

SISTEM MONITORING KEAMANAN RUMAH MENGUNAKAN *FINGERPRINT* DAN *FACE* *RECOGNITION* BERBASIS *MACHINE LEARNING*

Siti Allanurin ^{1*}, Yusuf Muharam ²

^{1,2} Teknik Informatika, Universitas Bale Bandung, Bandung, Indonesia.

Email: stallanr571@gmail.com*

ABSTRAK

Keamanan rumah merupakan aspek penting dalam membatasi dan mengontrol akses masuk dengan efektif. Terdapat banyak kasus pembobolan rumah yang terjadi akibat penggunaan sistem kunci konvensional yang tidak lagi mampu untuk memberi perlindungan optimal. Penelitian ini merancang dan membangun sistem monitoring keamanan rumah berbasis *Internet Of Things* (IoT) menggunakan autentikasi biometrik *Fingerprint* dan *Face Recognition*. Sensor *Fingerprint* AS608 digunakan dengan algoritma *Minutiae-Based Matching* yang telah terdapat di dalam sensor tersebut, dan *Face Recognition* dikembangkan menggunakan metode *Machine Learning* berbasis *Local Binary Patterns Histogram* (LBPH). Sistem diintegrasikan dengan mikrokontroler ESP32, kamera CCTV, serta notifikasi *WhatsApp* otomatis untuk memberikan peringatan ketika terjadi akses ilegal. *Website Dashboard* dikembangkan menggunakan Flask dan Tailwind CSS untuk menampilkan status autentikasi dan aktivitas secara real-time. Hasil pengujian menunjukkan bahwa sensor *Fingerprint* mencapai akurasi 90%, sedangkan *Face Recognition* optimal pada jarak 30 cm dengan tingkat keberhasilan 90%. Notifikasi *WhatsApp* berhasil dikirim dengan delay rata-rata ± 1 detik. Sistem ini terbukti efektif untuk meningkatkan keamanan rumah dengan pemantauan *real-time* dan autentikasi ganda berbasis biometrik.

Kata Kunci: *Face Recognition; Fingerprint; Internet of Things; Machine Learning; Sistem monitoring*

ABSTRACT

Home security is an important aspect in limiting and controlling access effectively. Many home intrusion cases occur due to the use of conventional locking systems that are no longer capable of providing optimal protection. This research designs and develops a home security monitoring system based on the *Internet of Things* (IoT) using biometric authentication through *Fingerprint* and *Face Recognition*. The AS608 fingerprint sensor is implemented with the built-in *Minutiae-Based Matching* algorithm, while *Face Recognition* is developed using a *Machine Learning* approach based on *Local Binary Patterns Histogram* (LBPH). The system is integrated with an ESP32 microcontroller, CCTV camera, and automated *WhatsApp* notifications to provide alerts when unauthorized access is detected. A web-based dashboard is developed using Flask and Tailwind CSS to display real-time authentication status and activity monitoring. Experimental results show that the fingerprint sensor achieves an accuracy of 90%, while *Face Recognition* performs optimally at a distance of 30 cm with a 90% success rate. *WhatsApp* notifications are successfully delivered with an average delay of approximately ± 1 second. The system is proven to be effective in enhancing home security through real-time monitoring and dual biometric authentication.

Keywords: *Face Recognition; Fingerprint; Internet of Things; Machine Learning; Monitoring System*

1. Pendahuluan

Keamanan rumah merupakan aspek fundamental dalam menjaga kenyamanan dan keselamatan penghuni. Namun, mayoritas masyarakat masih mengandalkan kunci konvensional yang rentan hilang, di duplikasi, serta tidak mampu mendeteksi upaya akses ilegal, sehingga meningkatkan risiko pencurian dan pembobolan (Nasir & Al Gifari, 2024). Sistem keamanan modern berbasis *Internet of Things* (IoT) menawarkan kemudahan pemantauan dan pengendalian akses jarak jauh secara *real-time*, khususnya melalui autentikasi biometrik seperti *Fingerprint* dan *Face Recognition* yang mampu mengenali identitas pengguna dengan tingkat akurasi tinggi (Joevan Maulana Florian et al., 2024).

Desa wargaluyu sebagai wilayah pedesaan yang masih terbatas dalam adopsi teknologi keamanan modern menunjukkan kebutuhan terhadap solusi keamanan rumah yang adaptif dan efisien. Pada penelitian sebelumnya telah mengembangkan sistem keamanan berbasis IoT, seperti integrasi sensor gerak, autentikasi sidik jari, dan notifikasi otomatis (nas Putra & Indah Fenriana, 2024), namun sebagian besar belum menerapkan *Face Recognition* dan belum menyediakan pemantauan terpusat melalui dashboard web sehingga tingkat keamanan belum optimal (Wijaya Setiady & Amanda Ginting, 2023).

