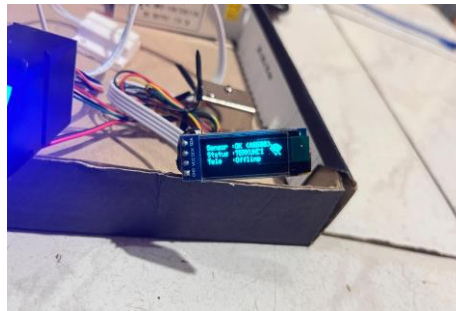
Implementasi perangkat keras menghasilkan sebuah purwarupa kotak persembahan berbentuk kotak persegi panjang berbahan dasar papan multiplek yang dilapisi cat berwarna gelap. Pemilihan bahan multiplek dilakukan dengan mempertimbangkan kemudahan dalam proses pembuatan purwarupa serta bobot perangkat yang relatif ringan sehingga alat dapat dipindahkan dengan mudah. Pada bagian pintu kotak dipasang sensor sidik jari AS608 dan layar OLED 0,91 inci. Sensor sidik jari AS608 digunakan sebagai komponen utama dalam proses autentikasi pengguna sebelum sistem memberikan akses untuk membuka kotak. Sementara itu, layar OLED digunakan untuk memberikan informasi mengenai kondisi sistem kepada pengguna. Informasi yang ditampilkan meliputi status sensor sidik jari, status kunci, serta status koneksi Telegram secara real-time. Pada layar juga ditampilkan ikon kekuatan sinyal Wi-Fi sehingga pengguna dapat mengetahui kondisi konektivitas perangkat secara langsung. Bagian dalam kotak memuat NodeMCU ESP8266 sebagai mikrokontroler utama, modul relay *solenoid*, modul relay buzzer, serta modul power supply 12V. Seluruh komponen tersebut dirangkai dan ditempatkan sedemikian rupa agar tidak mengganggu mekanisme buka-tutup pintu.

Penataan komponen dan kabel menjadi salah satu bagian penting dalam implementasi perangkat keras karena jalur kabel yang tidak tertata dapat mengganggu pergerakan mekanisme solenoid. Oleh karena itu, sambungan kabel menggunakan konektor dan pengikat kabel (*cable tie*) untuk menjaga kestabilan rangkaian selama alat digunakan berulang kali. Bentuk akhir purwarupa sistem keamanan kotak uang ditunjukkan pada Gambar 6.



Gambar 6. Purwarupa Akhir Sistem Keamanan Kotak Persembahan

Pengujian awal terhadap perangkat keras dilakukan dengan memastikan seluruh sensor dan aktuator dapat berfungsi sesuai dengan rancangan. Pengujian dilakukan pada sensor sidik jari, layar OLED, *solenoid door lock*, buzzer, *magnetic door switch*, serta komponen pendukung lainnya. Layar OLED mampu menampilkan tiga baris informasi yang terdiri atas status sensor sidik jari, status kunci, dan status koneksi Telegram. Status kunci yang ditampilkan meliputi kondisi TERKUNCI, TERBUKA, ALARM AKTIF, dan LOCKDOWN. Selain informasi tersebut, ikon kekuatan sinyal Wi-Fi ditampilkan pada pojok kanan layar. Kondisi tampilan OLED pada saat sistem berada dalam keadaan siaga dengan status kotak terkunci dan koneksi Wi-Fi belum tersambung ditunjukkan pada Gambar 7.



Gambar 7. Tampilan OLED pada Kondisi Sistem Siaga (Status Terkunci)

Purwarupa kotak persembahan yang dihasilkan memiliki dimensi kurang lebih 20 cm × 15 cm × 25 cm dengan bobot yang relatif ringan karena menggunakan bahan multiplek. Dimensi tersebut memungkinkan seluruh komponen utama ditempatkan di dalam kotak tanpa mengganggu fungsi mekanisme penguncian. Proses pemasangan sensor sidik jari dan layar OLED pada bagian pintu dilakukan dengan melubangi papan sesuai dengan ukuran modul. Pemasangan tersebut bertujuan agar permukaan sensor dapat sejajar dengan permukaan pintu sehingga pengguna dapat menempelkan jari dengan nyaman tanpa perlu membuka penutup tambahan. Berdasarkan pengamatan selama pengujian, seluruh sambungan kabel yang menggunakan konektor dan pengikat kabel (*cable tie*) tetap stabil selama alat dioperasikan berulang kali. Hal tersebut menunjukkan bahwa pemasangan komponen telah mampu mendukung pengoperasian purwarupa. Meskipun demikian, kerapian jalur kabel di dalam kotak masih perlu diperhatikan agar tidak mengganggu pergerakan mekanisme solenoid ketika pintu dibuka maupun ditutup.

