

# Optimization of Latency and Security in Multi-Door Access Control Systems through Centralized Mobile Biometric Verification

Agustinus Bimo Gumelar<sup>1\*</sup>, Laxmi Utari<sup>2</sup>, Ageng Salmanarrizqie<sup>3</sup>, Muhammad Nasir<sup>4</sup>

<sup>1</sup>Program Studi Informatika, Fakultas Teknologi Informasi, Universitas Ciputra Surabaya, 60219, Indonesia

<sup>2</sup>Jurusan Teknik Informatika, Fakultas Ilmu Komputer, Universitas Narotama, Surabaya, 60117, Indonesia

<sup>3</sup>Gantara Studio, PT. Air Media Nusantara, Surabaya, 60283, Indonesia

<sup>4</sup>Politeknik Negeri Lhokseumawe, Lhokseumawe, 24301, Indonesia

## Informasi Artikel

Diterima : 13 Mei 2026  
Revisi : 20 Mei 2026  
Publikasi : 30 Juni 2026

## Kata Kunci:

Multi-door access control  
Biometric authentication  
Wireless connectivity  
Mobile security  
Internet of Things

## ABSTRAK

Eskalasi kebutuhan terhadap keamanan fisik dalam paradigma digital menuntut solusi kontrol akses multi-titik yang tangguh. Penelitian ini menyajikan perancangan arsitektur dan implementasi sistem penguncian multi-pintu terpusat yang terintegrasi dengan autentikasi biometrik dan konektivitas nirkabel. Metodologi yang diterapkan menggunakan pendekatan pengembangan sistem terintegrasi, memanfaatkan Arduino Uno sebagai pengendali utama dan ESP8266 untuk transmisi data nirkabel yang terhubung melalui aplikasi seluler. Metrik kinerja kuantitatif memvalidasi efisiensi sistem dengan catatan latensi rata-rata 1,2 detik pada lima titik akses serta akurasi autentikasi biometrik mencapai 96%. Notifikasi status waktu nyata berhasil dikirimkan dalam ambang batas dua detik guna memastikan transparansi operasional. Analisis menunjukkan bahwa stabilitas jaringan merupakan determinan kinerja kritis, di mana atenuasi sinyal di bawah -75 dBm berdampak signifikan terhadap responsivitas. Temuan ini mengindikasikan bahwa konvergensi biometrik seluler dan perangkat keras terdistribusi menyediakan kerangka kerja yang skalabel dan hemat biaya bagi infrastruktur keamanan modern.

## ABSTRACT

The escalating demand for sophisticated physical security within the digital paradigm necessitates robust multi-point access control solutions. This research presents the architectural design and implementation of a centralized multi-door locking system integrated with biometric authentication and wireless connectivity. The methodology utilizes an integrated systems approach, employing Arduino Uno as the primary controller and ESP8266 for wireless data transmission, interfaced through a dedicated mobile application. Quantitative performance metrics validate the system efficiency, recording an average latency of 1.2 seconds across five access points and a biometric authentication accuracy of 96%. Real-time status notifications were successfully delivered within a two-second threshold, ensuring operational transparency. Analysis identifies network stability as a critical performance determinant, where signal attenuation below -75 dBm significantly impacts responsiveness. The findings suggest that the convergence of mobile biometrics and distributed hardware provides a scalable and cost-effective framework for modern security infrastructures.

This is an open-access article under the [CC BY-SA](#) license



*\*Penulis Koresponden*

Email: bimo.gumelar@ciputra.ac.id

Cara sitasi IEEE::

- 
- [1] A. B. Gumelar, L. Utari, A. Salmanarrizqie, M. Nasir, "Optimization of Latency and Security in Multi-Door Access Control Systems through Centralized Mobile Biometric Verification" *Journal of Artificial Intelligence and Software Engineering (J-AISE)*, vol. 6, no. 2, p. 212-221, Juni 2026. doi:10.30811/jaise.v6i2.9153
- 

## 1. PENDAHULUAN

Di era digital modern, kebutuhan akan sistem keamanan fisik terintegrasi semakin meningkat, terutama di gedung-gedung perumahan dan komersial. Konsep rumah pintar tidak akan lengkap tanpa sistem penguncian pintu otomatis, dan sangatlah penting bahwa sistem tersebut mampu memberikan standar keamanan dan kenyamanan yang tinggi secara bersamaan [1]. Guna memenuhi persyaratan tersebut, teknologi *Internet of Things* (IoT) muncul sebagai standar definitif yang menawarkan fasilitas tangguh untuk pemantauan waktu nyata dan kontrol terpusat [2], [3]. Namun, integrasi teknologi ini harus dilakukan dengan analisis keamanan yang menyeluruh, karena analisis otomatis sering kali menyoroti kerentanan kritis dalam konfigurasi, yang dapat dimanfaatkan dalam domain layanan digital [4]. Berbagai protokol nirkabel, termasuk *MQTT*, *Zigbee*, dan *LoRaWAN*, telah diterima secara luas dalam berbagai penelitian untuk meningkatkan efisiensi komunikasi antarperangkat, terutama dalam konteks keamanan perumahan dan domain lain seperti manajemen energi hibrida [5], [6], [7].

Terlepas dari maturitas protokol tersebut, tantangan kritis tetap bertahan pada aspek latensi sistem selama eksekusi tugas jamak dalam lingkungan sistem tertanam. Bukti ilmiah menunjukkan bahwa implementasi algoritma penjadwalan tugas yang teroptimasi sangat esensial untuk memitigasi keterlambatan transmisi dan menjamin responsivitas sistem [8]. Implementasi sistem kontrol akses saat ini menunjukkan keterbatasan arsitektural yang signifikan. Mayoritas kerangka kerja yang tersedia masih terbatas pada kontrol titik tunggal, yang menyebabkan inefisiensi pada lingkungan yang memerlukan pengelolaan akses jamak [9], [10]. Keterbatasan ini semakin diperparah oleh penggunaan teknologi yang kurang optimal. Misalnya, sistem berbasis *RFID* dan *Bluetooth* memiliki jangkauan yang terbatas, yang membuatnya rentan terhadap serangan spoofing, yaitu pemalsuan sinyal untuk mendapatkan akses tanpa izin. Di sisi lain, solusi yang lebih canggih seperti pengenalan wajah memerlukan perangkat keras tambahan, seperti kamera, dsb., agar dapat beroperasi secara efektif [11], [12]. Namun, terlepas dari persyaratan ini, solusi pengenalan wajah, terutama yang digabungkan dengan verifikasi digital, telah menunjukkan kesulitan dalam mempertahankan tingkat akurasi yang tinggi sambil merespons perubahan lingkungan dengan cepat [13].