Berdasarkan kondisi tersebut, rumusan masalah dalam penelitian ini yaitu bagaimana merancang sistem monitoring keamanan rumah yang mampu memberikan autentikasi ganda dan pemantauan *real-time* untuk mendeteksi akses tidak sah. Penelitian ini bertujuan mengembangkan sistem keamanan rumah berbasis IoT dengan integrasi *Fingerprint* dan *Face Recognition* berbasis *Machine Learning*, dilengkapi notifikasi otomatis ke WhatsApp dan dashboard web untuk pengelolaan akses. Dengan demikian, penelitian ini diharapkan dapat menghasilkan solusi keamanan yang lebih adaptif, akurat, serta mudah digunakan oleh masyarakat terutama di lingkungan pedesaan.

2. Metoda

Penelitian ini menggunakan metode pengembangan *Waterfall* yang terdiri dari tahapan identifikasi masalah, pengumpulan data, analisis kebutuhan, perancangan, implementasi, dan pengujian. Tahapan tersebut menjadi dasar dalam membangun sistem monitoring keamanan rumah berbasis autentikasi biometrik dan *Internet of Things* (IoT).

2.1 Identifikasi Masalah

Tahap ini dilakukan dengan observasi lapangan, wawancara, dan penyebaran kuesioner kepada warga Desa Wargaluyu untuk mengetahui kondisi keamanan rumah. Ditemukan bahwa sistem kunci konvensional tidak memiliki log aktivitas dan rentan terjadi duplikasi kunci.

2.2 Pengumpulan Data

Pengumpulan data dilakukan melalui observasi langsung, wawancara dengan perangkat desa, penyebaran kuesioner kepada masyarakat, serta studi pustaka mengenai *Fingerprint*, *Face Recognition*, IoT ESP32, *WhatsApp API*, dan sistem *dashboard web*.

2.3 Analisis Kebutuhan

Analisis ini mencakup kebutuhan fungsional sistem, yaitu autentikasi *Fingerprint*, *Face Recognition* berbasis algoritma LBPH, pengiriman notifikasi *real-time* melalui *WhatsApp*, dan monitoring aktivitas melalui *dashboard web*. Kebutuhan non-fungsional meliputi perangkat keras (ESP32, sensor *fingerprint* AS608, CCTV, *relay*, *solenoid door lock*, *buzzer*) dan perangkat lunak (Arduino IDE, Flask, MySQL, MQTT, dan API *WhatsApp*).

2.4 Perancangan Sistem

Perancangan dilakukan menggunakan UML (*Use Case Diagram*, *Activity Diagram*, dan *Class Diagram*) serta penyusunan blok diagram untuk menggambarkan hubungan antar komponen sistem. Perangkat keras dirakit berdasarkan skema rangkaian, sedangkan *dashboard web* dirancang menggunakan Figma dan diimplementasikan menggunakan Flask.

2.5 Implementasi Sistem

Mikrokontroler ESP32 diprogram untuk mengelola autentikasi dan kontrol solenoid *door lock*, sementara sistem *Face Recognition* dilatih menggunakan metode LBPH. Sistem dihubungkan melalui jaringan IoT menggunakan protokol MQTT dan dilengkapi notifikasi otomatis melalui *WhatsApp*.

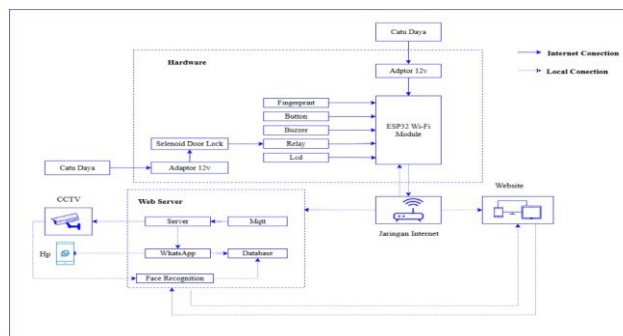
2.6 Pengujian Sistem

Pengujian dilakukan menggunakan metode *Black Box Testing* untuk memastikan semua fungsi berjalan sesuai rancangan, termasuk autentikasi biometrik, kontrol pintu, tampilan log aktivitas pada *dashboard web*, serta pengiriman notifikasi *WhatsApp* secara *real-time*.