3.2 Implementasi Perangkat Lunak

Firmware diunggah ke NodeMCU ESP8266 melalui Arduino IDE (board NodeMCU 1.0 ESP-12E, flash 4 MB, CPU 80 MHz, kecepatan unggah 115200 baud) dan mengatur seluruh proses kerja sistem, mulai dari pembacaan sensor sidik jari dan sensor pintu, pengendalian *solenoid* dan buzzer, pembaruan OLED, hingga komunikasi dengan Telegram. Bot Telegram yang dibuat melalui @BotFather dilengkapi menu interaktif, seperti “Buka Brankas”, “Kunci Brankas”, “Daftar Jari”, “Status”, dan “Log”, serta perintah langsung seperti `/setwifi`, sehingga pengguna dapat memantau dan mengendalikan sistem tanpa berinteraksi langsung dengan perangkat. Penamaan “brankas” pada berkas program, menu, dan label notifikasi merupakan penamaan bawaan *firmware* yang merujuk pada kotak persembahan. Fungsi-fungsi utama program ditunjukkan pada Tabel 4.

Tabel 4. Fungsi Utama pada Program `iot_brankas.ino`

No	Fungsi	Deskripsi
1	<code>setup()</code>	Inisialisasi hardware, OLED, sensor AS608, LittleFS, dan koneksi Wi-Fi awal
2	<code>loop()</code>	Proses non-blocking pembacaan sensor pintu, sensor jari, timer lockdown, dan polling Telegram
3	<code>connectWiFi() / testAndApplyNewWiFi()</code>	Mengelola koneksi Wi-Fi aktif serta pengujian dan Safe Rollback jaringan baru
4	<code>requestUnlock() / triggerUnlockSequence()</code>	Mengaktifkan relay solenoid secara instan saat autentikasi valid
5	<code>checkFingerprint()</code>	Membaca dan mencocokkan data sidik jari dari sensor AS608
6	<code>processTelegramCommand()</code>	Mengelola seluruh perintah yang diterima melalui Telegram
7	<code>updateMainOLEDDashboard()</code>	Memperbarui tampilan status pada layar OLED
8	<code>loadConfig() / saveConfig() / addAuditLog()</code>	Membaca-menulis konfigurasi dan mencatat log audit aktivitas

3.3 Hasil Pengujian Sistem

Pengujian sistem dilakukan menggunakan metode pengujian black-box (*black-box testing*), yaitu pengujian yang berfokus pada kesesuaian antara input yang diberikan dan output yang dihasilkan sistem tanpa meninjau struktur kode program secara internal. Jumlah percobaan dan parameter evaluasi mengikuti Subbab 2.6, sebagai data awal untuk menilai kinerja purwarupa. Pengujian autentikasi sidik jari dilakukan dengan menempelkan jari yang telah terdaftar maupun yang belum

terdaftar pada sensor AS608. Hasil pengujian ditunjukkan pada Tabel 5. Berdasarkan hasil pengujian, dari 3 percobaan menggunakan sidik jari yang telah terdaftar, seluruh percobaan berhasil memberikan akses dengan tingkat keberhasilan 100%. Sementara itu, 2 percobaan menggunakan sidik jari yang tidak terdaftar seluruhnya berhasil ditolak oleh sistem. Dengan rumus pada Subbab 2.6, akurasi keputusan akses = $(5 \div 5) \times 100\% = 100\%$, FAR = $(0 \div 2) \times 100\% = 0\%$, FRR = $(0 \div 3) \times 100\% = 0\%$, dan waktu respons autentikasi rata-rata = $(0,9 + 1,0 + 1,1 + 0,8 + 1,0) \div 5 = 4,8 \div 5 = 0,96$ detik.

