Integrative Perspectives of Social and Science Journal (IPSSJ)
ipssj.com ippsj2024@gmail.com E-ISSN: 3064-4011

Rancang Bangun Sistem Keamanan Akses Data Center Berbasis Internet of Things (IoT) Menggunakan Biometric Fingerprint Authentication dengan Monitoring dan Notifikasi Real-Time (Studi Kasus: Data Center PT XYZ)

Ferdynan Janika Jayapertela[1*], Bambang Irawan[2]
[1] Program Studi Teknik Informatika, Fakultas Ilmu Komputer, Universitas Esa Unggul
[2] Program Studi Teknik Informatika, Fakultas Ilmu Komputer, Universitas Esa Unggul
*Corresponding Email: [1] ferdyanjanika@gmail.com, [2] bambangirawan@gmail.com

Abstrak
PT XYZ menyimpan data produksi, transaksi, dan sertifikasi produk yang bersifat rahasia pada *Data Center*-nya, sementara sistem keamanan akses fisik ruang tersebut masih mengandalkan kunci mekanik, kartu akses, dan kata sandi yang rentan digandakan, dipinjamkan, atau diretas, sehingga identitas pengguna yang mengakses ruangan tidak dapat dipastikan secara akurat. Kondisi ini menuntut mekanisme otentikasi yang lebih andal serta kemampuan pengawasan yang responsif terhadap upaya akses tidak sah. Penelitian ini bertujuan merancang dan membangun purwarupa sistem keamanan akses *Data Center* berbasis *Internet of Things (IoT)* yang menggunakan otentikasi biometrik sidik jari, dilengkapi mekanisme *monitoring* status akses secara *Real-Time* dan notifikasi otomatis melalui Telegram *Bot API*. Penelitian menggunakan pendekatan *Research and Development* dengan model pengembangan *Prototyping*, memanfaatkan mikrokontroler *NodeMCU V3* (ESP8266), sensor sidik jari AS608, solenoid *Door Lock*, serta basis data *Real-Time* berbasis *Cloud* (Firebase) untuk pencatatan log akses. Pengujian *Black box* menunjukkan tingkat keberhasilan 100% pada 12 skenario pengujian. Pengujian akurasi otentikasi sebanyak 40 kali percobaan menghasilkan *False Acceptance Rate (FAR)* sebesar 0,00% dan *False Rejection Rate (FRR)* sebesar 10,00%, dengan rata-rata waktu respons sistem 1,25 detik dan latensi notifikasi Telegram rata-rata 1,81 detik, serta mekanisme *buffering* yang menjaga konsistensi log saat koneksi *Wi-Fi* terputus. Purwarupa ini mampu meningkatkan keandalan pengendalian akses, mempercepat respons terhadap insiden keamanan, serta menghasilkan pencatatan log akses yang terdokumentasi secara otomatis sebagai bahan audit keamanan *Data Center* PT XYZ.
Kata kunci: *Internet of Things, otentikasi biometrik, sidik jari, keamanan akses, monitoring Real-Time, notifikasi Telegram*

Abstract
PT XYZ stores confidential production, transaction, and product certification data in its Data Center, yet the physical access security of the room still relies on mechanical keys, access cards, and passwords that are vulnerable to duplication, lending, or hacking, making it difficult to accurately verify the identity of anyone entering the room. This condition calls for a more reliable authentication mechanism along with responsive monitoring of unauthorized access attempts. This study aims to design and build a prototype of an Internet of Things (IoT)-based Data Center access security system that uses fingerprint biometric authentication, equipped with real-time access status monitoring and automatic notifications via the Telegram Bot API. The study applies a Research and Development approach with a Prototyping development model, utilizing a NodeMCU V3 (ESP8266) microcontroller, an AS608 fingerprint sensor, a solenoid door lock, and a cloud-based real-time database (Firebase) for access log recording. Black-box testing shows a 100% success rate across 12 test scenarios. Authentication accuracy testing over 40 verification attempts yields a False Acceptance Rate (FAR) of 0.00% and a False Rejection Rate (FRR) of 10.00%, with an average system response time of 1.25 seconds and an average Telegram notification latency of 1.81 seconds, while the buffering mechanism preserves log consistency during Wi-Fi outages. The prototype improves access control reliability, accelerates response to security incidents, and automatically produces documented access logs to support security audits at the PT XYZ Data Center.
Keywords: *Internet of Things, biometric Authentication, fingerprint, access security, Real-Time monitoring, Telegram notification*

PENDAHULUAN

PT XYZ memiliki Data Center yang menyimpan data produksi, transaksi, mutu produk, hingga data administrasi yang bersifat rahasia dan sensitif, sehingga keamanan akses fisik menuju ruangan tersebut menjadi kebutuhan yang tidak dapat ditawar. Sistem keamanan akses konvensional yang digunakan saat ini, yaitu kunci mekanik, kartu akses, dan kata sandi,

memiliki kelemahan mendasar karena mengandalkan kepemilikan (something you have) maupun pengetahuan (something you know), yang keduanya rentan digandakan, dipinjamkan, atau diretas sehingga identitas pengguna yang mengakses ruangan tidak dapat dipastikan secara akurat (Ragothaman dkk., 2023).