3. Hasil dan Pembahasan

3.1 Perancangan Sistem

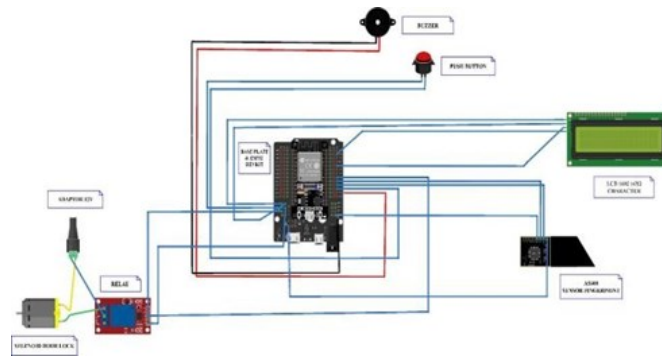
Perancangan sistem mencakup perancangan perangkat keras dan perangkat lunak. Perangkat keras menggunakan ESP32 sebagai mikrokontroler utama yang terhubung dengan sensor *Fingerprint AS608*, kamera CCTV untuk *Face Recognition*, *relay*, *solenoid door lock*, dan *buzzer*. Perangkat lunak dibangun menggunakan Flask sebagai *web server*, kemudian MySQL sebagai basis data, dan protokol MQTT sebagai komunikasi data antarperangkat IoT.



Gambar 1. Blok Diagram Sistem Monitoring Keamanan Rumah

Gambar diatas merupakan blok diagram sistem monitoring keamanan rumah berbasis IoT dan *website*, terdiri dari tiga bagian utama yaitu perangkat keras (*Hardware*), *web server*, dan *website* sebagai antarmuka.

Perancangan rangkaian sistem dilakukan menggunakan *Fritzing* untuk memetakan koneksi antar komponen seperti ESP32, *fingerprint*, CCTV, *relay*, dan *solenoid door lock* agar sistem dapat terintegrasi dan berfungsi sesuai kebutuhan.

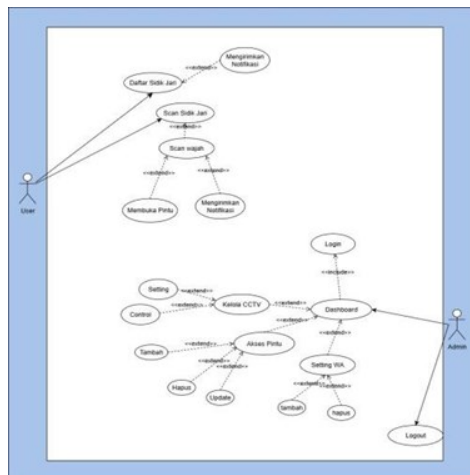


Gambar 2. Wiring Seluruh Alat Sistem

Untuk menggambarkan proses dan struktur sistem secara konseptual digunakan pendekatan *Unified Modeling Language* (UML). UML berfungsi untuk memodelkan interaksi pengguna dengan sistem, alur proses utama, serta struktur data yang digunakan.

A. Use Case Diagram

Use Case Diagram menggambarkan interaksi antara aktor (*User* dan *Admin*) dengan sistem. Diagram ini menunjukkan fungsi utama sistem, seperti autentikasi pengguna, kontrol akses pintu, pemantauan CCTV, serta pengelolaan sistem melalui dashboard web. Interaksi keduanya ditampilkan untuk memperjelas perbedaan hak akses dan peran dalam penggunaan sistem.



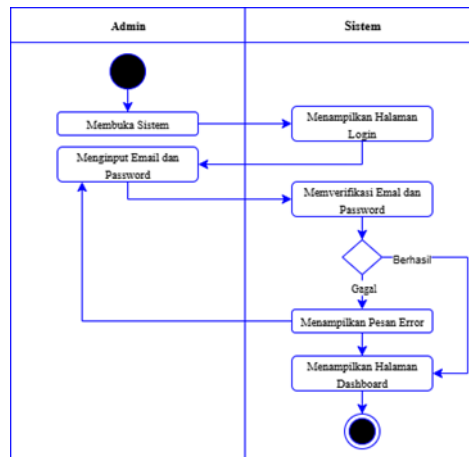
Gambar 3. Use Case Diagram

B. Activity Diagram

Activity Diagram digunakan untuk menggambarkan alur aktivitas dan tahapan proses dalam sistem. Diagram ini menunjukkan urutan tindakan, pengambilan keputusan, serta perpindahan antar aktivitas dengan menggunakan simbol UML. Dengan demikian, aktivitas yang kompleks dapat divisualisasikan menjadi lebih jelas dan mudah dipahami. Diagram ini memodelkan proses kerja sistem serta interaksi antar komponen secara terstruktur.

a. Login

Tahapan perancangan merupakan langkah penting dalam pembangunan perangkat lunak karena berfungsi untuk menggambarkan alur sistem yang akan dibangun, struktur data, serta interaksi antara pengguna dan sistem. Pada penelitian ini, perancangan sistem dilakukan melalui pendekatan *Unified Modeling Language* (UML).