Tabel 5. Hasil Pengujian Autentikasi Sidik Jari

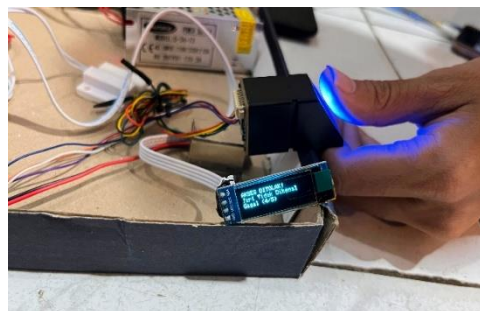
Percobaan ke-	Status Jari	Hasil Sistem	Waktu Respons (detik)
1	Terdaftar	Akses Diterima	0,9
2	Terdaftar	Akses Diterima	1,0
3	Tidak Terdaftar	Akses Ditolak	1,1
4	Tidak Terdaftar	Akses Ditolak	0,8
5	Terdaftar	Akses Diterima	1,0

Gambar 8 menunjukkan kondisi ketika sidik jari pengguna berhasil dikenali oleh sensor AS608. Setelah proses autentikasi berhasil, sistem memberikan akses dengan mengaktifkan mekanisme pembukaan kunci dan menampilkan informasi status pada OLED. Sistem juga memberikan notifikasi melalui Telegram sebagai informasi bahwa autentikasi berhasil dilakukan.



Gambar 8. Tampilan OLED Saat Autentikasi Sidik Jari Berhasil

Gambar 9 menunjukkan kondisi ketika sidik jari yang digunakan tidak sesuai dengan data sidik jari yang telah terdaftar. Sistem menolak akses sehingga mekanisme pengunci tetap dalam kondisi terkunci. Informasi mengenai kegagalan autentikasi juga ditampilkan pada sistem dan dapat diteruskan melalui Telegram sebagai pemberitahuan kepada pengguna.



Gambar 9. Tampilan OLED Saat Autentikasi Sidik Jari Tidak Berhasil

Pengujian berikutnya dilakukan terhadap fitur notifikasi Telegram. Pengujian dilakukan dengan mengamati apakah aktivitas yang terjadi pada kotak persembahan dapat dikirimkan ke akun Telegram pengguna yang telah terdaftar. Aktivitas yang diuji meliputi pembukaan kunci, penguncian kembali, percobaan akses yang gagal, peringatan lockdown, dan peringatan pembukaan paksa. Hasil pengujian menunjukkan bahwa seluruh notifikasi berhasil terkirim dengan tingkat keberhasilan 100%. Waktu pengiriman pesan berada pada kisaran 0,9 hingga 1,3 detik. Hasil pengujian dapat dilihat pada Tabel 6.

Tabel 6. Hasil Pengujian Notifikasi Telegram

No	Jenis Notifikasi	Terkirim	Waktu Kirim (detik)
1	Brankas Dibuka	Berhasil	1,2
2	Brankas Terkunci Kembali	Berhasil	1,1
3	Percobaan Akses Ditolak	Berhasil	1,3
4	Peringatan Lockdown	Berhasil	1,0
5	Peringatan Pembukaan Paksa	Berhasil	0,9



Format pesan multi-line dapat ditampilkan dengan rapi tanpa karakter escape yang tidak diinginkan. Hasil tersebut menunjukkan bahwa komunikasi antara NodeMCU ESP8266 dengan layanan Telegram dapat berjalan sesuai dengan rancangan.

Pengujian mode lockdown dilakukan dengan menempelkan sidik jari yang tidak dikenali secara berturut-turut. Hasil pengujian menunjukkan bahwa sistem secara konsisten mengaktifkan mode *lockdown* selama 3 menit setelah kegagalan autentikasi kelima, ditandai dengan nonaktifnya sensor sidik jari, bunyi buzzer kontinu, serta notifikasi darurat yang dikirimkan ke Telegram. Selama mode *lockdown* berlangsung, sistem tidak menerima input sidik jari apa pun hingga waktu tunggu berakhir, mekanisme ini digunakan untuk membatasi percobaan autentikasi berulang menggunakan sidik jari yang tidak terdaftar.

Pengujian deteksi pembukaan paksa dilakukan dengan membuka pintu kotak secara paksa tanpa melalui proses autentikasi sidik jari maupun perintah Telegram. Sensor *magnetic door switch* berhasil mendeteksi perubahan posisi pintu dan sistem secara otomatis mengaktifkan alarm buzzer secara kontinu disertai pengiriman notifikasi darurat ke Telegram.