Kondisi ini, oleh karena itu, menunjukkan adanya kesenjangan yang signifikan dalam literatur. Meskipun otentikasi biometrik, seperti pengenalan sidik jari, sudah umum dan mudah ditemukan di semua perangkat seluler modern, penggunaannya sebagai fitur keamanan utama masih terbatas, terutama dalam kaitannya dengan sistem penguncian multi-pintu [14]. Namun, ini merupakan kondisi kritis, terutama mengingat pengguna Android sangat rentan terhadap berbagai ancaman siber. Oleh karena itu, perlu dipahami perilaku pengguna, termasuk risiko yang mungkin terjadi seperti pencurian data, untuk memastikan keefektifan solusi keamanan berbasis seluler [15]. Berbagai alternatif telah diajukan, seperti penggunaan kode QR [16], pengenalan suara menggunakan NodeMCU [17], dan integrasi sensor lingkungan dengan pemberitahuan dini bahaya [18]. Terlepas dari metode otentikasi yang digunakan, tujuan utamanya selalu untuk meningkatkan efisiensi akses ke ruangan.

Penelitian ini berharap dapat mengisi kesenjangan tersebut dengan merancang sistem penguncian pintu berbasis Android yang mampu mengelola lebih dari satu pintu, dengan proses verifikasi sidik jari dilakukan langsung dari *smartphone* pengguna. Sistem penguncian pintu yang diusulkan tidak hanya memenuhi kebutuhan akan fleksibilitas dalam pengelolaan akses pintu, sebagaimana disebutkan dalam literatur, tetapi juga menawarkan solusi keamanan sidik jari yang komprehensif tanpa memerlukan penggunaan perangkat tambahan. Tujuan utama penelitian ini adalah merancang sistem kontrol akses multi-pintu berbasis Android yang menggunakan verifikasi sidik jari, dengan fasilitas operasi real-time melalui koneksi WiFi. Sistem penguncian pintu yang diusulkan ini diharapkan dapat menawarkan solusi keamanan yang hemat biaya, efisien, dan canggih, terutama dalam situasi yang memerlukan kontrol akses multi-pintu secara bersamaan.

Secara keseluruhan, artikel ini disajikan dalam serangkaian bagian yang mendefinisikan isi dan memandu pembaca melalui proses hingga kesimpulan. Artikel ini diawali dengan Pendahuluan, yang memaparkan latar belakang masalah, tinjauan pustaka singkat mengenai solusi yang ada, serta tujuan penelitian. Bagian selanjutnya adalah Metodologi, yang menjelaskan proses penelitian secara terperinci. Proses tersebut disajikan dalam langkah-langkah berikut: identifikasi masalah, studi literatur, rekayasa persyaratan, desain arsitektur sistem, dan skenario pengujian. Bagian selanjutnya adalah hasil penelitian, yang disajikan dalam bagian Hasil dan Pembahasan. Di sini, hasil fungsional sistem disajikan. Hasil tersebut mencakup

analisis desain UML, implementasi antarmuka, dan analisis kuantitatif terhadap kinerja sistem secara keseluruhan. Akhirnya, artikel ini disimpulkan dalam bagian Kesimpulan, di mana hasil penelitian dirangkum secara singkat dan rekomendasi untuk pengembangan sistem di masa depan diberikan.

## 2. METODE

Metodologi yang digunakan dalam pelaksanaan penelitian ini telah dirancang dengan matang dan memastikan bahwa proses pengembangan tetap berjalan sesuai rencana sepanjang penelitian. Metodologi tersebut dibagi menjadi enam tahap utama, yaitu identifikasi masalah, tinjauan pustaka, rekayasa persyaratan, perancangan sistem, implementasi perangkat keras dan perangkat lunak, serta pengujian fungsional.

### 2.1. Identifikasi Masalah

Penelitian ini diawali dengan identifikasi masalah utama yang terkait dengan sistem penguncian pintu yang saat ini digunakan. Telah diamati bahwa terdapat sejumlah keterbatasan dalam sistem ini, seperti ketidakmampuan untuk mengendalikan beberapa pintu sekaligus, kurangnya integrasi dengan teknologi digital seperti aplikasi Android, serta tidak adanya sistem keamanan tambahan yang didasarkan pada teknologi biometrik seperti sidik jari. Keterbatasan-keterbatasan ini menjadi landasan untuk mengembangkan sistem penguncian pintu yang didasarkan pada teknologi Android dan pemindaian sidik jari.

### 2.2. Tinjauan Pustaka

Eksplorasi literatur mengungkapkan adanya kesenjangan fungsional dalam pengembangan sistem keamanan berbasis IoT. Kerangka kerja sistem SAFE yang memanfaatkan algoritma *Haar Cascade* dan *Local Binary Pattern Histogram* (LBPH) pada platform Raspberry Pi memberikan inovasi pada aspek pengenalan wajah [19]. Implementasi serupa menggunakan protokol WebSocket pada modul ESP32-CAM menunjukkan stabilitas komunikasi yang baik untuk deteksi wajah, namun memerlukan komputasi yang intensif dibandingkan dengan verifikasi biometrik sidik jari [3]. Meskipun demikian, solusi-solusi tersebut sering kali bersifat monolitik untuk satu titik akses dan belum mengoptimalkan mobilitas perangkat seluler. Sebagai perbandingan, optimalisasi efisiensi pada sistem autentikasi seluler terbukti mampu mereduksi hambatan operasional dan meningkatkan kepuasan pengguna dalam manajemen akses digital [20].

Penggunaan RFID dan WiFi juga telah diusulkan, namun tetap rentan terhadap risiko duplikasi fisik perangkat akses [21]. erentanan ini menuntut adanya mekanisme pemantauan kinerja jaringan yang ketat guna memastikan distribusi notifikasi peringatan berjalan secara konsisten dan aman [22]. Selain itu, tantangan latensi pada transmisi data nirkabel menjadi variabel kritis yang memerlukan algoritma penjadwalan teroptimasi guna memitigasi keterlambatan respons pada sistem tertanam [8].

Dalam studi sebelumnya, sistem penguncian pintu dengan dukungan pengenalan suara dan NodeMCU ESP8622 telah diajukan sebagai alternatif solusi [17]. Namun, model tersebut belum sepenuhnya mengintegrasikan pemantauan keamanan waktu nyata yang mampu memberikan respons instan terhadap anomali di lingkungan operasional [23]. Studi lain juga menerapkan metode Quality Function Deployment untuk menganalisis persyaratan sistem yang diusulkan secara sistematis [24].