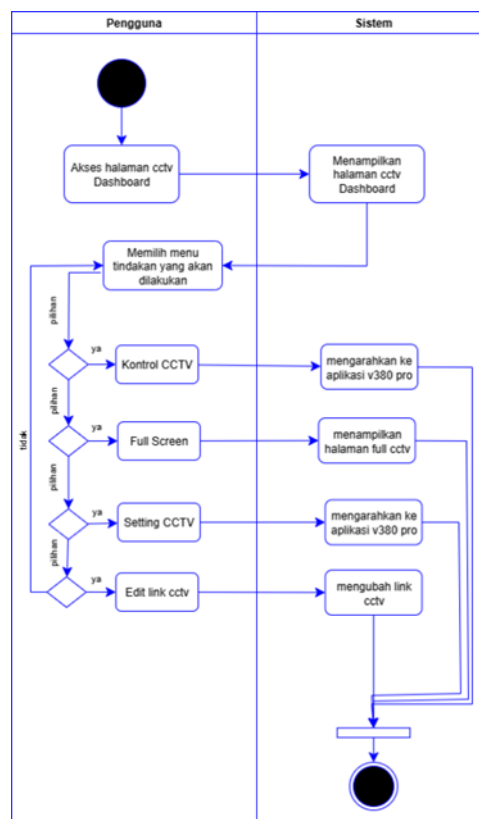


Gambar 4. Login

Activity Diagram ini menggambarkan alur login Admin. Admin memasukkan *email* dan *password*, kemudian sistem melakukan validasi. Jika data valid, sistem menampilkan halaman *dashboard*; jika tidak valid, sistem menampilkan pesan kesalahan dan tetap berada pada halaman *login*.

b. Activity Diagram Menu CCTV

Activity Diagram ini menggambarkan alur interaksi Admin saat mengakses fitur CCTV pada *dashboard* sistem monitoring keamanan rumah.

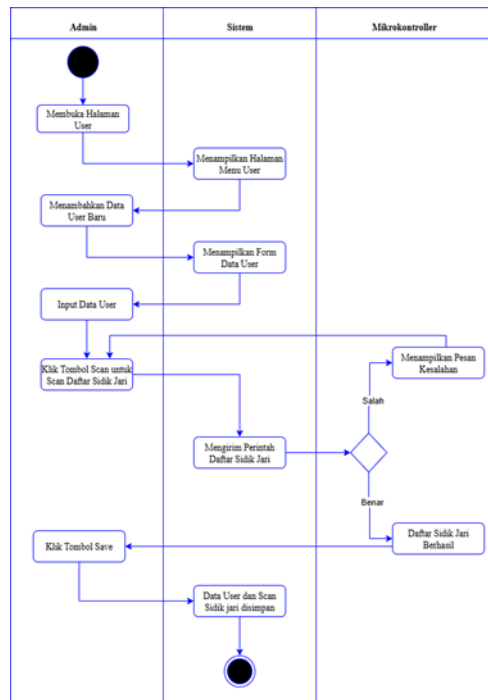


Gambar 5. Menu CCTV

c. Activity Diagram Menambahkan User

Activity Diagram ini menggambarkan alur interaksi Admin saat akan menambah *user* untuk mendapatkan ijin autentikasi akses pintu.

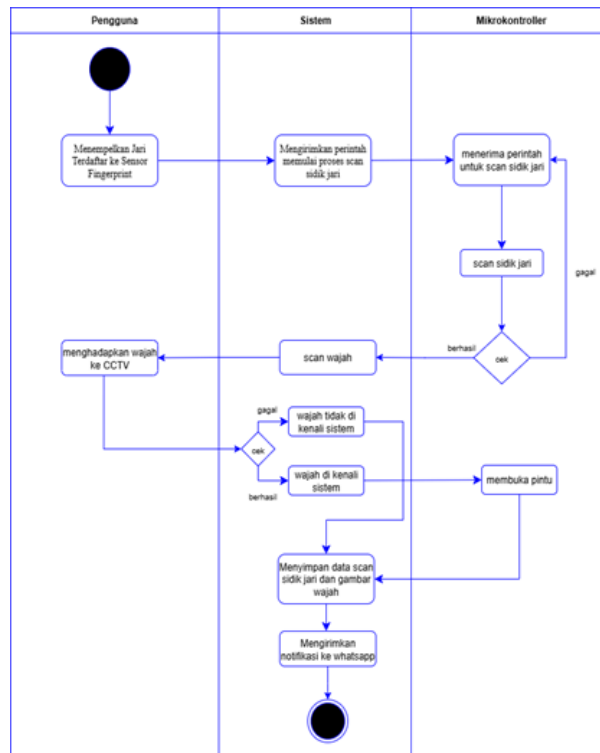
Activity Diagram diatas menjelaskan alur yang dilakukan Admin untuk menambahkan data user baru sekaligus mendaftarkan sidik jari ke dalam sistem. Proses dimulai saat *Admin* membuka halaman menu pengguna pada dashboard. *Admin* memilih tombol Tambah untuk menambahkan user baru dan mengisi *form input* data user.