Teknologi biometrik menjadi solusi otentikasi yang semakin banyak diadopsi karena karakteristiknya yang unik dan melekat pada individu (something you are) (Yang dkk., 2021). Sidik jari merupakan salah satu modalitas biometrik yang paling banyak diintegrasikan pada perangkat IoT berdaya rendah karena kebutuhan komputasi yang ringan dan biaya modul yang terjangkau, dengan waktu pengenalan yang hanya membutuhkan sekitar satu detik dan waktu buka pintu sekitar lima detik pada purwarupa sejenis (Alsayaydeh dkk., 2025). Mikrokontroler berbasis modul Wi-Fi keluaran Espressif Systems, seperti ESP8266, menjadi komponen kunci dalam arsitektur IoT karena konektivitas Wi-Fi terintegrasi serta dukungan antarmuka periferal (SPI, I2C, UART, PWM) (Hercog dkk., 2023), dengan arsitektur yang umumnya dibangun atas lapisan persepsi, lapisan jaringan, dan lapisan aplikasi (Shaheen dkk., 2024).

Beberapa penelitian terdahulu telah membuktikan efektivitas integrasi sensor sidik jari dengan platform IoT untuk berbagai kebutuhan pengamanan ruangan, di antaranya sistem keamanan pintu berbasis fingerprint dan IoT yang statusnya dapat dipantau secara daring (Fauziman & Mukhaiyar, 2023), sistem kunci pintu pintar berbasis ESP32 dengan sidik jari, keypad, dan Firebase yang mencapai keberhasilan pengujian Black box 100% (Permana dkk., 2024), basis data real-time berbasis Cloud yang mampu menyinkronkan data antar perangkat IoT dengan latensi rendah (Efendi dkk., 2025; Sung dkk., 2023), integrasi biometrik dan IoT pada pintu otomatis menggunakan face recognition (Zulfikar dkk., 2023), serta pemanfaatan sensor fingerprint pada pengamanan area parkir (Pahrudin, 2021) dan brankas penyimpanan barang berharga (Indra & Supriyanto, 2024). Penelitian-penelitian tersebut umumnya masih berfokus pada pengamanan rumah tinggal, gudang, brankas, maupun kendaraan parkir, dan baru mengimplementasikan salah satu aspek saja (otentikasi biometrik atau notifikasi real-time), sehingga penelitian yang secara spesifik mengintegrasikan otentikasi biometrik, monitoring real-time, dan notifikasi otomatis pada konteks pengamanan Data Center perusahaan pertambangan masih sangat terbatas.

Aspek notifikasi real-time juga menjadi perhatian penting, sebagaimana ditunjukkan pada perancangan alat kontrol akses pintu berbasis sidik jari yang dilengkapi notifikasi Telegram (Hanafie dkk., 2023; Raditya dkk., 2023). Kesenjangan (research gap) inilah yang menjadi peluang sekaligus kebaruan (novelty) yang coba dijawab melalui penelitian ini, dengan merancang purwarupa sistem yang mengintegrasikan ketiga aspek tersebut secara menyeluruh dengan mengambil studi kasus nyata pada Data Center PT XYZ, mengacu pada model kontrol akses adaptif dan berlapis yang semakin dibutuhkan seiring meningkatnya heterogenitas perangkat IoT (Ahsan & Pathan, 2025). Berdasarkan uraian tersebut, penelitian ini merancang dan membangun purwarupa sistem keamanan akses Data Center berbasis IoT dengan otentikasi biometrik sidik jari yang dilengkapi monitoring dan notifikasi real-time.