Berdasarkan pembahasan ini, sangat jelas bahwa sistem yang diusulkan, dengan dukungan aplikasi Android serta fitur autentikasi sidik jari yang tersedia pada ponsel pintar itu sendiri, merupakan solusi yang paling reliabel, aman, dan tepat bagi manajemen akses multi-pintu.

### 2.3. Rekayasa Persyaratan

Berdasarkan tinjauan pustaka yang ada, telah diidentifikasi bahwa sistem Android terintegrasi akan menjadi solusi yang tepat untuk masalah ini. Untuk mewujudkan solusi ini, tim proyek telah mengidentifikasi persyaratan sistem dalam tiga bidang utama: perangkat keras, perangkat lunak, dan data. Untuk masing-masing bidang tersebut, telah ditetapkan spesifikasi teknis minimum, sebagaimana disajikan pada Tabel 1.

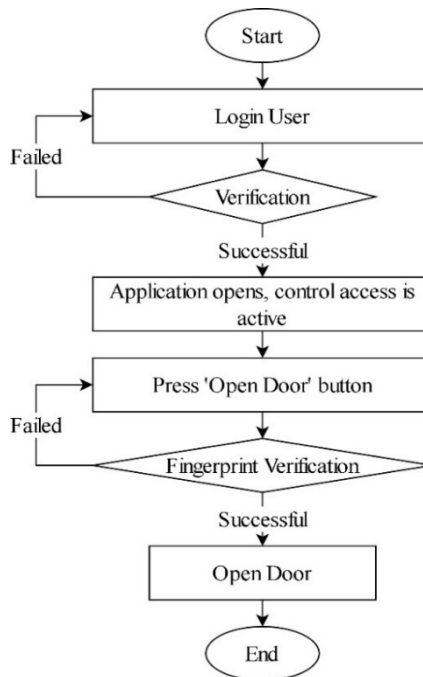
Tabel 1. Persyaratan Perangkat Keras dan Perangkat Lunak

| Jenis Persyaratan | Rincian                                                                                                               |
|-------------------|-----------------------------------------------------------------------------------------------------------------------|
| <i>Hardware</i>   | Laptop (Intel i5, RAM 8 GB), prototipe pintu berbasis <i>Arduino</i> , ponsel pintar Android dengan sensor sidik jari |
| <i>Software</i>   | Windows 10, Android Studio, Visual Studio Code                                                                        |
| <i>Data</i>       | Data sidik jari pengguna, informasi akun pengguna                                                                     |

Tiga bidang, yaitu perangkat keras, perangkat lunak, dan data, dapat dianggap sebagai pilar-pilar yang menjadi landasan fase pengembangan sistem ini, serta fase pengujian. Ketiga bidang tersebut telah dikembangkan untuk memastikan bahwa setiap aspek sistem ini dirancang guna mencapai tujuan utama penelitian ini, yaitu meningkatkan efisiensi dan keamanan dalam sistem kontrol akses multi-pintu.

## 2.4. Perancangan dan Pengembangan Aplikasi

Setelah spesifikasi persyaratan ditetapkan, proyek dilanjutkan ke tahap perancangan. Proses perancangan sistem dimulai dengan pemodelan alur kerja berdasarkan pendekatan prototipe, seperti yang ditunjukkan pada Gambar 1.



Gambar 1. Model proses sistem penguncian pintu otomatis (Prototipe)

Untuk antarmuka pengguna, digunakan pendekatan desain yang berpusat pada pengguna, dengan tujuan agar pengguna dapat berinteraksi dengan kontrol pintu secara intuitif. Pada saat yang sama, desain basis data relasional dilakukan menggunakan arsitektur MySQL, dengan tujuan menggunakan basis data tersebut sebagai tempat penyimpanan data pengguna serta riwayat penggunaan pintu. Penggunaan basis data ini juga memungkinkan pertukaran data antara aplikasi dan perangkat secara efisien. Untuk proses otentikasi, digunakan sensor sidik jari pada perangkat Android.

## 2.5. Implementasi

Setelah arsitektur sistem dan desain antarmuka selesai, sistem tersebut diimplementasikan baik secara fisik maupun fungsional. Pada tahap implementasi, mikrokontroler Arduino Uno berfungsi sebagai pengendali sistem, sedangkan modul ESP8266 bertindak sebagai jembatan antara perangkat keras dan aplikasi Android. Aplikasi tersebut dikembangkan menggunakan Android Studio dengan bahasa pemrograman Java. Fitur utama aplikasi meliputi pendaftaran pengguna, pemindaian sidik jari menggunakan API Android, dan pengendalian pintu melalui jaringan nirkabel.

## 2.6. Pengujian

Sistem akhir tersebut kemudian menjalani evaluasi menyeluruh. Pengujian dilakukan untuk mengevaluasi kinerja dan keandalan sistem secara keseluruhan. Pendekatan terstruktur dalam pengujian diperlukan untuk memastikan validitas fungsional yang tinggi. Sebagai contoh, penerapan pengujian kotak hitam dengan menggunakan metode *Equivalence Partitioning* terbukti efektif dalam mengidentifikasi celah dalam integrasi sistem serta menguji fitur validasi input pada lingkungan sistem yang kompleks [25]. Parameter pengujian dikembangkan secara sistematis dan disajikan dalam Tabel 2.

Tabel 2. Parameter Pengujian Sistem

| Parameter yang diuji     | Indikator                                                       |
|--------------------------|-----------------------------------------------------------------|
| Waktu respons sistem     | Kecepatan pembukaan/penguncian pintu (dalam milidetik)          |
| Akurasi otentikasi       | Jumlah otentikasi yang berhasil dibandingkan dengan total upaya |
| Stabilitas pemberitahuan | Konsistensi pemberitahuan real-time yang diterima pengguna      |

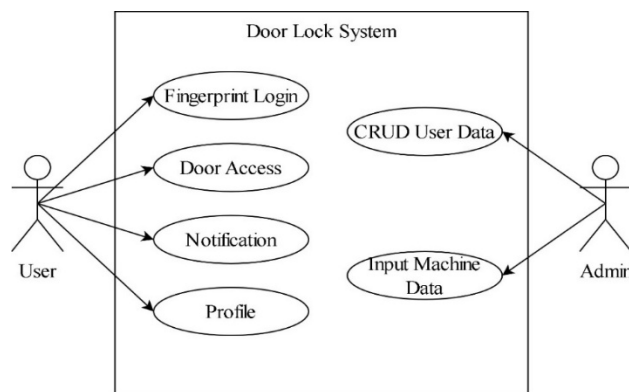
Parameter-parameter tersebut dievaluasi dalam berbagai skenario penggunaan untuk memastikan bahwa sistem tersebut stabil dan andal dalam kondisi penggunaan di dunia nyata.