Gambar 6. Menambahkan User

d. Activity Diagram Akses Pintu dengan Autentifikasi

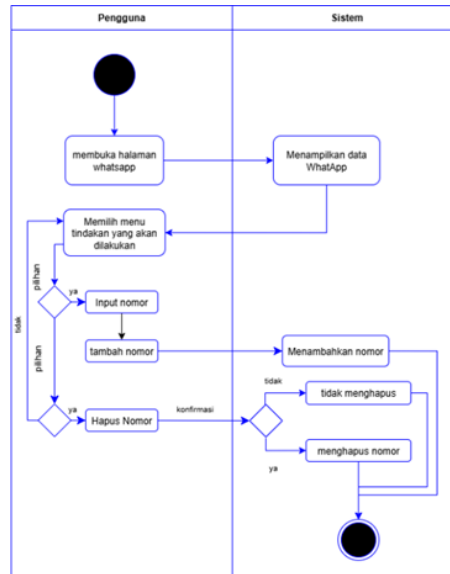
Activity Diagram dibawah ini menggambarkan alur interaksi yang dilakukan user pada saat akan membuka pintu melalui autentikasi menggunakan sidik jari dan *face recognition*.



Gambar 7. Akses Pintu dengan Autentifikasi

e. Activity Diagram Menu WhatsApp

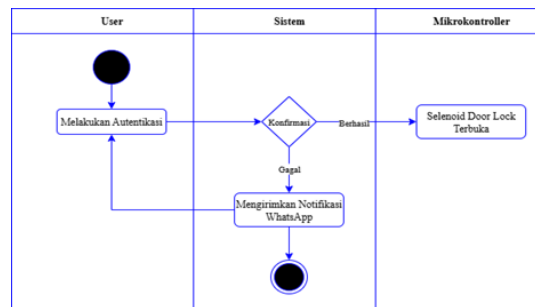
Activity Diagram berikut menggambarkan alur pengelolaan nomor *WhatsApp* pada sistem. Pengguna dapat menambah atau menghapus nomor melalui halaman *WhatsApp*, sementara sistem merespons dengan menampilkan data, memproses penambahan, atau melakukan penghapusan sesuai pilihan pengguna.



Gambar 8. Menu *WhatsApp*

f. Activity Diagram Notifikasi WhatsApp

Activity Diagram di bawah ini menggambarkan alur proses yang dilakukan sistem untuk mengelola pengiriman notifikasi melalui *WhatsApp*.



Gambar 9. Notifikasi *WhatsApp*

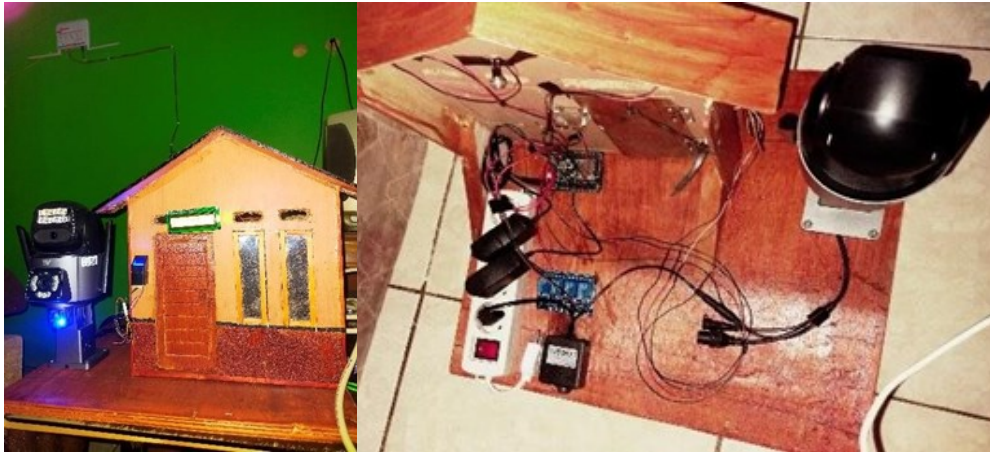
Activity Diagram status kesehatan pada bagian admin untuk menambahkan hasil cek kesehatan pelanggan.

3.2 Implementasi Perancangan Sistem

Adapun hasil dari implementasi perancangan antarmuka yang telah dibuat pada sistem monitoring keamanan rumah sebagai berikut.

