

PERANCANGAN SISTEM KEMAMAN PINTU BERBASIS *BIOMETRIK* SIDIK JARI UNTUK RUANG SERVER MENGUNAKAN METODE *AGILE* DI DISKOMINFO PROVINSI BANTEN

Ali Maruf Iskandar¹, Ahmad Rufa'i², Adith Aulia Rahman³.

Fakultas Teknik, Program Studi Informatika, Universitas Primagraha
Komplek Griya Gemilang Sakti, Jl. Trip Jamaksari, Kaligandu, Kec. Serang, Kota Serang, Bante
e-mail: ^{*1}alimarufiskandarr@gmail.com, ^{*2}arufai936@gmail.com,
^{*3}adithauliarahman@gmail.com.

Abstak

Keamanan ruang server merupakan aspek penting dalam menjaga kerahasiaan dan integritas data layanan publik. Sistem keamanan konvensional yang masih digunakan di Dinas Komunikasi dan Informatika Provinsi Banten memiliki kelemahan, seperti risiko duplikasi kunci, penyalahgunaan akses, serta keterbatasan pengawasan. Penelitian ini bertujuan merancang dan mengimplementasikan sistem keamanan pintu ruang server berbasis biometrik sidik jari untuk meningkatkan keamanan dan efektivitas kontrol akses. Metode penelitian yang digunakan adalah Agile, dipilih karena fleksibel dan adaptif terhadap perubahan kebutuhan pengguna. Tahapan penelitian meliputi analisis kebutuhan, perancangan sistem, implementasi, dan pengujian. Sistem dikembangkan menggunakan modul fingerprint yang terintegrasi dengan NodeMCU ESP8266, solenoid door lock, relay, LCD, dan buzzer. Hasil pengujian menunjukkan sistem mampu mengenali sidik jari terdaftar dengan akurasi yang baik, waktu respon cepat, serta menolak akses tidak sah secara konsisten. Sistem juga menyediakan pencatatan dan notifikasi akses sebagai bentuk pengawasan. Penelitian ini berdampak pada peningkatan keamanan ruang server dan pengurangan risiko akses ilegal.

Kata kunci: sistem keamanan, biometrik sidik jari, ruang server, NodeMCU ESP8266, Agile.

Abstract

Server room security is a critical aspect in maintaining the confidentiality and integrity of public service data. Conventional security systems still used at the Banten Province Communication and Informatics Office have several weaknesses, including the risk of key duplication, access misuse, and limited monitoring capabilities. This study aims to design and implement a fingerprint-based biometric door security system to improve security and access control effectiveness. The research methodology employs the Agile method, selected for its flexibility and adaptability to changing user requirements. The research stages include requirements analysis, system design, implementation, and testing. The system is developed using a fingerprint module integrated with NodeMCU ESP8266, a solenoid door lock, relay, LCD, and buzzer. Test results indicate that the system is able to accurately recognize registered fingerprints, provide fast response times, and consistently deny unauthorized access. In addition, the system supports access logging and notification features to enhance supervision. This research contributes to improved server room security and reduces the risk of illegal access

Keywords: Security System, Fingerprint, Server Room, Arduino, Agile Method.

PENDAHULUAN

Perkembangan teknologi saat ini menawarkan kemudahan kepada para pengguna dalam berbagai sendi kehidupan Teknologi biometri sedang berkembang dengan sangat cepat, dan sebagian besar digunakan dalam bidang keamanan karena memiliki kemampuan untuk melakukan proses identifikasi dan verifikasi. Otentikasi biometrik, yang berasal dari kata Yunani "*bios*", yang berarti "hidup", dan "*metron*", yang berarti "mengukur," dapat diartikan sebagai studi tentang metode otomatis untuk mengenali manusia berdasarkan satu atau lebih bagian tubuh manusia atau tindakan unik mereka. Dalam bidang teknologi informasi, biometrik terkait dengan teknologi yang digunakan untuk menganalisa fisik dan kelakuan manusia untuk mengkonfirmasi identitas. Contohnya dalam pengenalan fisik manusia adalah sidik jari, retina, iris, dan pola wajah.

Keamanan informasi merupakan aspek fundamental dalam pengelolaan teknologi informasi, khususnya pada instansi pemerintahan yang menyimpan data strategis dan sensitif. Ruang server sebagai pusat penyimpanan dan pengolahan data membutuhkan sistem keamanan yang andal untuk menjamin kerahasiaan, integritas, dan ketersediaan informasi. Beberapa penelitian menyatakan bahwa lemahnya kontrol akses fisik dapat meningkatkan risiko kebocoran data dan penyalahgunaan sistem (Permana et al., 2022; Sukma et al., 2023).