### 3. HASIL DAN PEMBAHASAN

Berdasarkan metodologi yang telah dijabarkan pada bagian sebelumnya, bagian ini difokuskan pada penyajian hasil penelitian. Hal ini dilakukan melalui analisis desain dan arsitektur sistem dengan menggunakan pemodelan UML. Selanjutnya, dibahas pula analisis implementasi antarmuka aplikasi serta evaluasi fungsional sistem. Selain itu, bagian ini juga mencakup analisis kelebihan dan kekurangan sistem, serta implikasi dan prospek pengembangan di masa mendatang.

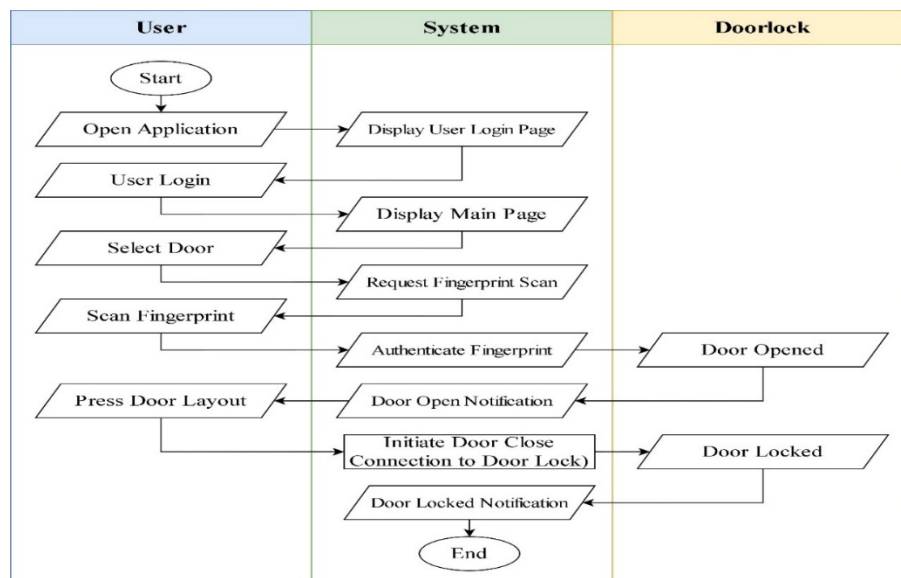
#### 3.1. Desain Sistem dan Analisis Struktur Berbasis UML

*Use case diagram* yang ditampilkan pada Gambar 2 mengidentifikasi area interaksi utama antara pengguna dan sistem penguncian otomatis. Persyaratan ditentukan dengan mengidentifikasi area interaksi dengan aktor utama serta area fungsionalitas utama, seperti pendaftaran pengguna, verifikasi sidik jari, dan pemantauan status pintu. Hal ini memastikan bahwa fungsionalitas sistem selaras dengan tujuan penelitian untuk mengembangkan sistem multi-pintu yang efisien dan efektif.



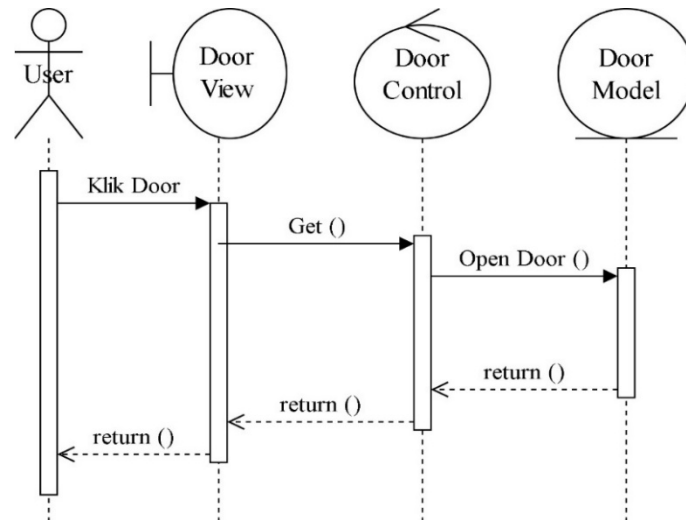
Gambar 2. Use Case Diagram Aplikasi

*Activity diagram* yang ditunjukkan pada Gambar 3, merupakan representasi visual terperinci dari seluruh alur kerja dan logika internal aplikasi. Diagram ini secara jelas menggambarkan semua proses langkah demi langkah dalam sistem, termasuk keputusan percabangan kritis seperti yang berkaitan dengan hasil pemindaian biometrik yang berhasil atau gagal. Diagram ini sangat penting dalam memahami perilaku dinamis sistem, termasuk proses-proses seperti masukan awal pengguna melalui antarmuka Android, hingga eksekusi fisik akhir perintah penguncian pintu.



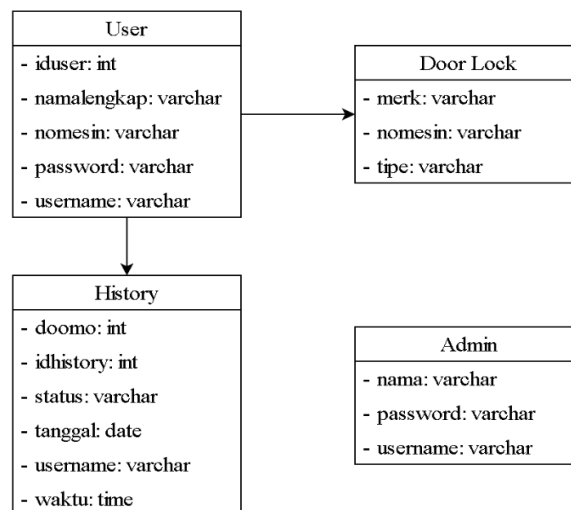
Gambar 3. Activity Diagram Aplikasi

*Sequence diagram* yang ditunjukkan pada Gambar 4, merupakan representasi dari alur komunikasi kronologis antara berbagai objek dan komponen dalam jaringan terintegrasi. Diagram ini menyoroti urutan komunikasi pesan antara berbagai komponen sistem, seperti aplikasi Android, modul WiFi ESP8266, dan pengontrol Arduino Uno, selama operasi waktu nyata. Hal ini sangat penting untuk memastikan bahwa komunikasi data yang berkaitan dengan verifikasi biometrik dilakukan dengan latensi minimal.