1) Realisasi Rangkaian Sistem

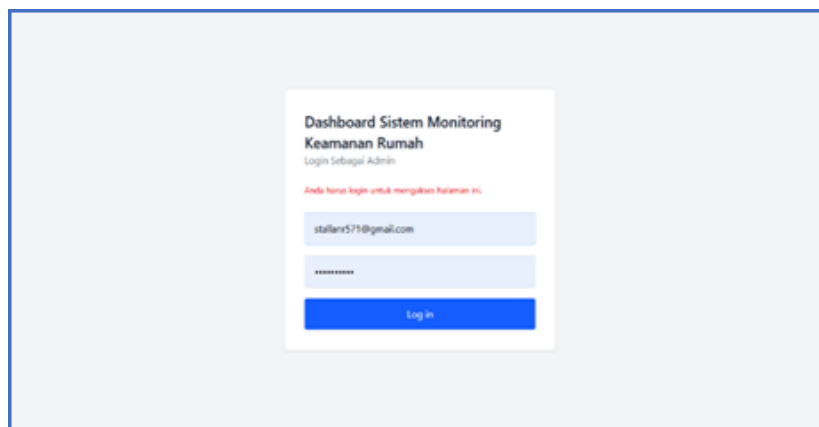
Dibawah ini merupakan tampilan depan dan belakang dari realisasi rangkaian sistem yang telah dirancang sebelumnya menggunakan fritzing.



Gambar 10. Tampilan alat monitoring

2) Login

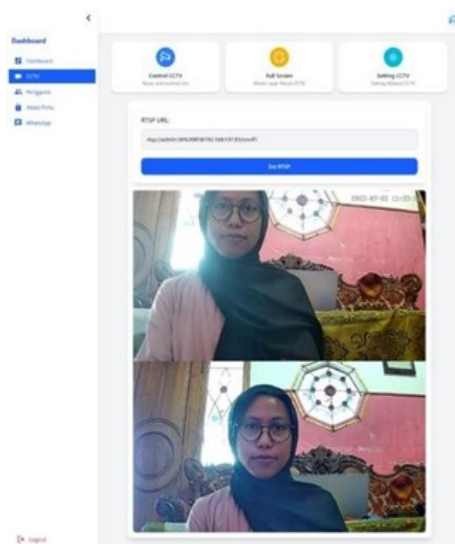
Sebelum mengakses sistem monitoring keamanan rumah, admin melakukan Login menggunakan email dan password yang telah terdaftar.



Gambar 11. Halaman Login

3) Menu CCTV

Pada halaman menu CCTV, admin dapat melakukan semua kontrol CCTV, dan memantau semua pergerakan yang tertangkap oleh kamera.



Gambar 12. Menu CCTV

4) Menambahkan User

Halaman ini terdapat pada halaman pengguna, dan admin dapat menambahkan data diri dan registrasi sidik jari dan wajah untuk dapat akses pint.

Gambar 14. Menu Tambah User

Pada halaman tambah pengguna, admin dapat mendaftarkan pengguna baru untuk akses pintu dengan registrasi wajah dan sidik jari. Halaman ini menampilkan form data diri serta proses perekaman biometrik untuk autentikasi menggunakan *Face Recognition* dan *Fingerprint*.

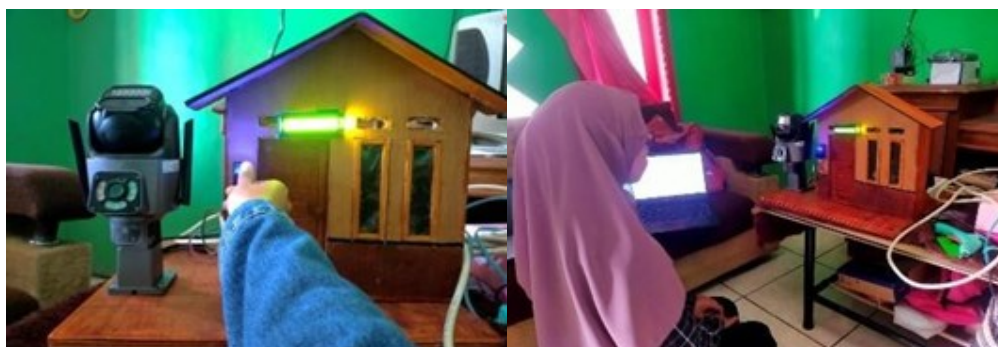


Gambar 15. Proses Registrasi Fingerprint

5) Akses Pintu

Berikut merupakan implementasi proses akses pintu beserta tampilan halaman akses pintu yang menampilkan riwayat aktivitas akses pengguna.

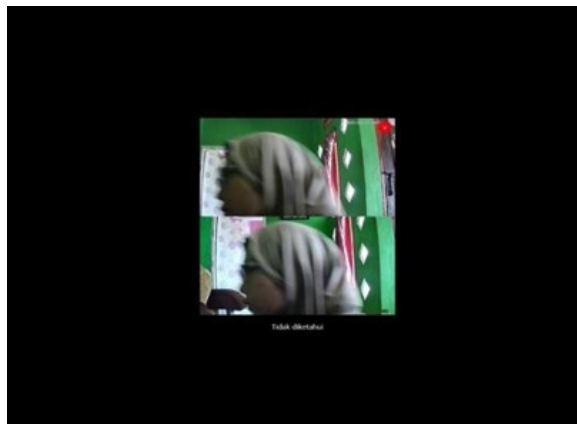
Gambar 16. Menu akses pintu



Gambar 17. Proses Akses Pintu dengan Autentikasi

Autentikasi sidik jari menggunakan sensor AS608 dengan metode *minutiae-based matching*. Pada saat registrasi, sensor menangkap citra sidik jari, melakukan *pre-processing* (peningkatan kualitas citra), lalu mengekstrak titik ciri sebagai template dan menyimpannya sebagai ID pengguna. Saat autentikasi, sidik jari yang dipindai kembali diekstraksi dan dicocokkan dengan template tersimpan. Jika cocok, akses dilanjutkan ke proses verifikasi wajah; jika tidak, akses ditolak dan sistem mengirim notifikasi.