METODE

Penelitian ini menggunakan pendekatan Research and Development (R&D) dengan metode perancangan sistem tertanam (embedded system design) dan model pengembangan Prototyping, yang meliputi tahapan identifikasi kebutuhan, perancangan cepat (quick design), pembangunan purwarupa, evaluasi oleh pengguna, serta perbaikan purwarupa secara iterati

Tabel 1. Tahapan Penelitian dengan Model Prototyping

No.	Tahapan	Kegiatan
1.	Identifikasi Kebutuhan	Melakukan observasi dan wawancara mengenai sistem akses konvensional yang berjalan di Data Center PT XYZ untuk merumuskan kebutuhan fungsional dan non-fungsional sistem.
2.	Perancangan Cepat (Quick Design)	Merancang arsitektur IoT tiga lapisan, diagram blok, skema rangkaian perangkat keras, flowchart proses verifikasi dan pendaftaran, serta struktur basis data Firebase Realtime Database.
3.	Pembangunan Purwarupa	Mengimplementasikan perangkat keras (NodeMCU V3, sensor fingerprint, solenoid Door Lock, LCD, Buzzer) dan firmware menggunakan Arduino IDE, terintegrasi dengan Firebase dan Telegram Bot API.
4.	Evaluasi Purwarupa	Menguji purwarupa melalui Black Box Testing terhadap fungsi sistem serta pengujian non-fungsional terhadap akurasi otentikasi, waktu respons, dan kecepatan notifikasi.
5.	Perbaikan Sistem	Melakukan perbaikan terhadap purwarupa berdasarkan hasil evaluasi, seperti penyesuaian posisi sensor dan mekanisme Fail-Safe, hingga diperoleh sistem yang sesuai kebutuhan.

Metode Pengumpulan Data

Data diperoleh melalui observasi langsung dan wawancara di lokasi Data Center PT XYZ untuk mengidentifikasi kondisi sistem akses yang berjalan, serta studi pustaka terhadap jurnal dan penelitian terdahulu yang relevan dengan sistem keamanan berbasis biometrik dan IoT.

1.1.1. Observasi dan Wawancara

Observasi dilakukan untuk mengidentifikasi mekanisme akses yang berjalan saat ini, yaitu kombinasi kunci mekanik, kartu akses, dan kata sandi, sekaligus mengidentifikasi kelemahan berupa ketiadaan verifikasi identitas yang melekat pada individu, keterlambatan informasi saat terjadi akses di luar jam pengawasan, serta tidak tersedianya data riwayat akses yang terdokumentasi secara digital. Observasi dan wawancara dilaksanakan pada 6 Oktober 2025 hingga 31 Maret 2026 dengan melibatkan 20 narasumber dari divisi ICT (Information & Communication Technology) dan SSC (Shared Service Center) PT XYZ. Adapun perancangan, pembangunan purwarupa, dan pengujian sistem dilakukan di tempat penelitian mandiri peneliti dalam bentuk purwarupa pintu skala miniatur, karena pertimbangan keamanan operasional perusahaan tidak memungkinkan pemasangan purwarupa secara langsung pada pintu Data Center yang sesungguhnya.

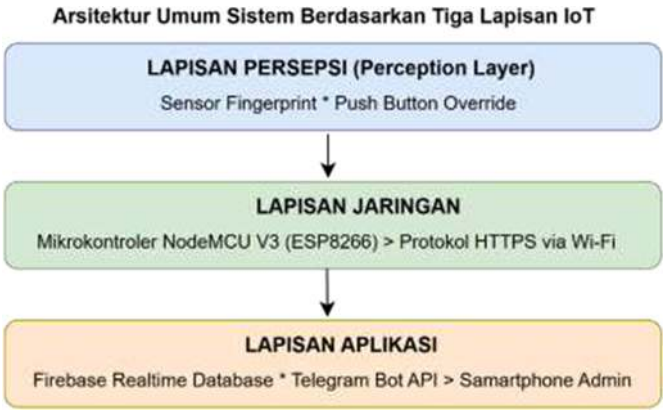
1.1.2. Studi Pustaka

Peneliti mengumpulkan referensi dari jurnal dan penelitian terdahulu yang berkaitan dengan kontrol akses IoT, otentikasi biometrik sidik jari, arsitektur mikrokontroler berbasis Wi-Fi, serta layanan basis data dan notifikasi berbasis Cloud sebagai dasar perancangan sistem.

Perancangan Arsitektur dan Perangkat Sistem

Penelitian ini menggunakan pendekatan Research and Development dengan arsitektur sistem yang mengadopsi konsep arsitektur IoT tiga lapisan sebagaimana dijelaskan oleh Shaheen dkk. (2024), yaitu lapisan persepsi, lapisan jaringan, dan lapisan aplikasi, agar setiap lapisan dapat dirancang dan diuji secara terarah sebelum diintegrasikan menjadi satu kesatuan purwarupa.

Lapisan persepsi pada arsitektur ini terdiri atas sensor fingerprint AS608 dan tombol exit yang bertugas menangkap data masukan. Lapisan jaringan direpresentasikan oleh Mikrokontroler NodeMCU V3 (ESP8266) yang memproses data dan meneruskannya melalui protokol HTTPS. Lapisan aplikasi terdiri atas Firebase Realtime Database sebagai media penyimpanan dan Telegram Bot API sebagai media notifikasi, yang keduanya dapat diakses administrator melalui smartphone tanpa memerlukan aplikasi khusus. Gambaran arsitektur tersebut disajikan pada Gambar 1.