Pada praktiknya, masih banyak instansi yang menggunakan sistem keamanan konvensional seperti kunci fisik atau kartu akses. Metode ini memiliki berbagai kelemahan, antara lain mudah hilang, dapat digandakan, serta tidak mampu mencatat dan memantau aktivitas akses secara terstruktur. Penelitian oleh Masrizal et al. (2022) dan Hanif et al. (2024) menunjukkan bahwa sistem pengamanan berbasis kunci konvensional kurang efektif dalam mencegah akses tidak sah dan sulit diterapkan pada lingkungan yang membutuhkan tingkat keamanan tinggi.

Sebagai alternatif, teknologi biometrik sidik jari telah banyak diterapkan dalam sistem kontrol akses karena memiliki tingkat akurasi dan keunikan yang tinggi. Hadiyanto et al. (2021) menyatakan bahwa sistem biometrik sidik jari unggul dalam hal kecepatan autentikasi dan keandalan dibandingkan metode identifikasi lainnya. Selain itu, Setiawan et al. (2022) menegaskan bahwa biometrik sidik jari relatif mudah diimplementasikan dan memiliki biaya yang lebih efisien untuk penggunaan jangka panjang.

Perkembangan Internet of Things (IoT) turut mendorong integrasi sistem keamanan dengan perangkat cerdas yang memungkinkan monitoring dan notifikasi secara real-time. Penelitian Ardiansah et al. (2024) membuktikan bahwa penggabungan modul fingerprint dengan mikrokontroler berbasis IoT mampu meningkatkan efektivitas sistem keamanan pintu otomatis. Namun, sebagian besar penelitian sebelumnya masih berfokus pada lingkungan rumah tinggal atau skala personal, sehingga penerapannya pada instansi pemerintahan masih terbatas.

Oleh karena itu, penelitian ini berfokus pada perancangan dan implementasi sistem keamanan pintu ruang server berbasis biometrik sidik jari menggunakan NodeMCU ESP8266 di Dinas Komunikasi dan Informatika Provinsi Banten. Metode Agile digunakan dalam pengembangan sistem karena mampu memberikan fleksibilitas, adaptasi cepat terhadap kebutuhan pengguna, serta peningkatan kualitas sistem secara bertahap (Pratasik & Rianto, 2020). Diharapkan, penelitian ini dapat memberikan kontribusi nyata dalam meningkatkan keamanan ruang server, mengurangi risiko akses ilegal, serta mendukung pengawasan yang lebih terstruktur dan efisien di lingkungan pemerintahan.

Oleh karena itu, penelitian ini berfokus pada perancangan dan implementasi sistem keamanan pintu ruang server berbasis biometrik sidik jari menggunakan NodeMCU ESP8266 di Dinas Komunikasi dan Informatika Provinsi Banten. Penggunaan metode Agile dipilih karena dinilai mampu mendukung proses pengembangan sistem yang fleksibel, adaptif terhadap kebutuhan pengguna, serta memungkinkan penyempurnaan sistem secara bertahap. Melalui penelitian ini,

penulis meyakini bahwa sistem yang dikembangkan dapat meningkatkan keamanan ruang server, meminimalkan risiko akses ilegal, serta mendukung pengawasan akses yang lebih terstruktur dan efisien di lingkungan pemerintahan.

METODE PENELITIAN

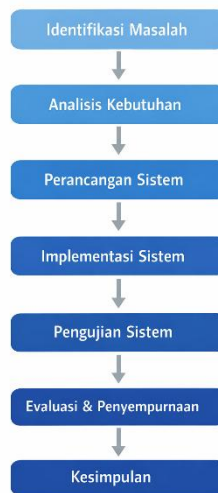
Penelitian ini menggunakan pendekatan rekayasa sistem dengan metode pengembangan perangkat lunak Agile untuk merancang dan mengimplementasikan sistem keamanan pintu ruang server berbasis biometrik sidik jari. Metode Agile dipilih karena mampu mendukung pengembangan sistem secara iteratif, fleksibel, dan adaptif terhadap perubahan kebutuhan pengguna, khususnya pada lingkungan instansi pemerintahan yang dinamis. Beberapa penelitian sebelumnya menyatakan bahwa metode Agile efektif digunakan pada pengembangan sistem berbasis IoT dan keamanan karena memungkinkan perbaikan berkelanjutan melalui umpan balik pengguna (Pratasik & Rianto, 2020; Ardiansah et al., 2024).