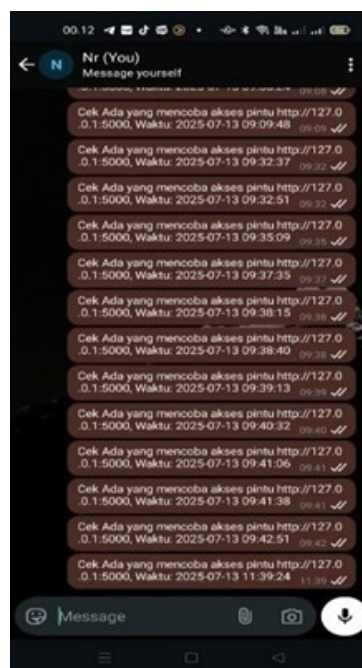
Face recognition pada sistem ini menggunakan algoritma *Local Binary Patterns Histogram* (LBPH) berbasis *supervised learning*. Proses dimulai dari registrasi wajah, kemudian citra melalui tahapan *pre-processing* (*grayscale, resize, cropping, dan noise removal*). Selanjutnya dilakukan ekstraksi fitur menggunakan LBPH untuk menghasilkan histogram wajah sebagai representasi identitas. Model kemudian dilatih dengan dataset berlabel. Saat autentikasi, sistem membandingkan fitur wajah hasil tangkapan kamera dengan model yang telah dilatih untuk menentukan kecocokan. Jika cocok, pintu terbuka; jika tidak, akses ditolak dan sistem mencatat serta mengirim notifikasi.



Gambar 18. Tampilan Foto dengan Status False

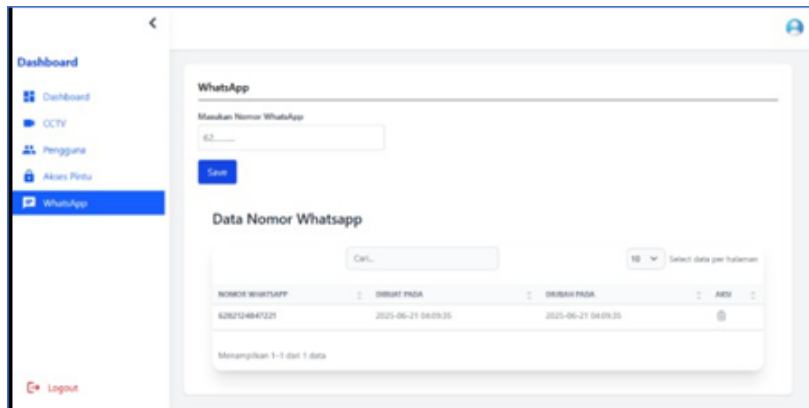
6) Halaman WhatsApp

Halaman ini digunakan untuk menambahkan nomor WhatsApp yang akan menerima notifikasi jika terjadi kegagalan akses pintu.



Gambar 19. Tampilan halaman WhatsApps

7) Tampilan Notifikasi WhatsApp



Gambar 20. Notifikasi Peringatan WhatsApp

3.3 Pengujian Sistem

A. Pengujian *Fingerprint*

Tabel 1. Pengujian *Fingerprint*

No	Jari yang digunakan	Jumlah percobaan	Berhasil	Gagal	Persentase keberhasilan (%)
1.	Ibu Jari	10	10	0	100%
2.	Jari Telunjuk	10	10	0	100%
3.	Jari Tengah	10	9	1	90%
4.	Jari Manis	10	8	2	80%
5.	Jari Kelingking	10	8	2	80%

B. Pengujian *Face Recognition* Berdasarkan Jarak

Tabel 2. Pengujian *Face Recognition* berdasarkan jarak

No	Jarak (cm)	Jumlah Percobaan	Berhasil	Gagal	Persentase Keberhasilan (%)
1.	20	10	6	4	60%
2.	30	10	9	1	90%
3.	50	10	5	5	50%
4.	70	10	1	9	10%
5.	100	10	0	10	0%