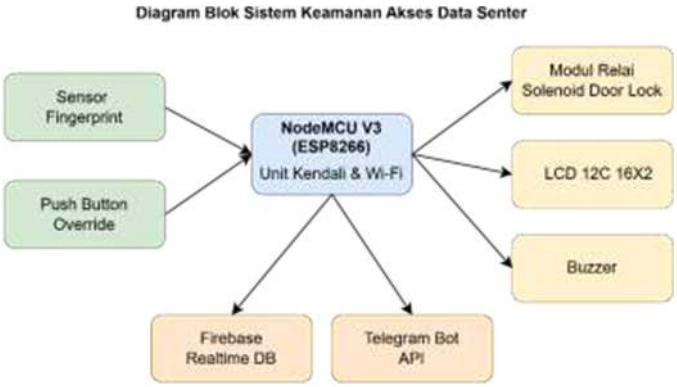
Gambar 1. Arsitektur Umum Sistem Berdasarkan Tiga Lapisan IoT

Perancangan Diagram Blok dan Rangkaian Perangkat Keras

NodeMCU V3 berperan sebagai unit kendali utama yang menghubungkan perangkat input (sensor fingerprint dan tombol exit) dengan perangkat output (modul relai, solenoid Door Lock, LCD, Buzzer), sekaligus menjembatani komunikasi data menuju layanan Cloud, memanfaatkan antarmuka UART, I2C, dan GPIO yang tersedia pada keluarga mikrokontroler berbasis chip Espressif (Hercog dkk., 2023). Pendekatan integrasi fingerprint, mikrokontroler, dan solenoid Door Lock ini merujuk pada konfigurasi yang diterapkan oleh Fauziman dan Mukhaiyar (2023).

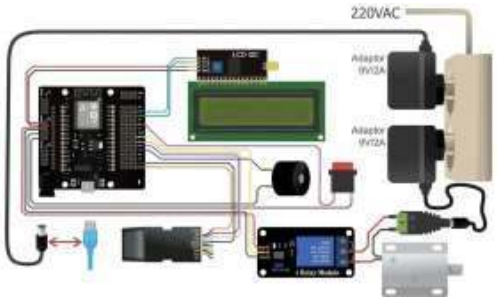
Sensor fingerprint dihubungkan melalui antarmuka SoftwareSerial, LCD melalui antarmuka I2C, sedangkan modul relai/solenoid, Buzzer, dan tombol exit dikendalikan melalui pin digital GPIO biasa, dengan referensi waktu pencatatan akses diperoleh melalui sinkronisasi Network Time Protocol (NTP) tanpa memerlukan modul RTC tambahan.

Diagram blok sistem secara menyeluruh disajikan pada Gambar 2, sedangkan skema rangkaian perangkat keras yang menghubungkan seluruh modul disajikan pada Gambar 3.



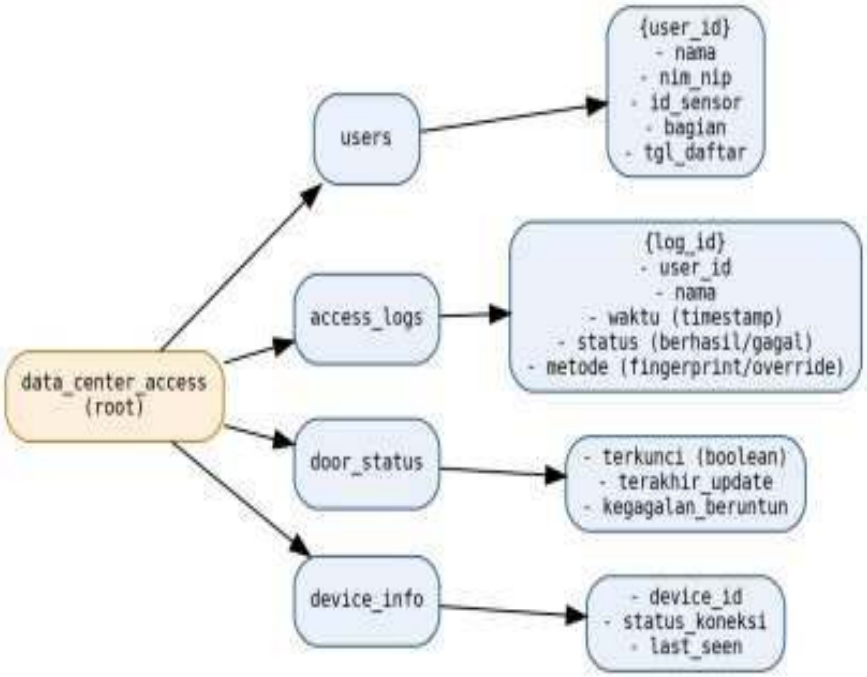
Gambar 2. Diagram Blok Sistem Keamanan Akses *Data Center*

Catu daya utama berupa adaptor 9V/2A digunakan untuk menggerakkan solenoid Door Lock melalui modul relai, sedangkan tegangan 5V hasil step-down mencatu NodeMCU V3, LCD, dan modul relai.