Tahapan penelitian diawali dengan analisis kebutuhan sistem yang dilakukan melalui observasi langsung dan wawancara dengan pihak terkait di Dinas Komunikasi dan Informatika Provinsi Banten. Pada tahap ini digunakan pendekatan kualitatif untuk memahami kondisi sistem keamanan yang berjalan, mengidentifikasi permasalahan, serta menentukan kebutuhan fungsional dan non-fungsional sistem. Luaran dari tahap ini berupa spesifikasi kebutuhan sistem keamanan pintu ruang server yang menjadi dasar dalam proses perancangan. Tahap berikutnya adalah perancangan sistem yang mencakup perancangan arsitektur perangkat keras dan perangkat lunak dengan menggunakan pendekatan pemodelan Unified Modeling Language (UML) untuk menggambarkan alur proses dan interaksi pengguna dengan sistem. Sistem dirancang dengan mengintegrasikan modul fingerprint sebagai perangkat autentikasi utama dengan NodeMCU ESP8266, solenoid door lock, relay, LCD, dan buzzer, sehingga menghasilkan luaran berupa rancangan arsitektur sistem, diagram alur proses, dan desain antarmuka pengguna.

Setelah tahap perancangan selesai, penelitian dilanjutkan dengan tahap implementasi sistem, yaitu pengembangan sistem berdasarkan rancangan yang telah dibuat melalui integrasi perangkat keras dan perangkat lunak menggunakan Arduino IDE. Pada tahap ini diterapkan pendekatan iteratif metode Agile, di mana proses pengembangan dan penyempurnaan dilakukan secara bertahap berdasarkan hasil evaluasi selama pengembangan berlangsung. Luaran dari tahap ini adalah prototipe sistem keamanan pintu ruang server berbasis biometrik sidik jari yang telah berfungsi secara operasional sesuai dengan kebutuhan yang dirumuskan.

Tahap selanjutnya adalah pengujian sistem yang bertujuan untuk memastikan sistem berjalan sesuai dengan spesifikasi yang telah ditetapkan. Pengujian dilakukan terhadap fungsi autentikasi sidik jari, mekanisme pembukaan dan penguncian pintu, penolakan akses tidak sah, serta tampilan informasi pada LCD dan notifikasi sistem dengan menggunakan pendekatan pengujian fungsional. Luaran dari tahap ini berupa data hasil pengujian yang menunjukkan tingkat keberhasilan autentikasi, kecepatan respon sistem, dan keandalan dalam menolak akses ilegal. Berdasarkan hasil tersebut, dilakukan tahap evaluasi dan penyempurnaan sistem dengan mempertimbangkan umpan balik pengguna agar sistem semakin stabil, efisien, dan siap diterapkan di lingkungan operasional. Seluruh rangkaian tahapan ini dirangkum dalam sebuah diagram alir penelitian yang menggambarkan keterkaitan antara analisis kebutuhan, perancangan, implementasi, pengujian, hingga evaluasi dan penyempurnaan sistem.

Dalam pengembangan sistem keamanan pintu berbasis biometrik sidik jari ini, metodologi penelitian mencakup beberapa tahapan teknis utama yang saling berkaitan, yaitu perancangan sistem, implementasi perangkat, serta pemodelan sistem menggunakan *Unified Modeling Language* (UML). Ketiga tahapan ini dilakukan secara terstruktur untuk memastikan bahwa sistem yang dibangun memiliki rancangan yang jelas, terimplementasi secara fungsional, serta terdokumentasi dengan baik dari sisi alur proses dan interaksi pengguna. Oleh karena itu, penjelasan berikut menguraikan secara

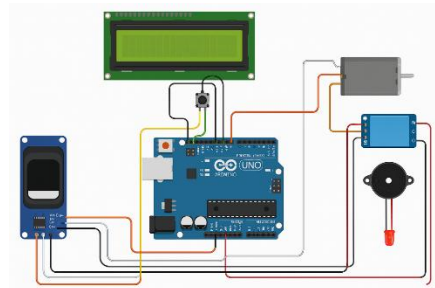


Gambar 1 Diagram Alur

rinci masing-masing tahapan tersebut beserta peran dan luaran yang dihasilkan dalam mendukung tercapainya tujuan penelitian.

1. Perancangan Sistem

Tahap perancangan sistem bertujuan untuk merumuskan bentuk, struktur, dan mekanisme kerja sistem keamanan pintu berbasis biometrik sidik jari sebelum direalisasikan secara fisik. Pada tahap ini dilakukan perancangan arsitektur sistem yang menggambarkan hubungan



Gambar 2 Arsitektur perancangan Sistem

antar komponen, alur kerja sistem, serta mekanisme autentikasi pengguna, mulai dari proses pembacaan sidik jari, verifikasi data, pengendalian kunci pintu, hingga penyampaian informasi kepada pengguna melalui LCD dan notifikasi. Berdasarkan rancangan tersebut, sistem kemudian direalisasikan melalui integrasi perangkat keras dan perangkat lunak. Implementasi perangkat keras meliputi penggabungan modul fingerprint, NodeMCU ESP8266, relay, solenoid door lock, LCD, buzzer, push button, dan catu daya ke dalam satu kesatuan sistem yang saling terhubung.