Gambar 4. Sequence Diagram Aplikasi

*Class diagram* seperti yang ditunjukkan pada Gambar 5 di atas menjelaskan struktur statis perangkat lunak dengan mengidentifikasi entitas-entitas utama dan hubungan antarentitas yang terkait. Arsitektur sistem ini memiliki kelas-kelas utama seperti *User*, *DoorLock*, *History*, dan *Admin*. Kelas-kelas ini saling terkait untuk pengelolaan izin akses sistem yang efektif serta pencatatan informasi riwayat sistem.



Gambar 5. Class Diagram Aplikasi

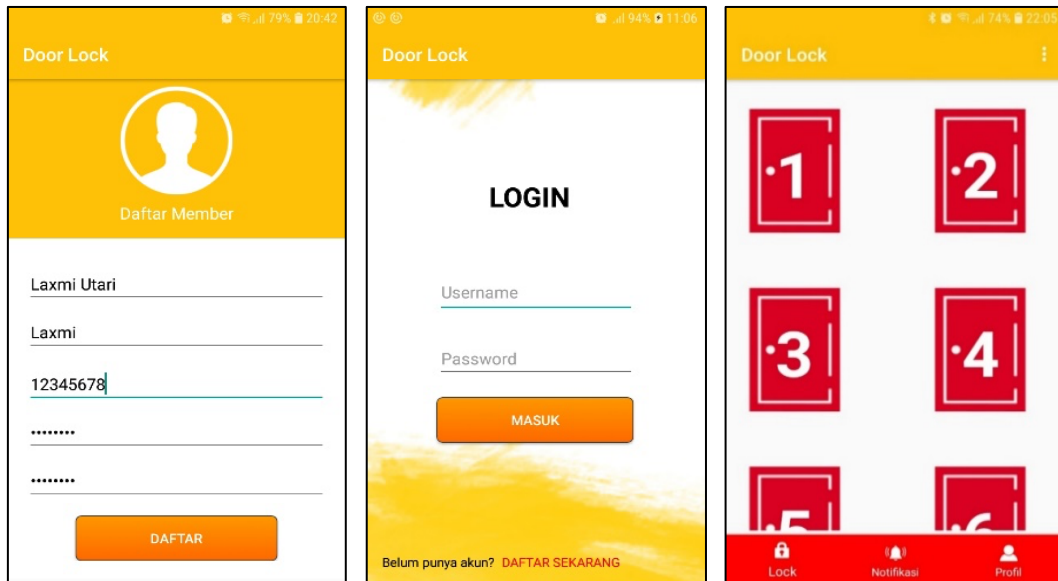
Pemodelan yang komprehensif yang ditampilkan dalam keempat *UML diagram* di atas memberikan landasan teoretis bagi pengembangan fisik sistem. Tahap perancangan dalam proses pengembangan sangat penting karena tahap ini mengidentifikasi semua persyaratan sebelum proses pemrograman dan integrasi perangkat keras dilakukan. Pendekatan ini meminimalkan kesalahan dalam arsitektur sistem serta memberikan kerangka kerja yang efektif untuk pengembangan antarmuka pengguna dan pengujian kinerja sistem.

### 3.2. Implementasi Aplikasi dan Evaluasi Fungsional

Setelah arsitektur sistem didefinisikan berdasarkan *UML diagram*, tahap selanjutnya adalah mengubah aplikasi menjadi implementasi sistem yang berfungsi.

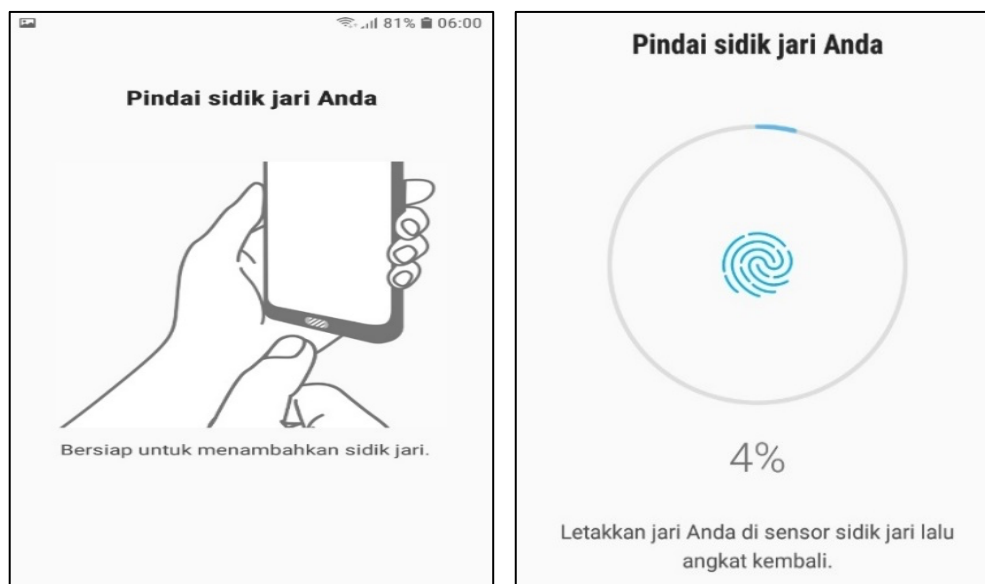
#### 3.2.1. Implementasi Antarmuka Aplikasi

Sistem ini telah diimplementasikan menggunakan lingkungan Android Studio dengan menyertakan beberapa antarmuka layar utama yang ramah pengguna, seperti yang ditunjukkan pada alur kerja sistem pada Gambar 6. Pada tahap pertama alur kerja sistem (Gambar 6, kiri), pengguna diharuskan mendaftarkan akun menggunakan halaman pendaftaran. Setelah tahap pendaftaran, pengguna diberi opsi untuk masuk menggunakan halaman login (Gambar 6, tengah) guna memanfaatkan fitur-fitur utama aplikasi. Setelah tahap login, pengguna diarahkan ke halaman utama aplikasi (Gambar 6, kanan), yang menampilkan tata letak untuk kontrol akses pintu-pintu yang terdaftar.