Gambar 3. Skema Rangkaian Perangkat Keras Sistem

Basis data dirancang menggunakan struktur non-relasional berbasis pohon JSON sesuai karakteristik Firebase Realtime Database, yang memungkinkan sinkronisasi data secara instan tanpa proses polling (Efendi dkk., 2025; Sung dkk., 2023). Struktur basis data terdiri atas empat node utama, yaitu users untuk identitas pengguna terdaftar, access_logs untuk riwayat setiap peristiwa akses, door_status untuk kondisi pintu terkini, dan device_info untuk status konektivitas perangkat, sebagaimana disajikan pada Gambar 4 dan Tabel 2.



Gambar 4. Struktur Basis Data *Firebase RealTime Database*

Notifikasi dirancang menggunakan Telegram Bot API dengan mekanisme pengiriman pesan berbasis permintaan HTTPS yang berisi token bot, chat ID administrator, serta isi pesan, mengacu pada pendekatan yang diterapkan oleh Hanafie dkk. (2023) dan Raditya dkk. (2023). Setiap kategori peristiwa (akses berhasil, akses gagal, akses ilegal, dan perangkat offline) dirancang memiliki format pesan berbeda agar administrator dapat langsung mengenali tingkat urgensi tanpa perlu membuka aplikasi monitoring tambahan.

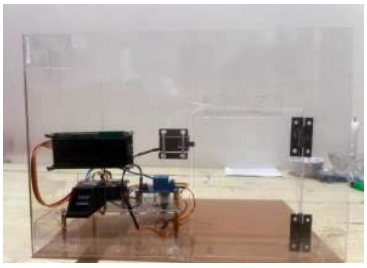
Tabel 2. Rincian Atribut Basis Data Firebase

No.	Node	Atribut	Keterangan
1.	users/{user_id}	nama, nim_nip, id_sensor, bagian, tgl_daftar	Identitas pengguna terdaftar yang terhubung dengan ID slot pada sensor fingerprint.
2.	access_logs/{log_id}	user_id, nama, waktu, status, metode	Riwayat setiap peristiwa akses beserta status berhasil/gagal dan metode akses.
3.	door_status	terkunci, terakhir_update, kegagalan_beruntun	Status kondisi pintu dan penghitung kegagalan beruntun secara real-time.
4.	device_info	device_id, status_koneksi, last_seen	Informasi status konektivitas mikrokontroler ke jaringan dan basis data.

HASIL DAN PEMBAHASAN

Implementasi Perangkat Keras (Hardware)

Purwarupa pintu skala miniatur dibangun mengikuti rancangan arsitektur dan skema rangkaian pada sub-bab 2.3. Komponen elektronik utama (NodeMCU V3, modul relai, Buzzer, adaptor catu daya) ditempatkan dalam panel enclosure berbahan plastik ABS berukuran 20 cm x 15 cm x 8 cm. Sensor fingerprint AS608 dan LCD 16x2 I2C dipasang pada sisi luar pintu, sedangkan tombol Override manual dipasang di bagian dalam panel sebagai mekanisme darurat untuk membuka pintu dari dalam ruangan tanpa proses otentikasi. Foto purwarupa tampak depan dan tampak belakang disajikan pada Gambar 5 dan Gambar 6.



Gambar 5. Foto Purwarupa Tampak Depan

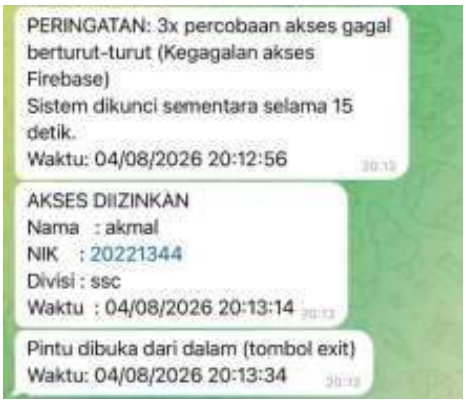
Implementasi Perangkat Lunak (Software) dan Cloud

Firmware purwarupa dikembangkan menggunakan Arduino IDE, dengan konfigurasi pin sensor fingerprint via SoftwareSerial, modul relai, Buzzer, LCD I2C, dan tombol Override. Sinkronisasi waktu dilakukan melalui protokol Network Time Protocol (NTP) dari server NTP publik agar setiap log akses tercatat dengan timestamp yang presisi tanpa modul RTC tambahan. Tata letak pengkabelan dan komponen internal purwarupa disajikan pada Gambar 6.



