Vol 3.No.1 2024 Hal 221-237

Rancang Bangun Sistem Keamanan Pintu Ganda menggunakan Password dan Sidik Jari Berbasis Internet of Things (IoT)

Zulhanip. S[1], Mhd Arief Hasan[2*], Yogo Turnandes[3]
[1,2]Program Studi Teknik Informatika Fakultas Ilmu Komputer Universitas Lancang Kuning
[,3]Program Studi Bisnis Digital Fakultas Ilmu Komputer Universitas Lancang Kuning

[1,2,3]Jl. Yos Sudarso KM. 8 Rumbai, Pekanbaru, Riau, telp. 0811 753 2015
e-mail: [1]Zulhanif1508@gmail.com , [2*]m.arif@unilak.ac.id, [3]turnandes@unilak.ac.id

Abstrak

Sistem keamanan pintu berbasis Internet of Things (IoT) ini dirancang untuk meningkatkan proteksi rumah dengan mengintegrasikan autentikasi sidik jari, keypad, serta deteksi ancaman melalui sensor getar dan reed switch. Penelitian ini bertujuan untuk mengembangkan solusi keamanan yang efektif dan modern, yang mampu memberikan akses hanya kepada pengguna yang sah serta memberikan notifikasi real-time ketika terdeteksi adanya usaha pembobolan. Sistem ini menggunakan Firebase Realtime Database untuk sinkronisasi data dan pengiriman notifikasi secara cepat melalui aplikasi mobile. Hasil pengujian menunjukkan bahwa sistem dapat mendeteksi dan mengautentikasi pengguna dengan waktu respon rata-rata 1,7 detik, serta mengirimkan notifikasi kepada pengguna dalam waktu rata-rata 3,75 detik, bahkan pada jarak hingga 11 kilometer. Dengan demikian, sistem ini terbukti efektif dalam meningkatkan keamanan pintu secara proaktif dan responsif, serta memberikan kendali penuh kepada pengguna melalui aplikasi mobile. Namun, pengembangan lebih lanjut diperlukan untuk meningkatkan ketahanan sistem terhadap kondisi lingkungan yang ekstrem dan gangguan jaringan.

Kata Kunci*: Sistem Keamanan, Internet Of Things (IoT), Autentikasi Sidik Jari, Deteksi Ancaman, Notifikasi Real-Time.*

Abstract

This Internet of Things (IoT)-based door security system is designed to enhance home protection by integrating fingerprint authentication, a keypad, and threat detection using a vibration sensor and reed switch. The objective of this research is to develop an effective and modern security solution that grants access only to authorized users while providing real-time notifications when an attempted break-in is detected. The system utilizes Firebase Realtime Database for data synchronization and fast notification delivery through a mobile application. Test results show that the system can detect and authenticate users with an average response time of 1.7 seconds and send notifications to users with an average delivery time of 3.75 seconds, even at distances up to 11 kilometers. Thus, the system has proven effective in enhancing door security proactively and responsively, providing users full control via a mobile app. However, further development is needed to improve system resilience in extreme environmental conditions and network disruptions.

Keywords*: Security system, Internet of Things (IoT), Fingerprint Authentication, Threat Detection, Real-Time Notification.*

1. PENDAHULUAN

Keamanan rumah merupakan aspek vital yang terus menjadi perhatian di era modern. Dalam kehidupan sehari-hari, banyak kegiatan dilakukan di luar rumah, meninggalkan rumah dalam keadaan kosong untuk jangka waktu yang lama. Keadaan ini menjadikan rumah yang tidak dilengkapi dengan sistem keamanan yang memadai menjadi target potensial bagi tindakan kriminal.

Meskipun banyak rumah saat ini sudah dilengkapi dengan kamera CCTV, teknologi ini sering kali hanya berfungsi sebagai alat perekam kejadian tanpa memberikan pencegahan atau respons cepat terhadap ancaman yang sedang terjadi.

Sistem kunci konvensional yang masih banyak digunakan juga memiliki kelemahan signifikan. Kunci ini rentan terhadap pembobolan, baik melalui penggandaan kunci maupun manipulasi lainnya. Keamanan rumah yang masih bergantung pada teknologi lama ini mengakibatkan pemilik rumah hanya dapat mengambil tindakan setelah kejadian terjadi, yang sering kali sudah terlambat untuk mencegah kerugian. Oleh karena itu, diperlukan solusi yang mampu memberikan perlindungan yang lebih baik dan respons yang lebih cepat.