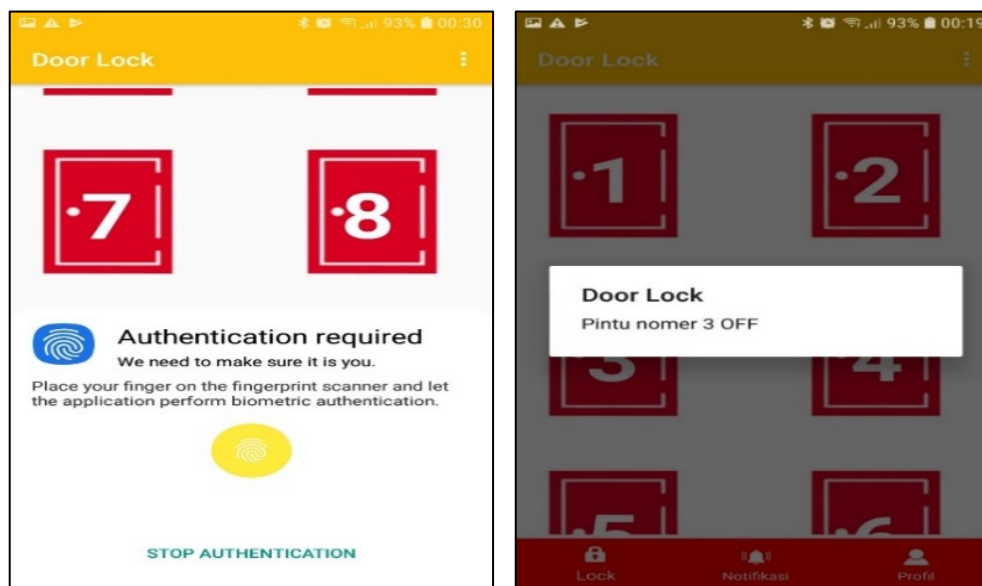
Gambar 6. Halaman Pendaftaran (Kiri) dan Halaman Masuk (Tengah), serta Tata Letak Kontrol Pintu (Kanan)

Prosedur pendaftaran sidik jari dimulai segera setelah pengguna mengaktifkan dan mengonfigurasi fitur keamanan. Saat prosedur konfigurasi dimulai, akan muncul pemberitahuan *pop-up*, seperti yang ditunjukkan pada Gambar 7 (Kiri), yang meminta pengguna untuk mulai memindai sidik jarinya. Setelah itu, antarmuka akan memandu pengguna melalui serangkaian langkah tentang cara meletakkan sidik jari pada sensor, seperti yang digambarkan pada Gambar 7 (Kanan).



Gambar 7. Pemberitahuan Pemindaian Sidik Jari (Kiri) dan Pendaftaran Sidik Jari (Kanan)

Ke depannya, untuk setiap upaya pengguna lainnya dalam mengakses pintu mana pun, pengguna akan diminta untuk memilih pintu yang ingin diakses. Setelah memilih pintu, sistem akan menginisiasi permintaan verifikasi pengguna, seperti yang ditunjukkan pada Gambar 8 (Kiri), untuk memastikan identitasnya. Setelah verifikasi berhasil, sistem akan menjalankan perintah, baik untuk membuka maupun mengunci pintu, dan kemudian mengirimkan pemberitahuan real-time mengenai status pintu, seperti yang ditunjukkan pada Gambar 8 (Kanan).



Gambar 8. Permintaan Sidik Jari (Kiri) dan Pemberitahuan Pintu Terkunci (Kanan)

Komponen antarmuka ini memastikan bahwa proses otentikasi biometrik bersifat intuitif dan aman bagi pengguna akhir. Dengan memberikan umpan balik visual yang jelas selama fase pemindaian dan pelaksanaan perintah, aplikasi ini menjaga tingkat transparansi yang tinggi terkait status sistem. Dengan terintegrasinya komponen aplikasi dan perangkat keras secara penuh, penelitian dilanjutkan ke serangkaian evaluasi yang ketat untuk memverifikasi keandalan dan kinerja sistem secara keseluruhan dalam skenario dunia nyata.

### 3.2.2. Evaluasi Fungsi Sistem

Setelah mengimplementasikan antarmuka aplikasi, dilakukan pengujian fungsional untuk mengevaluasi kinerja sistem. Berdasarkan hasil yang disajikan pada Tabel 3, terlihat bahwa kinerja sistem memuaskan. Waktu respons rata-rata sebesar 1,2 detik menunjukkan bahwa sistem mampu beroperasi secara real-time. Selain itu, keandalan otentikasi sidik jari mencapai 96%, yang menandakan bahwa sistem ini dapat diandalkan dalam melakukan otentikasi biometrik. Hal ini sejalan dengan studi sebelumnya [24], meskipun sistem yang diusulkan ini menambahkan aspek otentikasi biometrik. Dibandingkan dengan sistem berbasis teknologi RFID [21], sistem yang diusulkan ini memiliki beberapa keunggulan karena tidak memerlukan media fisik yang berisiko hilang. Selain itu, hasil penelitian ini mengonfirmasi temuan sebelumnya oleh [19], yang menekankan perlunya sistem kontrol akses terintegrasi dengan antarmuka digital yang ramah pengguna.

Tabel 3. Analisis Hasil Uji Fungsi Sistem

| Parameter                      | Hasil Pengamatan                                       |
|--------------------------------|--------------------------------------------------------|
| Waktu respons rata-rata        | 1,2 detik (rata-rata dari 5 pintu dalam 10 sesi)       |
| Keberhasilan otentikasi        | 24 dari 25 upaya berhasil (96%)                        |
| Pemberitahuan <i>real-time</i> | Diterima dalam waktu maksimal 2 detik setelah eksekusi |
| Stabilitas koneksi WiFi        | Menurun ketika sinyal < -75 dBm                        |

Data kuantitatif yang diperoleh dari pengujian ini menunjukkan keefektifan solusi keamanan multi-pintu secara keseluruhan dalam menjaga responsivitas real-time dan akurasi tinggi pada otentikasi biometrik. Meskipun parameter kinerja inti berhasil memenuhi tujuan penelitian awal, ketergantungan yang teramat terhadap kekuatan sinyal menegaskan pentingnya kualitas infrastruktur jaringan. Temuan empiris ini memberikan gambaran menyeluruh mengenai kinerja operasional sistem, yang mengarah pada evaluasi lebih mendetail mengenai kelebihan dan keterbatasan spesifik yang teridentifikasi selama proses implementasi.