Gambar 6. Foto Purwarupa Tampak Belakang (Tata Letak Komponen Internal)

Notifikasi ke administrator diimplementasikan melalui Telegram Bot API dengan mendaftarkan bot melalui BotFather, memperoleh token Bot HTTPS API, serta menetapkan Chat ID administrator tempat pesan peringatan dan laporan akses dikirimkan. Contoh notifikasi yang diterima administrator disajikan pada Gambar 7.



Gambar 7. Screenshot Notifikasi Telegram

Sistem turut dilengkapi mekanisme buffering yang menyimpan data log sementara secara lokal pada saat koneksi Wi-Fi terputus, kemudian mengunggah seluruh data tertunda ke Firebase begitu koneksi kembali tersambung, sebagaimana dibuktikan pada Gambar 8.



Gambar 8. Bukti Sinkronisasi Ulang Data Firebase Setelah Koneksi Wi-Fi Pulih

Hasil implementasi menunjukkan bahwa seluruh komponen perangkat keras dan perangkat lunak berhasil terintegrasi sesuai rancangan pada Bagian 2, sehingga purwarupa siap dilanjutkan ke tahap pengujian fungsional dan non-fungsional.

Pengujian Sistem

Pengujian fungsional dilakukan menggunakan metode Black Box Testing untuk memastikan setiap fitur berjalan sesuai spesifikasi, mengacu pada pendekatan yang diterapkan Permana dkk. (2024) yang mencapai keberhasilan 100% pada sistem sejenis. Pengujian non-fungsional dilakukan untuk mengukur akurasi otentikasi (FAR dan FRR)

mengacu pada parameter evaluasi biometrik lazim (Ragothaman dkk., 2023), waktu respons sistem, kecepatan notifikasi Telegram, dan konsistensi konektivitas jaringan. Rekapitulasi hasil pengujian fungsional ditunjukkan pada Tabel 3.

Tabel 3. Rekapitulasi Hasil Pengujian Black Box

No.	Kategori Pengujian	Jumlah Skenario	Jumlah Berhasil	Persentase Keberhasilan
1.	Mode Pendaftaran (Enrollment)	3	3	100%
2.	Verifikasi Akses Sah	3	3	100%
3.	Verifikasi Akses Ditolak dan Fail-Safe	3	3	100%
4.	Tombol Override dan Auto-Lock	3	3	100%
5.	Total Keseluruhan Skenario	12	12	100%

Berdasarkan Tabel 3, seluruh 12 skenario pengujian Black Box, meliputi pendaftaran pengguna, verifikasi akses sah, penolakan akses ilegal beserta mekanisme Fail-Safe, hingga tombol Override dan Auto-Lock, dinyatakan berhasil dengan tingkat keberhasilan 100%. Pengujian akurasi otentikasi dilakukan sebanyak 40 kali percobaan verifikasi, terdiri atas 20 percobaan dengan sidik jari tidak terdaftar (FAR) dan 20 percobaan dengan sidik jari terdaftar (FRR), sedangkan pengujian waktu respons dan kecepatan notifikasi masing-masing dilakukan sebanyak 10 kali percobaan. Hasil pengujian non-fungsional terhadap akurasi otentikasi, waktu respons, kecepatan notifikasi, dan konsistensi konektivitas dirangkum pada Tabel 4.

Tabel 4. Rekapitulasi Hasil Pengujian Non-Fungsional

No.	Parameter	Hasil	Keterangan
1.	False Acceptance Rate (FAR)	0,00% (0 dari 20 percobaan)	Tidak ada sidik jari tidak terdaftar yang diterima sistem
2.	False Rejection Rate (FRR)	10,00% (2 dari 20 percobaan)	2 kali penolakan (percobaan ke-6 dan ke-14) akibat posisi jari kurang tepat/miring pada sensor
3.	Rata-rata Waktu Respons	1,25 detik	Diukur dari pemindaian jari hingga solenoid bergerak (10 percobaan)
4.	Rata-rata Latensi Notifikasi Telegram	1,81 detik	Diukur dari peristiwa akses hingga pesan diterima (10 percobaan)
5.	Konsistensi Konektivitas dan Buffering	Berhasil, tanpa kehilangan data	Data tersimpan lokal saat offline dan tersinkron otomatis saat online kembali