Tabel 1 Spesifikasi Perangkat Keras (*Hardware*)

No	Nama Modul	Berfungsi
1.	Node MCU8266	sebagai mikrokontroler utama yang mengendalikan seluruh proses sistem serta menghubungkan perangkat ke jaringan Wi-Fi.
2.	Sensor Fingerprint DY50	membaca dan mengenali sidik jari pengguna yang telah terdaftar.
3.	LCD 16x2 12C	menampilkan status sistem seperti “Akses Diterima” atau “Akses Ditolak”.
4.	Solenoid Doorlock	pengunci otomatis yang terbuka apabila autentikasi sidik jari berhasil.
5.	Relay 1 Chanel	mengatur aliran listrik menuju kunci solenoid sesuai sinyal dari NodeMCU.
6.	Buzzer	indikasi suara ketika proses autentikasi berhasil atau gagal.
7.	Push Button	kontrol manual atau tombol darurat untuk membuka pintu secara langsung jika terjadi gangguan pada sensor.
8.	Power supply 12V	sebagai sumber daya utama sistem.

Sementara itu, implementasi perangkat lunak dilakukan dengan memprogram NodeMCU menggunakan Arduino IDE untuk mengatur logika autentikasi, komunikasi dengan sensor, pengendalian aktuator, serta pengiriman notifikasi melalui Telegram Bot.

Tabel 2 Spesifikasi Perangkat Lunak (*Software*)

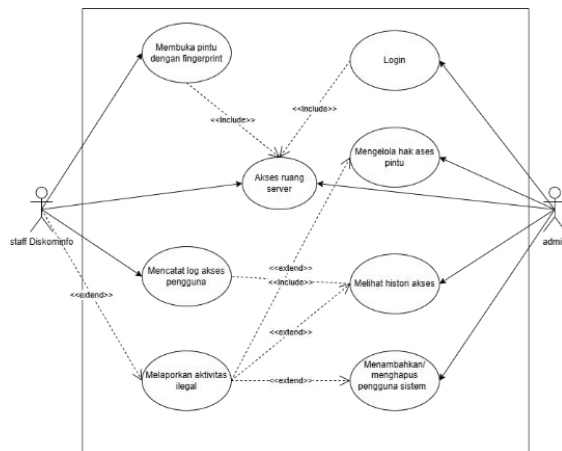
No	Nama Perangkat Lunak	Fungsi	Keterangan Penggunaan
1.	Arduino IDE	Lingkungan Pengembangan (IDE) untuk pemrograman mikrokontroler	Digunakan untuk menulis, mengunggah, dan melakukan debugging program pada NodeMCU ESP8266 yang mengatur proses autentikasi, kontrol solenoid, LCD, buzzer, serta komunikasi dengan sensor fingerprint.
2.	Library Fingerprint (Adafruit / DY50)	Pustaka komunikasi sensor sidik jari	Digunakan untuk proses pendaftaran, pencocokan, dan verifikasi sidik jari pada modul fingerprint DY50.
3.	Library ESP8266 WiFi	Koneksi jaringan	Digunakan untuk menghubungkan NodeMCU dengan jaringan Wi-Fi agar sistem dapat mengirim notifikasi dan data ke server atau aplikasi Telegram.

4.	Telegram Bot API	Layanan notifikasi berbasis pesan instan	Digunakan untuk mengirimkan informasi status pintu, hasil autentikasi, dan waktu akses kepada administrator secara real-time.
----	------------------	--	---

Dalam proses pengembangan, pendekatan iteratif metode Agile diterapkan agar sistem dapat diuji dan disempurnakan secara bertahap hingga mencapai kinerja yang stabil dan sesuai dengan kebutuhan. Luaran dari tahap ini adalah prototipe sistem keamanan pintu berbasis biometrik sidik jari yang telah terimplementasi dan dapat dioperasikan secara fungsional sebagai dasar untuk tahap pengujian.