Pengujian fitur *Safe Rollback* pada pengaturan Wi-Fi juga dilakukan dengan mengirimkan perintah `/setwifi` menggunakan kredensial yang salah. Hasil pengujian menunjukkan bahwa sistem secara otomatis kembali terhubung ke jaringan Wi-Fi sebelumnya setelah 15 detik pengujian gagal, mekanisme tersebut mencegah perangkat tetap berada pada konfigurasi jaringan yang tidak dapat digunakan. Fitur *Safe Rollback* merupakan fitur pendukung pada sistem IoT yang membantu menjaga konektivitas perangkat ketika terjadi kesalahan konfigurasi jaringan.

Secara keseluruhan, pengujian autentikasi menghasilkan akurasi keputusan akses 100% (FAR 0% dan FRR 0%) dengan waktu respons rata-rata 0,96 detik. Tingkat keberhasilan notifikasi Telegram = $(5 \div 5) \times 100\% = 100\%$, dan waktu kirim rata-rata = $(1,2 + 1,1 + 1,3 + 1,0 + 0,9) \div 5 = 5,5 \div 5 = 1,10$ detik, dengan kisaran 0,9–1,3 detik. Karena belum ada pengujian pembandingan tanpa mekanisme *hardware-first*, pengaruhnya terhadap waktu respons belum dapat dipisahkan secara kuantitatif.

Selain pengujian pada fitur keamanan utama, dilakukan pula pengujian terhadap fitur simulasi mode offline yang disediakan melalui menu Telegram “Test Offline”. Fitur ini memungkinkan pengguna menguji perilaku sistem ketika koneksi Wi-Fi diputus secara sengaja selama durasi tertentu, yaitu 1, 3, atau 5 menit, maupun secara kontinu hingga perangkat di-reset. Hasil pengujian ditunjukkan pada Tabel 7.

Tabel 7. Hasil Pengujian Mode Simulasi Offline

No	Skenario Mode Offline	Fungsi Lokal	Hasil
1	Offline 1 menit	Autentikasi sidik jari	Berfungsi normal
2	Offline 3 menit	Buka/kunci solenoid	Berfungsi normal
3	Offline 5 menit	Tampilan OLED	Berfungsi normal
4	Offline Kontinu	Deteksi pintu & alarm	Berfungsi normal
5	Wi-Fi tersambung kembali	Flush antrean Telegram	Tidak ada ghost message

Hasil pengujian menunjukkan bahwa fungsi keamanan lokal, yaitu autentikasi sidik jari, penguncian dan pembukaan *solenoid*, serta tampilan status pada OLED tetap berjalan normal meskipun koneksi Wi-Fi terputus. Setelah koneksi kembali tersambung, sistem melakukan flush terhadap antrean perintah Telegram yang tertunda sehingga tidak muncul pesan atau perintah lama yang tidak sesuai dengan kondisi terbaru sistem.

3.4 Pembahasan

3.4.1 Analisis Autentikasi dan Waktu Respons

Sistem mampu menjalankan autentikasi dengan akurasi 100%: sidik jari terdaftar membuka kunci, sedangkan sidik jari tidak terdaftar ditolak, sesuai dengan konsep keamanan biometrik pada penelitian sebelumnya [14], [7], [8]. Pada modul AS608, pencocokan *template* dilakukan oleh modul sensor, sedangkan ESP8266 menerima hasilnya melalui komunikasi serial dan mengaktifkan relay *solenoid* hanya apabila sidik jari dikenali, sehingga keputusan autentikasi tidak bergantung pada koneksi internet. Mekanisme *hardware-first asynchronous polling* juga memprioritaskan autentikasi dan deteksi pintu ketika sistem berkomunikasi dengan Telegram. Namun, kontribusi mekanisme ini terhadap waktu respons belum dibandingkan dengan konfigurasi tanpa mekanisme tersebut. Meskipun demikian, nilai 100% diperoleh dari percobaan yang terbatas (tiga sidik jari terdaftar dan dua tidak terdaftar) sehingga belum dapat digeneralisasi dan perlu diuji dengan lebih banyak pengguna, percobaan, serta variasi kondisi jari. Waktu respons autentikasi 0,8 hingga 1,1 detik dan notifikasi Telegram 0,9 hingga 1,3 detik; selisih yang kecil ini kemungkinan dipengaruhi kondisi jaringan serta komunikasi terenkripsi (TLS/SSL). Sebagai gambaran, penelitian kunci pintu berbasis ESP32 melaporkan notifikasi Telegram sekitar 2,3 detik untuk sidik jari tidak cocok dan 3,7 detik untuk pembukaan paksa [12], sedangkan sistem keamanan kendaraan berbasis ESP32 melaporkan rata-rata pengenalan sidik jari 1,8 detik [18]. Waktu purwarupa ini lebih singkat, tetapi perbandingan tersebut hanya indikatif karena perbedaan perangkat keras, jaringan, dan metode pengukuran.