Pembahasan

Dengan nilai FAR 0,00%, sistem menjamin tidak ada pihak tidak terdaftar yang dapat menembus ruang Data Center, sementara FRR 10,00% dan waktu respons rata-rata 1,25 detik

menunjukkan sistem tetap nyaman digunakan tanpa menghambat mobilitas staf resmi. Pencatatan log akses otomatis pada Firebase beserta notifikasi Telegram instan (latensi rata-rata 1,81 detik) memberikan transparansi penuh atas aktivitas fisik ruang server, menutup celah ketiadaan jejak audit dan keterlambatan respons pengawasan manual yang menjadi permasalahan pada sistem konvensional. Untuk menilai posisi hasil penelitian ini, hasil pengujian purwarupa dibandingkan dengan tiga penelitian terdahulu yang memiliki karakteristik serupa sebagaimana disajikan pada Tabel 5.

Tabel 5. Perbandingan Hasil dengan Penelitian Terdahulu

No.	Peneliti	Arsitektur	Waktu Respons	Keberhasilan Black Box	Fitur Fail-Safe / Notifikasi
1.	Alsayaydeh dkk. (2025)	Mikrokontroler + sidik jari	±1,00 detik (buka pintu ±5,00 detik)	-	Ada, lockout otomatis
2.	Permana dkk. (2024)	ESP32 + sidik jari + keypad + Firebase	-	100%	Tidak dilaporkan
3.	Hanafie dkk. (2023)	Sidik jari + Telegram Bot API	-	-	Notifikasi Telegram, tanpa lockout otomatis
4.	Purwarupa ini	NodeMCU V3 + sidik jari + Firebase + Telegram	1,25 detik	100%	Ada, lockout 15 detik + buffering offline

Purwarupa pada penelitian ini mencatatkan waktu respons total rata-rata 1,25 detik, sepadan dengan temuan Alsayaydeh dkk. (2025) meskipun menggunakan NodeMCU V3 yang lebih ekonomis dibandingkan ESP32 yang digunakan Permana dkk. (2024). Berbeda dengan Hanafie dkk. (2023) yang belum dilengkapi lockout otomatis dan mekanisme buffering saat offline, purwarupa ini menyempurnakan pendekatan tersebut dengan mengintegrasikan penguncian sementara 15 detik serta penyimpanan data lokal sementara ketika koneksi internet terputus. Hasil ini turut memperkuat argumen bahwa sensor sidik jari layak diterapkan pada berbagai skenario pengamanan aset bernilai tinggi (Indra & Supriyanto, 2024; Pahrudin, 2021), sejalan dengan pentingnya model kontrol akses yang adaptif dan akuntabel pada ekosistem IoT (Ahsan & Pathan, 2025). Meskipun demikian, purwarupa ini masih mengandalkan satu modalitas biometrik (single-factor authentication) dan sangat bergantung pada stabilitas jaringan Wi-Fi lokal untuk pengiriman notifikasi secara real-time. Selain itu, kapasitas penyimpanan template pada modul sensor AS608 (hingga 127–1000 template bergantung varian modul) memerlukan penyesuaian apabila purwarupa diterapkan untuk seluruh pegawai perusahaan.

SIMPULAN

Penelitian ini menghasilkan purwarupa sistem keamanan akses Data Center berbasis IoT yang menggunakan otentikasi biometrik sidik jari, dibangun menggunakan Mikrokontroler NodeMCU V3 (ESP8266), sensor fingerprint AS608, solenoid Door Lock, LCD 16x2 I2C, tombol Override, dan Buzzer yang terintegrasi dengan Firebase Realtime Database dan Telegram Bot API, dilengkapi mekanisme Auto-Lock pada akses masuk maupun keluar. Pengujian fungsional dengan metode Black Box menunjukkan tingkat keberhasilan 100%

pada 12 skenario pengujian, meliputi pendaftaran pengguna, verifikasi akses sah, penolakan akses ilegal beserta mekanisme Fail-Safe (lockout 15 detik), hingga tombol Override dan Auto-Lock.

Pengujian non-fungsional mencatatkan akurasi otentikasi dengan FAR 0,00% dan FRR 10,00% pada 40 kali percobaan verifikasi, rata-rata waktu respons sistem 1,25 detik, serta latensi notifikasi Telegram rata-rata 1,81 detik, dengan mekanisme buffering yang terbukti mampu menjaga konsistensi log data saat terjadi gangguan koneksi Wi-Fi. Dengan demikian, purwarupa ini terbukti mampu menutup celah keamanan pada sistem akses konvensional serta meningkatkan keandalan pengendalian akses Data Center PT XYZ. Pengembangan selanjutnya dapat diarahkan pada penambahan Multi-Factor Authentication, redundansi jaringan GSM/LTE, serta integrasi kamera pengawas otomatis.