Di sisi lain, teknologi Internet of Things (IoT) menawarkan solusi yang lebih canggih melalui sistem autentikasi biometrik dan kata sandi[1]. Namun, meskipun teknologi ini menjanjikan, implementasinya di lapangan masih terbatas. Banyak sistem keamanan berbasis IoT yang telah dikembangkan, namun tidak mampu memberikan informasi real-time kepada pemilik rumah ketika ancaman terjadi. Kekurangan ini menunjukkan adanya celah dalam sistem yang ada, terutama dalam hal kemampuan memberikan notifikasi dan respons secara langsung.

Penelitian ini menawarkan kontribusi baru dalam bidang keamanan rumah dengan mengembangkan sistem keamanan pintu ganda yang memadukan autentikasi sidik jari dan kata sandi berbasis IoT. Sistem ini tidak hanya menggantikan sistem keamanan konvensional tetapi juga meningkatkan kemampuan sistem dalam memberikan informasi kondisi rumah secara real-time kepada pengguna. Dengan demikian, sistem ini diharapkan dapat memberikan solusi yang lebih proaktif dan efektif dalam menghadapi ancaman keamanan.

Tujuan dari penelitian ini adalah untuk merancang dan mengembangkan sistem keamanan yang mampu menggantikan sistem konvensional dengan solusi digital yang lebih modern. Selain itu, penelitian ini juga bertujuan untuk meningkatkan responsivitas terhadap ancaman keamanan melalui pemanfaatan teknologi IoT secara efektif. Dengan demikian, penelitian ini diharapkan dapat memberikan kontribusi nyata dalam meningkatkan keamanan rumah di era digital ini[2], [3].

2. METODE PENELITIAN

Metode penelitian ini dirancang untuk mengembangkan dan menguji sebuah sistem keamanan pintu ganda berbasis Internet of Things (IoT) yang menggunakan autentikasi sidik jari dan kata sandi. Penelitian ini dilakukan secara bertahap, dimulai dari identifikasi masalah yang ada pada sistem keamanan konvensional, hingga pengujian efektivitas sistem yang telah dikembangkan. Setiap tahapan dalam penelitian ini diuraikan secara rinci untuk memastikan bahwa hasil yang diperoleh dapat memberikan kontribusi nyata dalam meningkatkan keamanan rumah di era digital.

a. Studi Pendahuluan

Studi pendahuluan dilakukan untuk memahami kondisi dan kelemahan sistem keamanan pintu yang masih menggunakan teknologi konvensional. Tahap ini bertujuan untuk mengidentifikasi masalah utama yang dihadapi oleh pengguna dalam menjaga keamanan rumah mereka. Penelitian dimulai dengan melakukan observasi langsung pada beberapa rumah yang masih menggunakan kunci konvensional. Observasi ini bertujuan untuk mengumpulkan data tentang efektivitas sistem kunci dalam menghadapi potensi ancaman seperti pembobolan atau penggandaan kunci.