3.4.2 Analisis Ketahanan terhadap Gangguan Koneksi dan Percobaan Akses Tidak Sah

Pada mode *offline*, autentikasi sidik jari, pengendalian *solenoid*, tampilan OLED, serta deteksi pintu dan alarm tetap berjalan tanpa koneksi Wi-Fi karena fungsi pengamanan fisik berada pada perangkat lokal, sedangkan internet digunakan terutama untuk komunikasi dan kendali melalui Telegram. Mode *lockdown* menonaktifkan sensor selama 3 menit setelah



lima kegagalan berturut-turut dengan buzzer dan notifikasi Telegram aktif, sedangkan *magnetic door switch* mendeteksi pembukaan paksa tanpa autentikasi dan memicu buzzer serta Telegram, sejalan dengan penggunaan *sensor magnetic* pada sistem deteksi pencurian [21]. Fitur *Safe Rollback* menguji konfigurasi Wi-Fi baru selama 15 detik dan kembali ke jaringan sebelumnya apabila koneksi gagal, sehingga perangkat tidak kehilangan konektivitas akibat kesalahan konfigurasi.

3.4.3 Peran Telegram dan Perbandingan dengan Penelitian Terkait

Telegram tidak hanya menjadi media pemberitahuan atas pembukaan, penguncian kembali, akses ditolak, *lockdown*, dan pembukaan paksa, tetapi juga media kendali sehingga menjadi bagian dari sistem IoT yang menghubungkan perangkat keamanan dengan pengguna. Pendekatan serupa telah diterapkan pada kunci pintu berbasis ESP32 dan *fingerprint* [12], kotak amal berbasis ESP32 [13], dan sistem berbasis NodeMCU [20]; penelitian kotak amal sebelumnya juga memanfaatkan teknologi komunikasi untuk memberi informasi keamanan kepada pengelola [1] serta menggabungkan *fingerprint* dengan Telegram untuk meningkatkan pemantauan [3]. Dibandingkan dengan penelitian pada Tabel 1, sistem ini diarahkan pada kotak persembahan gereja dan menambahkan deteksi pembukaan paksa, *lockdown* setelah lima kegagalan berturut-turut, serta pengujian fungsi keamanan lokal saat Wi-Fi terputus. Perbandingan ini bersifat kualitatif karena perbedaan objek, komponen, dan skenario pengujian belum memungkinkan perbandingan kuantitatif secara langsung.

3.4.4 Implementasi Metode R&D dan Keterbatasan Penelitian

Penerapan R&D mengikuti tahapan pada Subbab 2.1 hingga uji coba pemakaian: masalah diidentifikasi dari keterbatasan kunci konvensional, data dikumpulkan melalui studi literatur, rancangan perangkat keras dan perangkat lunak divalidasi melalui pemeriksaan kesesuaian terhadap kebutuhan sistem lalu direalisasikan menjadi purwarupa (Subbab 3.1 dan 3.2). Uji coba produk dilaksanakan sebagai pengujian fungsional *black-box* (Subbab 3.3), sedangkan uji coba pemakaian dilakukan melalui simulasi penggunaan, bukan pada operasional gereja yang sebenarnya. Artikel ini belum menyajikan data validasi dari ahli, rincian revisi desain dan produk, maupun hasil uji coba oleh pengguna sebenarnya, sehingga hal tersebut menjadi keterbatasan. Tahap produksi massal tidak dilaksanakan sehingga hasil penelitian masih berupa purwarupa yang diuji melalui skenario simulasi. Keterbatasan lainnya adalah jumlah pengulangan pengujian *lockdown*, deteksi pembukaan paksa, dan *Safe Rollback* yang tidak dirinci, bahan multiplek yang belum ditujukan untuk penggunaan jangka panjang, belum adanya kamera sebagai bukti visual, serta kapasitas sidik jari yang bergantung pada memori internal AS608.