DAFTAR PUSTAKA

Ahsan, M. S., & Pathan, A.-S. K. (2025). A comprehensive survey on the requirements, applications, and future challenges for access control models in IoT: The state of the art. *IoT, 6*(1), 9. https://doi.org/10.3390/IoT6010009

Alsayaydeh, J. A. J., Yusof, M. F., Mamchenko, S., Hamzah, R. A., & Herawan, S. G. (2025). Design and evaluation of a biometric IoT-based smart lock system with real-time monitoring and alert mechanisms. *International Journal of Advanced Computer Science and Applications, 16*(7), 1–10. https://doi.org/10.14569/IJACSA.2025.0160737

Efendi, A., Ammarullah, M. I., Isa, I. G. T., Sari, M. P., Izza, J. N., Nugroho, Y. S., Nasrullah, H., & Alfian, D. (2025). IoT-based elderly health monitoring system using Firebase cloud computing. *Health Science Reports, 8*(3), e70498. https://doi.org/10.1002/hsr2.70498

Fauziman, H., & Mukhaiyar, R. (2023). Rancang bangun sistem keamanan pintu menggunakan fingerprint berbasis Internet of Things (IoT). *JTEIN: Jurnal Teknik Elektro Indonesia, 4*(2), 529–537. https://doi.org/10.24036/jtein.v4i2.438

Hanafie, A., Husain, N. P., Sukirman, S., & Nurhidayah, U. (2023). Alat kontrol akses pintu menggunakan sidik jari dengan notifikasi telegram berbasis IoT. *ILTEK: Jurnal Teknologi, 18*(01), 1–5. https://doi.org/10.47398/iltek.v18i01.76

Hercog, D., Lerher, T., Truntič, M., & Težak, O. (2023). Design and implementation of ESP32-based IoT devices. *Sensors, 23*(15), 6739. https://doi.org/10.3390/s23156739

Indra, H., & Supriyanto, R. (2024). Prototype sistem keamanan brankas berbasis sensor sidik jari. *Jurnal Ilmiah Komputasi, 23*(1), 131–138. https://doi.org/10.32409/jikstik.23.1.3519

Pahrudin, R. (2021). Pemanfaatan biometrics fingerprint sensor dan barcode sensor pada sistem keamanan parkir. *Elkom: Jurnal Elektronika dan Komputer, 14*(1), 35–46. https://doi.org/10.51903/elkom.v14i1.363

Permana, K. A. K., Piarsa, I. N., & Wiranatha, A. A. K. A. C. (2024). IoT-based smart door lock system with fingerprint and keypad access. *Journal of Information Systems and Informatics, 6*(3), 2086–2098. https://doi.org/10.51519/journalisi.v6i3.844

Raditya, W., Surahman, A., Budiawan, A., Amanda, F., Dwi Putri, N., & Yudha, S. (2023). Penerapan sistem keamanan gerbang rumah berbasis Telegram menggunakan ESP8266. *Jurnal Teknik dan Sistem Komputer (JTIKOM), 3*(2), 93–103. https://doi.org/10.33365/jtikom.v3i2.2353

Ragothaman, K., Wang, Y., Rimal, B., & Lawrence, M. (2023). Access control for IoT: A survey of existing research, dynamic policies and future directions. *Sensors, 23*(4), 1805. https://doi.org/10.3390/s23041805

Shaheen, G., Alahmadi, F., Alsulami, A., & Salama, S. (2024). A survey on IoT security: IoT

architecture, security issues, challenges, and solutions. *International Journal of Computer Applications, 186*(16), 14–19. https://doi.org/10.5120/ijca2024923543

Sung, W.-T., Tofik Isa, I. G., & Hsiao, S.-J. (2023). An IoT-based aquaculture monitoring system using Firebase. *Computers, Materials & Continua, 76*(2), 2179–2200. https://doi.org/10.32604/cmc.2023.041022

Yang, W., Wang, S., Sahri, N. M., Karie, N. M., Ahmed, M., & Valli, C. (2021). Biometrics for Internet-of-Things security: A review. *Sensors, 21*(18), 6163. https://doi.org/10.3390/s21186163

Zulfikar, R., Sukardi, S., Mukhaiyar, R., & Myori, D. (2023). Rancang bangun keamanan pintu otomatis menggunakan face recognition berbasis Internet of Things (IoT). *JTEIN: Jurnal Teknik Elektro Indonesia, 4*(2), 445–453. https://doi.org/10.24036/jtein.v4i2.385