2. Pemodelan Sistem

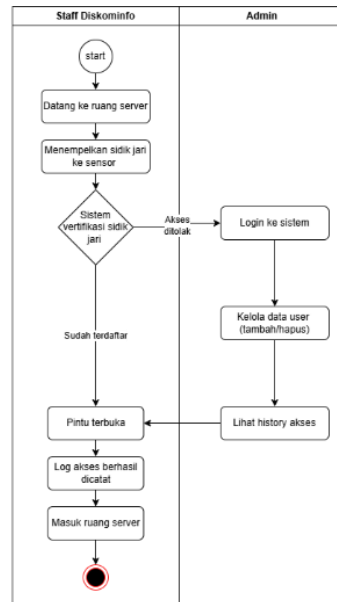
Pemodelan sistem dilakukan menggunakan Unified Modeling Language (UML) untuk menggambarkan struktur dan perilaku sistem keamanan pintu berbasis biometrik sidik jari secara visual dan terstruktur. UML digunakan sebagai alat bantu analisis dan dokumentasi guna mempermudah pemahaman terhadap kebutuhan fungsional, alur proses, serta interaksi antara pengguna dan sistem. Dalam penelitian ini, pemodelan sistem direpresentasikan melalui dua jenis diagram utama, yaitu Use Case Diagram dan Activity Diagram.



Gambar 3 Use Case Diagram Sistem Smart Door Lock

Use Case Diagram menggambarkan hubungan antara aktor dan sistem, sehingga dapat dipahami peran pengguna serta fungsi utama yang disediakan sistem keamanan pintu berbasis biometrik. Diagram ini menunjukkan bahwa hanya pengguna terdaftar yang memiliki hak akses untuk melakukan autentikasi dan membuka pintu, yang secara langsung merepresentasikan solusi terhadap permasalahan utama penelitian, yaitu tingginya risiko akses ilegal pada sistem pengamanan konvensional.

Sementara itu, *Activity Diagram* memvisualisasikan alur proses sistem mulai dari input sidik jari, proses verifikasi, hingga pengambilan keputusan untuk membuka atau menolak akses pintu. Alur ini menunjukkan bagaimana mekanisme kerja sistem mampu melakukan kontrol akses secara otomatis dan terstruktur.



Gambar 4 *Activity Diagram*
Sistem *Smart Door Lock*

Dengan demikian, penerapan alur sistem yang dimodelkan melalui Use Case Diagram dan *Activity Diagram* menunjukkan bahwa rancangan sistem yang diusulkan mampu meningkatkan keandalan dalam membedakan pengguna sah dan tidak sah, mempercepat proses autentikasi, serta menyediakan mekanisme pencatatan aktivitas yang mendukung fungsi pengawasan. Hal ini menegaskan bahwa model sistem yang dikembangkan tidak hanya layak secara teknis, tetapi juga efektif dan relevan dalam menjawab permasalahan keamanan ruang server yang menjadi fokus penelitian ini.

HASIL DAN PEMBAHASAN

Bagian ini menyajikan hasil implementasi dan pengujian sistem keamanan pintu ruang server berbasis biometrik sidik jari yang telah dirancang, serta analisis terhadap kinerja sistem dalam menjalankan fungsi autentikasi, kontrol akses, dan monitoring sesuai dengan tujuan penelitian.

1. Implementasi Sistem

Implementasi sistem dilakukan berdasarkan hasil perancangan yang telah disusun pada tahap metodologi. Implementasi ini meliputi realisasi perangkat keras (*hardware*) dan perangkat lunak (*software*) yang saling terintegrasi untuk membentuk sistem keamanan pintu ruang server berbasis biometrik sidik jari.

1) Implementasi Perangkat Keras (*Hardware*)

Implementasi perangkat keras mencakup penyusunan dan integrasi seluruh modul utama, komponen pendukung, serta komponen penunjang yang berperan dalam proses pembacaan sidik jari, pengolahan data, pengendalian aktuatur, dan penyampaian informasi. Secara umum, perangkat keras yang digunakan dalam sistem ini dapat dikelompokkan menjadi tiga bagian, yaitu modul utama, komponen,

dan komponen penunjang

Tabel 3 Implementasi Perangkat Keras (Hardware)

Modul Utama	Komponen Sistem	Komponen Penunjang
Sensor <i>Fingerprint</i> DY50	<i>Relay</i>	<i>Power Supply 12V</i>
NodeMCU ESP8266	<i>Solenoid Door Lock</i>	<i>Smartphone</i>
	LCD	
	<i>Buzzer</i>	
	<i>Push Button</i>	

Perakitan perangkat keras dilakukan dengan menghubungkan seluruh modul dan komponen sesuai dengan skema rangkaian yang telah dirancang. Sensor *fingerprint* dihubungkan ke NodeMCU melalui komunikasi serial, sementara relay digunakan sebagai pengendali solenoid *door lock*. LCD dan *buzzer* dihubungkan sebagai media informasi dan peringatan, sedangkan push button berfungsi sebagai kontrol manual. Setelah seluruh komponen terpasang, sistem diuji untuk memastikan bahwa setiap bagian dapat bekerja secara sinkron dan stabil.