4. KESIMPULAN

Penelitian ini telah menghasilkan purwarupa sistem keamanan kotak persembahan gereja berbasis *Internet of Things* yang mengintegrasikan sensor sidik jari AS608, NodeMCU ESP8266, *solenoid door lock*, *magnetic door switch*, OLED, buzzer, dan Telegram, sehingga rumusan masalah mengenai perancangan sistem yang mampu mengautentikasi pengguna, mengendalikan akses kunci, mendeteksi kondisi pintu, dan menyampaikan informasi keamanan secara *real-time* terjawab. Terkait kinerja fungsionalnya, pada pengujian *black-box* seluruh lima percobaan autentikasi menghasilkan keputusan yang sesuai (akurasi 100%, FAR dan FRR 0% pada jumlah percobaan yang terbatas) dengan waktu respons rata-rata 0,96 detik, dan seluruh lima jenis notifikasi Telegram berhasil terkirim dalam 0,9 hingga 1,3 detik. Mekanisme *lockdown* selama 3 menit setelah lima kali kegagalan autentikasi berturut-turut, deteksi pembukaan paksa menggunakan *magnetic door switch*, serta fungsi keamanan lokal saat koneksi Wi-Fi terputus juga bekerja sesuai rancangan. Kebaruan penelitian ini terletak pada integrasi fitur-fitur tersebut dalam satu purwarupa untuk kotak persembahan gereja dengan *firmware non-blocking* yang memprioritaskan proses lokal (*hardware-first*), dan kontribusinya berupa rancangan purwarupa, arsitektur *firmware* tersebut, serta data pengujian fungsional yang dapat menjadi acuan penelitian serupa. Keterbatasan penelitian ini adalah jumlah percobaan yang sedikit dan tidak dirincinya pengulangan pengujian *lockdown*, deteksi pembukaan paksa, dan *Safe Rollback*, belum adanya pembandingan untuk menilai pengaruh *hardware-first* terhadap waktu respons, belum adanya modul kamera, kapasitas sidik jari yang bergantung pada memori AS608, serta material multiplek. Penelitian selanjutnya dapat menambahkan modul kamera, baterai cadangan, *dashboard* berbasis perangkat seluler, material kotak yang lebih kuat seperti logam atau akrilik tebal, serta pengujian dengan jumlah pengguna dan percobaan yang lebih banyak.

5. PERNYATAAN PENULIS

5.1 Kontribusi Penulis

Konseptualisasi: K. Y. Y., A. F., dan K.;
 Metodologi: K. Y. Y., A. F., dan K.;
 Perangkat Lunak: K. Y. Y., A. F., dan K.;
 Validasi: K. Y. Y., A. F., dan K.;
 Analisis Formal: K. Y. Y., A. F., dan K.;





Investigasi: K. Y. Y., A. F., dan K.;

Sumber Daya: K. Y. Y., A. F., dan K.;

Kurasi Data: K. Y. Y., A. F., dan K.;

Penulisan Draf Awal: K. Y. Y., A. F., dan K.;

Penulisan, Peninjauan, dan Penyuntingan: K. Y. Y., A. F., dan K.;

Visualisasi: K. Y. Y., A. F., dan K.;

Seluruh penulis telah membaca dan menyetujui versi manuskrip yang telah diterbitkan.

5.2 Ketersediaan Data

Data yang digunakan dalam penelitian ini diperoleh dari hasil observasi, implementasi, dan pengujian sistem keamanan kotak persembahan gereja berbasis IoT yang dikembangkan oleh penulis. Data penelitian meliputi hasil pengujian autentikasi sidik jari, kondisi buka dan tutup kotak, respons kunci *solenoid*, buzzer, tampilan OLED, serta pengiriman notifikasi dan kendali melalui Telegram. Data hasil pengujian digunakan untuk menganalisis kinerja dan keberhasilan fungsi sistem. Data penelitian tersedia pada penulis dan dapat diberikan untuk keperluan verifikasi penelitian sesuai dengan kebijakan yang berlaku.

5.3 Pendanaan

Penelitian dan penulisan manuskrip ini didanai secara mandiri oleh penulis. Tidak terdapat sumber pendanaan dari lembaga pemerintah, institusi, perusahaan, maupun pihak eksternal lainnya.