C. Pengujian *Face Recognition* Berdasarkan Kondisi Pengguna

Tabel 3. Pengujian *Face Recognition* Berdasarkan Kondisi Pengguna

No	Kondisi Pengguna	Jumlah Percobaan	Berhasil	Gagal	Persentase Keberhasilan (%)
1.	Tanpa Jilbab	10	8	2	80%
2.	Jilbab Hitam Polos	10	1	9	10%
3.	Jilbab Warna Terang	10	9	1	90%
4.	Jilbab Bermotif	10	5	5	50%
5.	Menggunakan Masker	10	0	10	0%

D. Pengujian Notifikasi WhatsApp

Tabel 4. Pengujian Notifikasi WhatsApp

No	Skenario	Jumlah Percobaan	Terkirim	Tidak Terkirim	Rata-rata Delay (Detik)
1.	Autentikasi Berhasil	10	0	10	1
2.	Autentikasi Gagal	10	10	0	1
3.	Internet Tidak Stabil (kegagalan)	10	10	0	6

E. Pengujian Penyimpanan Data ke Dashboard Web

Tabel 5. Pengujian Penyimpanan Data ke Dashboard Web

No	Skenario	Jumlah Percobaan	Data Masuk	Data Hilang	Persentase Keberhasilan (%)
1.	Autentikasi Berhasil	10	10	0	100%
2.	Autentikasi Gagal	10	10	0	100%
3.	Internet Tidak Stabil (kegagalan)	10	10	0	100%

Pengujian menunjukkan bahwa autentikasi sidik jari bekerja sangat baik dengan tingkat keberhasilan hingga 100% pada beberapa jari. *Face recognition* memiliki keberhasilan terbaik pada jarak 30 cm (90%), dan menurun pada jarak lebih jauh serta kondisi jilbab hitam polos karena rendahnya kontras fitur wajah. Notifikasi *WhatsApp* berhasil terkirim dengan delay rata-rata ± 1 detik, dan meningkat menjadi ± 6 detik saat jaringan tidak stabil. Seluruh aktivitas autentikasi tercatat 100% pada *dashboard web*.

4. Simpulan dan Saran

Sistem monitoring keamanan rumah berbasis web dengan autentikasi *fingerprint* dan *face recognition* berhasil diimplementasikan dalam bentuk prototipe yang terintegrasi dengan perangkat IoT dan *dashboard real-time*. Sistem mampu melakukan kontrol akses pintu, monitoring CCTV, serta memberikan notifikasi otomatis melalui *WhatsApp* saat terjadi akses tidak sah. Hasil pengujian menunjukkan bahwa sensor *fingerprint* bekerja dengan akurasi lebih dari 90%, sementara *face recognition* optimal pada jarak 30 cm dengan keberhasilan 90%. Seluruh fungsi utama sistem, termasuk pencatatan log aktivitas dan pengiriman notifikasi, berjalan stabil sehingga sistem ini layak digunakan sebagai solusi keamanan rumah yang lebih modern dan responsif.

Untuk pengembangan selanjutnya, disarankan penggunaan kamera dengan resolusi lebih tinggi agar akurasi *face recognition* meningkat terutama pada kondisi pencahayaan rendah. Sistem notifikasi dapat diperluas ke platform lain seperti Telegram atau aplikasi *mobile*. *Hosting dashboard* pada server publik juga direkomendasikan agar sistem dapat diakses lebih fleksibel. Pengujian lanjutan pada variasi kondisi lingkungan, serta penambahan cadangan daya (UPS), diperlukan untuk memastikan sistem tetap stabil dan dapat beroperasi secara berkelanjutan.

Daftar Pustaka

- Joevan Maulana Florian, Lintang Wahyu Aji Saputro, Muhammad Anugrah Putra, Muhammad Hanif Hilmi, & Rudi Susanto. (2024). Rancangan Sistem Keamanan Pintu Rumah Joglo Menggunakan Fringerprint. <https://doi.org/10.47701/senatib.v4i1>
- Kosasih, R., & Daomara, C. (2021). Pengenalan Wajah dengan Menggunakan Metode Local Binary Patterns Histograms (LBPH). *Jurnal Media Informatika Budidarma*, 5(4), 1258. <https://doi.org/10.30865/mib.v5i4.3171>
- Lionar Putra, & Indah Fenriana. (2024). Rancang Bangun Smart Home System Berbasis Iot Dengan Integrasi Sidik Jari (Fingerprint) Dan Otomasi Elektronik.
- Nasir, M., & Al Gifari, Z. (2024). Politeknik Negeri Bengkalis. In *Seminar Nasional Industri dan Teknologi (SNIT)*.
- Wijaya Setiady, K., & Amanda Ginting, J. (2023). Perancangan Dan Implementasi Security Dan Sistem Kendali Otomatis Smart Home Menggunakan Nodemcu Design And Implementation Of Security And Smart Home Automatic Control Systems Using Nodemcu. *VI(1)*, 543–552. <https://doi.org/10.30813/j-alu.v2i2.3756>