Gambar 5 Perakitan Perangkat Keras
(Hardware)

2) Implementasi Perangkat Lunak (Software)

Implementasi perangkat lunak dilakukan dengan memprogram *NodeMCU* ESP8266 menggunakan *Arduino IDE*. Perangkat lunak berfungsi untuk mengatur alur logika sistem, proses pencocokan sidik jari, pengendalian perangkat keras, serta pengiriman notifikasi melalui jaringan. Tabel berikut menunjukkan perangkat lunak dan fungsinya dalam sistem.

Tabel 4 Implementasi Perangkat Lunak (Software)

Perangkat Lunak (<i>software</i>)	Fungsi
Arduino IDE	Lingkungan pengembangan untuk penulisan, kompilasi, dan unggah program ke <i>NodeMCU</i> .
Library Fingerprint	Mengelola proses pendaftaran, pencocokan, dan verifikasi sidik jari.

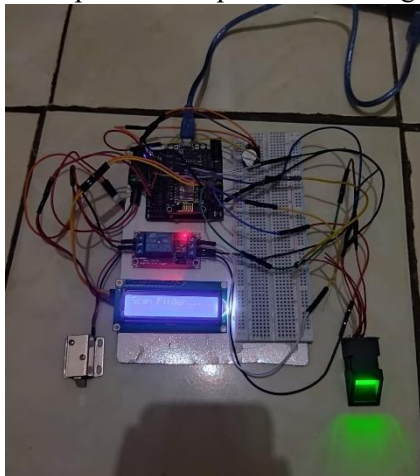
Library ESP8266 WiFi	Menghubungkan sistem ke jaringan internet.
Telegram Bot API	Mengirimkan notifikasi akses dan status pintu secara real-time.

2. Pengujian Sistem

Pengujian sistem dilakukan untuk memastikan bahwa seluruh fungsi yang telah dirancang dan diimplementasikan dapat berjalan dengan baik serta mampu menjawab permasalahan keamanan ruang server. Pengujian difokuskan pada kinerja sistem dalam memberikan akses, menolak akses tidak sah, serta mengirimkan informasi kepada administrator. Berdasarkan mekanisme kerja sistem, pengujian dibedakan menjadi tiga bagian, yaitu pengujian manual, pengujian otomatis menggunakan perangkat biometrik, dan pengujian sistem notifikasi melalui Telegram.

1) Pengujian Sistem Secara Manual

Pengujian manual dilakukan dengan menggunakan push button yang berfungsi sebagai akses alternatif dalam kondisi tertentu, seperti keadaan darurat atau gangguan pada sensor biometrik. Pada pengujian ini, tombol ditekan untuk memberikan perintah pembukaan pintu secara langsung.

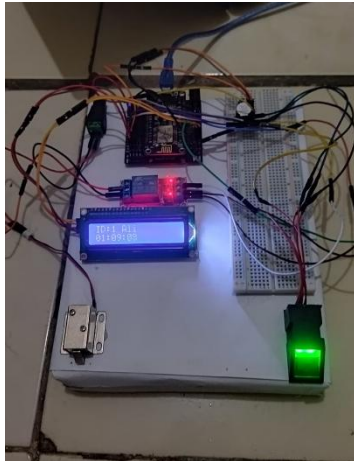


Gambar 6 Semua Perangkat ON

Tabel 5 Proses Uji Coba Sistem Secara Manual

Proses Pengujian	Hasil Pengujian	Analisis
Menekan push button untuk membuka pintu tanpa autentikasi sidik jari	1. Relay aktif, solenoid door lock membuka pintu, LCD menampilkan status akses manual, buzzer berbunyi, dan notifikasi terkirim ke Telegram	Sistem mampu memberikan akses alternatif dalam kondisi darurat. Mekanisme ini tetap berada dalam pengawasan karena setiap akses manual tercatat dan diinformasikan kepada administrator. Hal ini menunjukkan bahwa fleksibilitas akses tidak mengurangi aspek keamanan.

- 2) Pengujian Sistem Secara Otomatis Menggunakan *Fingerprint*
 Pengujian otomatis dilakukan dengan memanfaatkan modul fingerprint sebagai metode utama autentikasi. Pengujian dilakukan dengan membandingkan respon sistem terhadap sidik jari yang terdaftar dan yang tidak terdaftar.