5.4 Pernyataan Dewan Peninjau Institusional

Tidak Berlaku (*Not applicable*). Penelitian ini tidak melibatkan intervensi terhadap manusia, hewan, maupun data pribadi yang memerlukan persetujuan dari Dewan Peninjau Institusional (*Institutional Review Board*).

5.5 Pernyataan Persetujuan Berdasarkan Informasi

Tidak Berlaku (*Not applicable*). Penelitian ini berfokus pada perancangan, pengembangan, dan pengujian prototipe sistem keamanan kotak persembahan berbasis IoT dan tidak melibatkan penelitian terhadap subjek manusia sebagai objek penelitian.

5.6 Pernyataan Konflik Kepentingan

Para penulis menyatakan bahwa mereka tidak memiliki kepentingan keuangan yang bersaing atau hubungan pribadi yang diketahui yang dapat dianggap memengaruhi pekerjaan yang dilaporkan dalam artikel ini.

5.7 Penggunaan AI Generatif dan Teknologi Berbantuan AI dalam Proses Penulisan

Para penulis menggunakan AI Generatif untuk membantu meningkatkan kejelasan dan kualitas penulisan dalam artikel ini. Para penulis telah meninjau, memverifikasi, dan menyunting konten yang dihasilkan dengan bantuan AI serta bertanggung jawab penuh atas isi dan versi akhir publikasi.

REFERENCES

- [1] A. Rahman, M. Hanafi, R. Aswar, and I. A. Saputro, "Sistem keamanan kotak amal masjid berbasis wireless sensor network dan SMS gateway," in *Seminar Nasional Amikom Surakarta (SEMNASA)*, Sukoharjo, Indonesia, Nov. 2024. [Online]. Available: <https://ojs.amikomsolo.ac.id/index.php/semnasa/issue/view/2>.
- [2] A. Annabawi and F. H. S. Pratama, "Rancang bangun sistem keamanan pada kotak penyimpanan uang (Moneybox Plus) berbasis mikrokontroler Arduino," *Inf. Technol. J.*, vol. 10, no. 1, pp. 59–68, 2024, doi: 10.30742/melekitjournal.v10i1.293.
- [3] D. Hermawan, J. Jufrizel, A. Ullah, and A. Faizal, "Rancang bangun sistem keamanan kotak amal dengan akses fingerprint menggunakan ESP32-Cam dan Telegram berbasis IoT," *J. Media Inform. Budidarma*, vol. 7, no. 3, pp. 1013–1021, 2023, doi: 10.30865/mib.v7i3.6252.
- [4] A. Y. Chanifudin, S. D. Ayuni, A. H. Falah, and I. Sulistiyowati, "Automatic safe security system using pin code and fingerprint based on microcontroller with Telegram notification," *J. Electr. Eng. Comput. (JEECOM)*, vol. 7, no. 2, pp. 312–320, 2025, doi: 10.33650/jeeecom.v7i2.11972.
- [5] A. B. Sinabang, Martias, and H. Adiarto, "Alat pengaman brankas berbasis fingerprint menggunakan NodeMCU ESP8266 notifikasi Telegram," *INSANtek*, vol. 4, no. 1, pp. 18–24, 2023, doi: 10.31294/insantek.v4i1.2121.
- [6] S. Z. Amalia, "Prototype sistem pengaman dan pelacak brankas menggunakan fingerprint dan GPS berbasis Internet of Things," Skripsi, Universitas Islam Sultan Agung, Semarang, Indonesia, 2023. [Online]. Available: <https://repository.unissula.ac.id/id/eprint/33009>.
- [7] H. I. Ramadhan and R. Supriyanto, "Prototype sistem keamanan brankas berbasis sensor sidik jari," *J. Ilm. Komputasi*, vol. 23, no. 1, pp. 131–138, 2024, doi: 10.32409/jikstik.23.1.3519.
- [8] F. E. Safitri and T. Ta'ali, "Rancang bangun pengaman pintu otomatis menggunakan sidik jari (fingerprint) dan password berbasis Arduino," *J. Tek. Elektro Indones. (JTEIN)*, vol. 3, no. 2, pp. 425–436, 2022, doi: 10.24036/jtein.v3i2.269.
- [9] G. M. Kadena, K. A. Yasa, and I. G. S. Widharma, "Rancang bangun sistem pengaman pintu brankas menggunakan fingerprint dan keypad berbasis Arduino," Tugas Akhir, Politeknik Negeri Bali, Indonesia, 2023. [Online]. Available: https://repository.pnb.ac.id/id/eprint/10404/1/RAMA_36304_1815344054_full.pdf.