### 3.2.3. Kelebihan dan Keterbatasan Sistem

Berdasarkan hasil yang diperoleh dari evaluasi fungsional, kami dapat mengidentifikasi berbagai kelebihan dan keterbatasan yang terkait dengan pengembangan sistem penguncian pintu. Sistem penguncian pintu yang diusulkan memiliki beberapa kelebihan. Misalnya, sistem ini memberikan efisiensi operasional. Hal ini karena sistem memungkinkan pengguna untuk mengoperasikan beberapa pintu menggunakan satu antarmuka. Kedua, sistem ini menyediakan fitur keamanan tambahan. Hal ini karena sistem menggunakan teknologi sidik jari untuk tujuan otentikasi. Teknologi sidik jari sulit untuk dipalsukan. Terakhir, sistem ini menggunakan pendekatan modular. Artinya, sistem ini dapat diskalakan dan dapat ditingkatkan di masa depan tanpa perlu perancangan ulang yang besar.

Namun, sistem yang diusulkan memiliki beberapa keterbatasan. Misalnya, sistem ini memiliki masalah kompatibilitas perangkat. Sistem ini bekerja dengan baik pada perangkat Android yang dilengkapi dengan teknologi sidik jari. Kedua, sistem ini memiliki keterbatasan terkait stabilitas jaringan WiFi. Kinerja sistem sangat bergantung pada kualitas jaringan WiFi. Kinerja sistem terganggu ketika kekuatan sinyal jaringan WiFi turun di bawah -75 dBm.

### 3.2.4. Implikasi dan Potensi Pengembangan

Terlepas dari keterbatasannya, hasil penelitian dan konsep desain modular ini menawarkan berbagai peluang untuk pengembangan di masa depan. Hasil penelitian ini memiliki implikasi potensial bagi pengembangan sistem yang lebih tangguh dan serupa di bidang yang sama. Dalam hal pengembangan di masa depan, diajukan sejumlah rekomendasi. Hal ini mencakup integrasi IoT dengan sensor tambahan seperti kamera dan sistem alarm. Selain itu, kontrol akses berbasis cloud direkomendasikan untuk menyederhanakan administrasi. Penggunaan berbagai protokol komunikasi nirkabel seperti LoRaWAN dan Zigbee direkomendasikan untuk meningkatkan redundansi dan mengurangi ketergantungan pada WiFi. Peluang pengembangan lebih lanjut mencakup perluasan sistem untuk mendukung platform iOS guna memperluas jangkauan basis pengguna. Selain itu, penerapan enkripsi ujung-ke-ujung direkomendasikan untuk meningkatkan keamanan transfer data antara pengirim dan penerima data.

## 4. KESIMPULAN

Implementasi sistem penguncian pintu otomatis berbasis Android yang terintegrasi dengan autentikasi biometrik sidik jari dan protokol komunikasi nirkabel telah berhasil direalisasikan. Arsitektur sistem ini secara efektif mensintesis kontrol akses multi-titik melalui sinkronisasi antara mikrokontroler Arduino Uno, modul ESP8266, dan aplikasi seluler terpusat. Keberhasilan pengembangan ini membuktikan bahwa integrasi teknologi biometrik pada perangkat seluler mampu meningkatkan standar keamanan fisik sekaligus efisiensi operasional dalam manajemen akses gedung.

Evaluasi sistemik menunjukkan bahwa kinerja operasional selaras dengan parameter teknis yang ditetapkan pada fase perancangan awal. Data empiris mencatat latensi rata-rata sebesar 1,2 detik dalam eksekusi perintah pada lima titik akses dengan tingkat akurasi verifikasi biometrik mencapai 96%. Selain itu, mekanisme notifikasi waktu nyata terbukti stabil dengan distribusi informasi status yang konsisten berada dalam ambang batas dua detik. Temuan ini mengonfirmasi bahwa arsitektur yang diusulkan memiliki reliabilitas yang memadai untuk aplikasi keamanan kontemporer.

Meskipun menunjukkan performa yang solid, analisis mengidentifikasi bahwa keandalan sistem memiliki ketergantungan kritis terhadap stabilitas intensitas sinyal nirkabel, di mana atenuasi sinyal di bawah -75 dBm berdampak pada responsivitas perangkat. Oleh karena itu, penelitian mendatang disarankan untuk mengeksplorasi diversifikasi protokol komunikasi *Internet of Things* (IoT) guna meningkatkan redundansi jaringan. Prospek pengembangan selanjutnya juga mencakup ekspansi kompatibilitas sistem ke platform iOS serta integrasi algoritma enkripsi yang lebih lanjut untuk memperkuat integritas transmisi data pada infrastruktur skala besar.

## REFERENSI

- [1] L. Leung and M. Cheung, "The effects of technology readiness, risks, and benefits on smart home technology adoption: extending the Theory of Planned Behavior model," *Media Asia*, vol. 52, no. 1, pp. 80–101, Jan. 2025, doi: 10.1080/01296612.2024.2330771.
- [2] V. Nastiti, N. H. Cahyadi, and M. A. Jasmine, "Rancang bangun sistem monitoring kelelahan dan tracking pekerja konstruksi melalui safety vest berbasis iot," *NJCA (Nusantara J. Comput. Its Appl.)*, vol. 8, no. 2, pp. 39–46, 2023, doi: njca.v8i2.321.g116.
- [3] Safridi, M. Nasir, and U. Erdiansyah, "Implementation of WebSocket in an IoT-Based Smart Home Door Security System Using ESP32-CAM with Face Recognition," *J. Artif. Intell. Softw. Eng.*, vol. 6, no. 1, pp. 55–67, 2026, doi: 10.30811/jaise.v6i1.9052.
- [4] Rayhan Maulana and A. D. Wiranata, "Analisis Serangan Siber Di Website UHAMKA Dengan Metode Penetration Testing," *IDEALIS Indones. J. Inf. Syst.*, vol. 9, no. 1 SE-Table of Content, pp. 113–123, Feb. 2026, [Online]. Available: <https://jom.fti.budiluhur.ac.id/IDEALIS/article/view/3693>
- [5] M. Sayeduzzaman, T. Hasan, A. A. Nasser, and A. Negi, "An Internet of Things-Integrated Home Automation with Smart Security System," in *Automated Secure Computing for Next-Generation Systems*, 2024, pp. 243–273. doi: <https://doi.org/10.1002/9781394213948.ch13>.
- [6] F. Azzedin and T. Alhazmi, "Secure Data Distribution Architecture in IoT Using MQTT," *Appl. Sci.*, vol. 13, no. 4, pp. 1–13, 2023, doi: 10.3390/app13042515.
- [7] N. Afiyat and M. Muhtaromin, "Sistem Kontrol dan Monitoring Berbasis IoT pada Off-Grid Hybrid Power System PLTS-PLN," *NJCA (Nusantara J. Comput. Its Appl.)*, vol. 10, no. 1, pp. 9–17, Jun. 2025, doi: 10.36564/njca.v10i1.404.
- [8] B. Septian, A. Adrianda, M. F. Ridho, and M. Misbahuddin, "An IoT-Enabled Low Latency Automatic Identification System Using Round-Robin Scheduling Algorithm," *J. Artif. Intell. Softw. Eng.*, vol. 5, no. 2, pp. 403–409, 2025, doi: 10.30811/jaise.v5i2.6512.
- [9] W. Wang *et al.*, "Simultaneous Data Dissemination Among WiFi and ZigBee Devices," *IEEE/ACM Trans. Netw.*, vol. 31, no. 6, pp. 2545–2558, 2023, doi: 10.1109/TNET.2023.3243070.
- [10] I. P. B. E. Permadi, A. B. Gumelar, and A. Widodo, "Sistem Pengunci Multi Pintu dengan Mikrokontroler Arduino Mega 2560