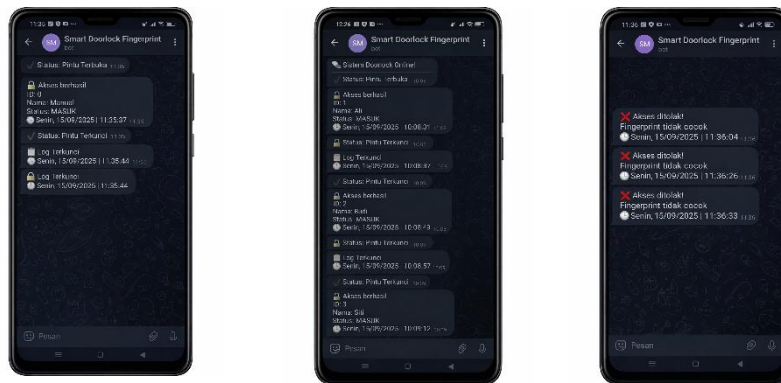


Gambar 7 Pengujian Sistem Menggunakan *Fingerprint*

Tabel 6 Pengujian Sistem Menggunakan *Fingerprint*

Proses Pengujian	Hasil Pengujian	Analisis
Sidik jari terdaftar ditempelkan pada sensor <i>fingerprint</i>	1. Sistem mengenali sidik jari, relay aktif, solenoid membuka pintu, LCD menampilkan identitas, buzzer berbunyi singkat, notifikasi terkirim	Sistem berhasil melakukan autentikasi pengguna yang sah dengan respon cepat dan akurat, menunjukkan keandalan teknologi biometrik sebagai pengganti kunci konvensional.
Sidik jari tidak terdaftar ditempelkan pada sensor <i>fingerprint</i>	2. Sistem menolak akses, pintu tetap terkunci, LCD menampilkan pesan “Akses Ditolak”, buzzer berbunyi peringatan, notifikasi terkirim	Mekanisme penolakan bekerja konsisten, membuktikan bahwa sistem efektif dalam mencegah akses ilegal ke ruang server.

- 3) Pengujian Sistem Notifikasi Telegram (Manual dan Otomatis)
 Pengujian sistem notifikasi dilakukan untuk memastikan bahwa setiap aktivitas akses, baik melalui mode manual maupun otomatis, dapat diinformasikan kepada administrator secara real-time melalui aplikasi Telegram.



Gambar 8 Pengujian Sistem Notifikasi Telegram

Proses Pengujian	Hasil Pengujian	Analisis
Akses pintu melalui <i>fingerprint</i> (berhasil dan gagal)	1. Pesan notifikasi terkirim berisi status akses, identitas pengguna, dan waktu kejadian	Sistem mampu melakukan monitoring real-time, sehingga administrator dapat mengetahui setiap aktivitas akses secara langsung.
Akses pintu melalui push button (manual)	2. Pesan notifikasi terkirim dengan keterangan akses manual dan waktu kejadian	Fitur notifikasi memastikan bahwa seluruh aktivitas, baik otomatis maupun manual, tetap tercatat sebagai log keamanan dan dapat digunakan untuk audit serta pengawasan.

KESIMPULAN

Berdasarkan hasil implementasi dan pengujian yang telah dibahas, sistem keamanan pintu ruang server berbasis biometrik sidik jari yang dikembangkan terbukti mampu meningkatkan pengendalian akses dibandingkan metode konvensional. Hasil pengujian menunjukkan bahwa autentikasi otomatis menggunakan sensor fingerprint dapat mengenali pengguna terdaftar secara akurat dan menolak akses tidak sah secara konsisten, yang ditandai dengan mekanisme penguncian pintu tetap aktif serta pemberian peringatan melalui LCD dan buzzer. Selain itu, mekanisme akses manual melalui push button dapat berfungsi sebagai alternatif dalam kondisi tertentu tanpa menghilangkan aspek pengawasan karena setiap aktivitas tetap tercatat. Pengujian fitur notifikasi Telegram juga menunjukkan bahwa sistem mampu mengirimkan informasi akses secara real-time, baik pada mode otomatis maupun manual, sehingga administrator dapat melakukan pemantauan jarak jauh dan memperoleh rekaman aktivitas secara terstruktur. Dengan demikian, sistem yang dirancang tidak hanya mampu menjawab permasalahan utama terkait risiko duplikasi kunci dan keterbatasan monitoring pada ruang server, tetapi juga memberikan solusi yang lebih aman, responsif, dan terkontrol melalui penerapan teknologi biometrik dan IoT. menampilkan status sesuai kondisi pintu, dan NodeMCU dapat mengirimkan notifikasi dengan stabil.

SARAN

Sebagai pengembangan ke depan, sistem keamanan pintu ruang server berbasis biometrik ini masih memiliki peluang untuk diteliti lebih lanjut. Salah satunya adalah dengan mengombinasikan sidik jari dengan metode identifikasi lain, seperti pengenalan wajah atau kartu akses, sehingga sistem memiliki lapisan keamanan tambahan. Penelitian selanjutnya juga dapat mengkaji penerapan sistem ini pada lebih dari satu ruang server dengan pengelolaan akses terpusat, sehingga pengawasan dapat dilakukan secara lebih menyeluruh. Selain itu, data riwayat akses yang dihasilkan dapat dimanfaatkan untuk analisis pola penggunaan dan deteksi aktivitas tidak normal, sehingga fungsi sistem tidak hanya sebagai pengaman pintu, tetapi juga sebagai alat bantu dalam pencegahan potensi ancaman keamanan di masa mendatang.