- [10] I. U. V. Simanjuntak and L. B. P. Asmara, "Rancang bangun sistem keamanan sepeda motor menggunakan fingerprint dan GPS tracker berbasis IoT," *Techné J. Ilm. Elektroteknika*, vol. 21, no. 1, pp. 31–44, 2022, doi: 10.31358/techne.v21i1.305.
- [11] N. R. Maulana and R. Djutalov, "Implementasi metode SDLC untuk pembuatan sistem penguncian pintu menggunakan fingerprint dengan modul NodeMCU ESP8266 berbasis Internet of Things," *LOGIC J. Ilmu Komput. Pendidik.*, vol. 1, no. 1, pp. 40–49, 2022. [Online]. Available: <https://journal.mediapublikasi.id/index.php/logic/article/download/1312/663>.
- [12] A. Ardiansah, M. Nuraeni, Ridwang, and Adriani, "Rancang bangun akses kunci pintu otomatis menggunakan fingerprint berbasis Internet of Things (IoT)," *Vertex Elektro*, vol. 16, no. 2, pp. 31–39, Aug. 2024, doi: 10.26618/jte.v16i2.15704.
- [13] N. A. Zuhriyah and S. Rosyadi, "Smart charity box with ESP32 and chatbot," *J. Robot. Autom. Electron. Eng.*, vol. 2, no. 2, pp. 87–99, Sep. 2024, doi: 10.21831/jraee.v2i2.613.
- [14] A. A. Mahligai, N. Iksan, P. Gunoto, and I. Y. Panessai, "Perancangan sistem keamanan brankas dengan verifikasi password dan sidik jari berbasis IoT," *Sigma Teknika*, vol. 5, no. 1, pp. 100–107, Jun. 2022, doi: 10.33373/sigmateknika.v5i1.4141.
- [15] W. A. S. Lestari and T. Z. Vitadiar, "Sistem keamanan pintu pagar menggunakan fingerprint dan alarm sebagai pengaman dengan notifikasi Telegram berbasis Internet of Things (IoT)," *Inovate J. Ilm. Inov. Teknol. Inf.*, vol. 8, no. 2, pp. 92–101, 2024, doi: 10.33752/inovate.v8i2.6165.
- [16] A. Z. Nusri and A. Alimuddin, "Rancang bangun security door lock menggunakan fingerprint berbasis mikrokontroler," *J. Ilm. Sist. Inf. Tek. Inform. (JISTI)*, vol. 5, no. 1, pp. 23–28, 2022, doi: 10.57093/jisti.v5i1.105.
- [17] Koesmariyanto, N. Hidayati, D. D. Cahyani, and N. B. Anto, "Smart locker menggunakan fingerprint dan face recognition sebagai sistem keamanan loker penyimpanan," *J. Appl. Smart Electr. Netw. Syst. (JASENS)*, vol. 4, no. 2, pp. 68–76, 2023, doi: 10.52158/jasens.v4i2.834.
- [18] M. T. A. Farisi, F. N. Azis, A. M. Fernanda, and P. Pramono, "Rancang bangun sistem keamanan kendaraan 2WD berbasis ESP32 dengan autentikasi sidik jari dan pelacakan lokasi melalui Telegram," in *Prosiding Seminar Nasional Teknologi Informasi dan Bisnis (SENATIB)*, 2025, pp. 1034–1042, doi: 10.47701/gvp1gq02.
- [19] Sugiyono, *Metode Penelitian Kuantitatif, Kualitatif, dan R&D*, 2nd ed., 5th printing. Bandung, Indonesia: Alfabeta, 2023, ISBN: 978-602-289-533-6.
- [20] M. Safii *et al.*, "Monitoring ketinggian permukaan air menggunakan Telegram bot berbasis NodeMCU ESP8266," *METIK J.*, vol. 6, no. 2, pp. 123–132, 2022, doi: 10.47002/METIK.V6I2.384.
- [21] A. Syahri and M. Basri, "Perancangan sistem keamanan untuk deteksi pencurian menggunakan sensor magnetic dan RFID berbasis Internet of Things," *Hello World J. Ilmu Komput.*, vol. 4, no. 3, pp. 163–170, 2025, doi: 10.56211/helloworld.v4i3.1166.