- R3,” *Jetri J. Ilm. Tek. Elektro*, pp. 47–56, Aug. 2019, doi: 10.25105/jetri.v17i1.4445.
- [11] I. K. A. Enriko, F. N. Gustiyana, G. H. Fahreja, and G. C. Giri, “LoRaWAN Network Planning for ODP Door Monitoring in Banyumas Districts,” *Jaict*, vol. 8, no. 1, p. 140, 2023, doi: 10.32497/jaict.v8i1.3939.
- [12] S. Soni, R. Soni, and A. A. Wao, “RFID-Based Digital Door Locking System,” *Indian J. Microprocess. Microcontroller*, vol. 1, no. 2, pp. 17–21, 2021, doi: 10.54105/ijmm.b1707.091221.
- [13] T. H. R. Bakar and A. D. Wowor, “Implementasi Algoritma Face Recognition Menggunakan Face-API.js Pada Sistem Verifikasi SIM Digital,” *IDEALIS Indones. J. Inf. Syst.*, vol. 8, no. 2 SE-Table of Content, pp. 236–247, Jul. 2025, doi: 10.36080/idealis.v8i2.3546.
- [14] S. Mulyati and S. Sadi, “IoT on Door Security Control Prototypes based RFID and Bluetooth,” *J. Tek.*, vol. 8, no. 2, pp. 2–7, 2019, doi: 10.31000/jt.v8i2.1527.
- [15] D. F. Tanjung and W. Wella, “PENGUKURAN KEAMANAN PENGGUNA ANDROID MENGGUNAKAN EXPECTACY BASED MODEL DAN ALTERNATIVE THREAT BASED MODEL,” *IDEALIS Indones. J. Inf. Syst.*, vol. 8, no. 1, pp. 150–159, Feb. 2025, doi: 10.36080/idealis.v8i1.3180.
- [16] H. Heriansyah, R. E. R, D. A. S, and S. ISTIQHARA, “Sistem Kunci Pintu Otomatis Kelas Perkuliahan Berbasis Android Terintegrasi Sistem Informasi Akademik,” *MIND J.*, vol. 5, no. 2, pp. 121–134, Jul. 2021, doi: 10.26760/mindjournal.v5i2.121-134.
- [17] S. Achmady, L. Qadriah, and A. Auzan, “Rancang Bangun Magnetic Solenoid Door Lock Dengan Speech Recognition Menggunakan NodeMCU Berbasis Android,” *J. Real Ris.*, vol. 4, no. 2, pp. 79–91, Jul. 2022, doi: 10.47647/jrr.v4i2.636.
- [18] S. Siswanto, M. Anif, D. N. Hayati, and Y. Yuhefizar, “Pengamanan Pintu Ruangan Menggunakan Arduino Mega 2560, MQ-2, DHT-11 Berbasis Android,” *J. RESTI (Rekayasa Sist. dan Teknol. Informasi)*, vol. 3, no. 1, pp. 66–72, Apr. 2019, doi: 10.29207/resti.v3i1.797.
- [19] J.-H. Leim, K.-W. Ng, A. S., S.-L. Ng, and S.-C. Haw, “SAFE: Security Door Lock System Using Haar-Cascade and LBPH Method,” *Appl. Comput. Eng.*, vol. 2, no. 1, 2023, doi: 10.54254/2755-2721/2/20220646.
- [20] R. Fitria, I. Sahputra, and R. Maulana, “Optimization of Employee Attendance System Using Face Recognition and Geotagging Based on Mobile Android,” *J. Artif. Intell. Softw. Eng.*, vol. 5, no. 2, pp. 510–527, 2025, doi: 10.30811/jaise.v5i2.6892.
- [21] S. Ramadhani and D. P. Putri, “Design of a Home Door Security System Based on NodeMCU ESP32 Using a Magnetic Reed Switch Sensor and Telegram Bot Application,” *Sinkron*, vol. 8, no. 4, pp. 2059–2068, 2023, doi: 10.33395/sinkron.v8i4.12688.
- [22] M. Munawir, K. Muttaqin, and W. Rezeki, “Implementation of Network Performance Monitoring (NPM) in Nagios for Sending Alert Via Telegram Notification Via Telegram,” *J. Artif. Intell. Softw. Eng.*, vol. 5, no. 1, p. 283, 2025, doi: 10.30811/jaise.v5i1.6516.
- [23] M. Alvian, B. Prastya, J. Maulindar, and E. Purwanto, “IoT-Based Real-Time Security System Implementation at Kaka Game Center Internet Café Informasi Artikel ABSTRAK,” *J. Artif. Intell. Softw. Eng.*, vol. 5, no. 3, pp. 1096–1108, 2025, doi: 10.30811/jaise.v5i3.7327.
- [24] I. Maulana, E. Azriadi, and J. Musrido, “Rancang Bangun Sistem Smart Door Lock Menggunakan Mikrokontroler Esp32 Berbasis Internet Of Things (Iot) dan Smartphone Android,” *J. Tek. Ind. Terintegrasi*, vol. 6, no. 1, pp. 195–208, Jun. 2023, doi: 10.31004/jutin.v6i1.15123.
- [25] M. B. Abdurrohman, D. H. H. Putra, R. D. Pramono, M. Z. Algifari, S. Indriasari, and M. Nasir, “Implementasi Equivalence Partitioning untuk Validasi Masukan Pada Situs Web Administrator Fishomie,” *IDEALIS Indones. J. Inf. Syst.*, vol. 9, no. 1 SE-Table of Content, pp. 124–132, Jan. 2026, doi: 10.36080/idealis.v9i1.3631.