DAFTAR PUSTAKA

- Ardiansah, R., Prasetyo, A., & Hidayat, R. (2023). Sistem keamanan pintu berbasis sidik jari menggunakan ESP8266 dan notifikasi Telegram. *Jurnal Teknologi dan Sistem Komputer*, 11(2), 85–93.
- Hadiyanto, T., Nugroho, A., & Setiawan, D. (2022). Implementasi sistem akses kontrol biometrik sidik jari pada ruang server. *Jurnal Informatika Mulawarman*, 17(1), 45–52.
- Hanif, M., Ramadhan, F., & Kurniawan, Y. (2023). Rancang bangun smart door lock berbasis IoT menggunakan NodeMCU. *Jurnal RESTI (Rekayasa Sistem dan Teknologi Informasi)*, 7(3), 512–520.
- Masrizal, M., Suryadi, D., & Putra, R. (2022). Analisis keamanan akses pintu menggunakan fingerprint dan RFID. *Jurnal Teknologi Informasi dan Ilmu Komputer*, 9(4), 789–797.
- Permana, A., Lestari, S., & Wahyudi, I. (2022). Sistem keamanan ruangan berbasis biometrik untuk lingkungan perkantoran. *Jurnal Sistem Informasi*, 18(2), 134–142.
- Pratasik, H., & Rianto, B. (2020). Penerapan metode Agile dalam pengembangan sistem berbasis IoT. *Jurnal Teknologi Informasi dan Terapan*, 7(1), 1–9.
- Setiawan, D., Hidayat, R., & Prabowo, T. (2022). Evaluasi akurasi sensor sidik jari pada sistem kontrol akses. *Jurnal Ilmiah Teknik Elektro*, 21(3), 210–218.
- Sukma, A., Wibowo, E., & Santoso, B. (2023). Analisis risiko keamanan fisik ruang server pada instansi pemerintah. *Jurnal Keamanan Informasi*, 5(1), 33–41.
- Yuliana, R., Prasetya, H., & Nugraha, A. (2021). Rancang bangun sistem smart lock berbasis Arduino dan fingerprint. *Jurnal Informatika Polinema*, 7(2), 98–105.
- Kurniawan, A., & Saputra, D. (2022). Sistem monitoring akses pintu menggunakan Telegram Bot. *Jurnal Teknologi Informasi dan Komunikasi*, 11(1), 56–64.
- Fauzan, M., & Rahman, F. (2021). Implementasi IoT pada sistem keamanan gedung. *Jurnal Teknik Informatika*, 9(2), 120–128.
- Putri, N., & Sari, D. (2020). Pengembangan sistem kontrol akses menggunakan biometrik. *Jurnal Ilmu Komputer dan Aplikasi*, 8(1), 45–53.
- Rizky, M., & Anwar, S. (2023). Integrasi NodeMCU ESP8266 pada sistem keamanan pintu otomatis. *Jurnal Teknologi Elektro*, 14(2), 175–183.

- Wahyuni, T., & Pratama, A. (2022). Sistem autentikasi berbasis fingerprint untuk ruang terbatas. *Jurnal Sistem Cerdas*, 5(3), 201–209.
- Saputra, R., & Hendra, Y. (2021). Perancangan sistem akses kontrol berbasis mikrokontroler. *Jurnal Teknologi Terapan*, 10(1), 60–68.
- Rahmawati, L., & Kurnia, A. (2023). Implementasi notifikasi real-time pada sistem keamanan IoT. *Jurnal Informatika dan Sistem Informasi*, 6(2), 145–153.
- Maulana, I., & Nugroho, S. (2020). Sistem keamanan pintu menggunakan fingerprint dan solenoid. *Jurnal Teknik Elektro Universitas Negeri*, 12(1), 34–41.
- Siregar, H., & Lubis, M. (2021). Analisis performa sistem biometrik sidik jari. *Jurnal Komputer dan Informatika*, 9(3), 250–258.
- Aziz, A., & Firdaus, M. (2022). Pengembangan sistem keamanan berbasis IoT di lingkungan perkantoran. *Jurnal Teknologi Informasi*, 13(2), 99–107.
- Herlambang, D., & Prakoso, A. (2023). Implementasi Agile pada pengembangan sistem embedded. *Jurnal Rekayasa Perangkat Lunak*, 5(1), 15–24.