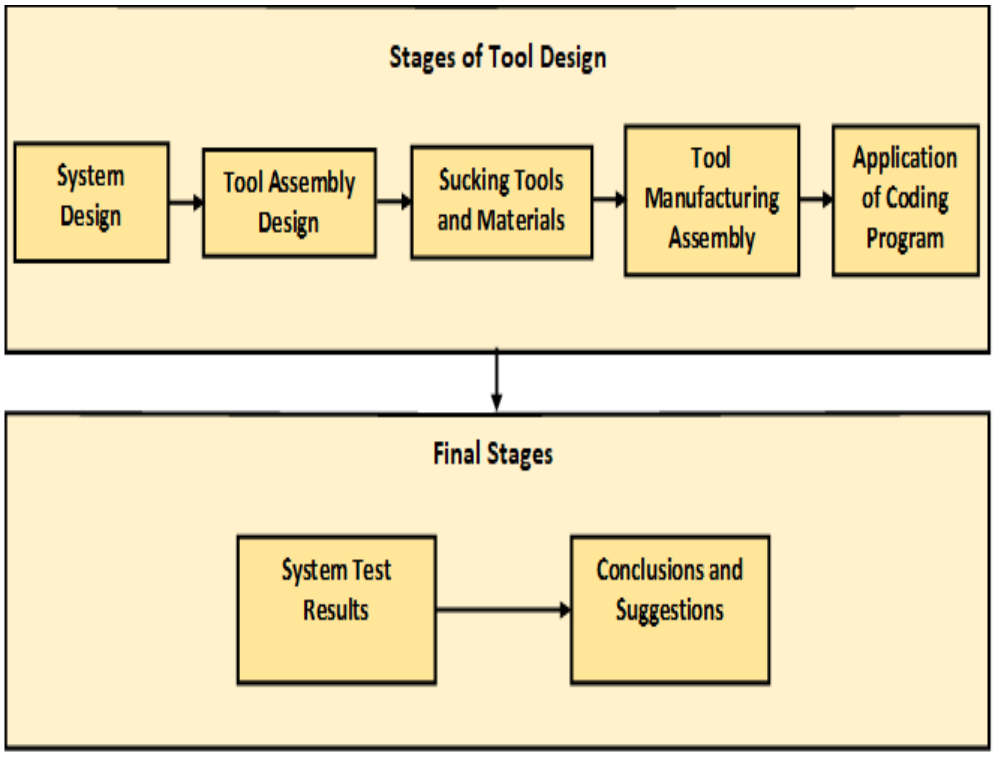
Selain observasi, tinjauan literatur juga dilakukan untuk memahami tren terbaru dalam teknologi keamanan rumah, khususnya yang berkaitan dengan penggunaan Internet of Things (IoT) dan autentikasi biometrik. Tinjauan literatur ini mencakup

analisis terhadap penelitian-penelitian sebelumnya yang telah mengembangkan sistem keamanan berbasis IoT, serta identifikasi kekurangan yang masih ada dalam implementasi teknologi ini. Dari hasil studi pendahuluan ini, ditemukan bahwa meskipun beberapa sistem keamanan modern telah dikembangkan, banyak di antaranya yang tidak mampu memberikan notifikasi real-time kepada pemilik rumah ketika terjadi ancaman.

Hasil dari studi pendahuluan ini menjadi dasar untuk merancang sistem keamanan yang mampu mengatasi kelemahan-kelemahan tersebut. Fokus dari sistem yang akan dikembangkan adalah meningkatkan keamanan melalui kombinasi autentikasi sidik jari dan kata sandi, serta memastikan bahwa pengguna dapat menerima informasi kondisi rumah secara real-time melalui konektivitas IoT.

b. Perancangan Sistem

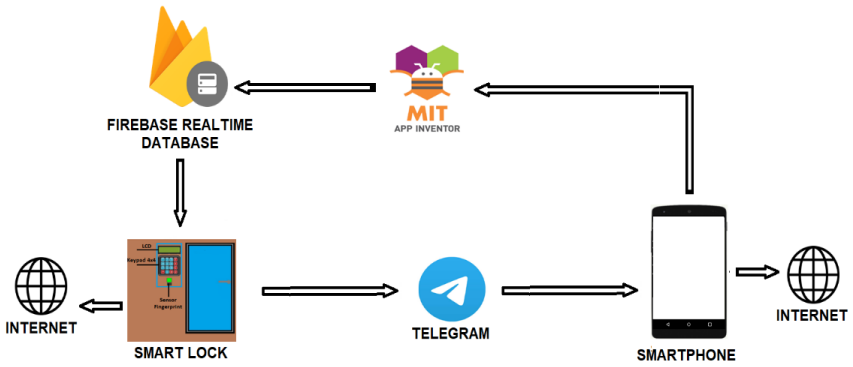
Perancangan sistem dalam penelitian ini melibatkan beberapa tahapan yang terstruktur, dimulai dari perancangan konsep hingga implementasi dan pengujian sistem. Gambar di bawah ini menggambarkan alur tahapan perancangan sistem yang terdiri dari lima langkah utama dalam proses perancangan alat, serta dua langkah akhir yang berfokus pada pengujian dan evaluasi sistem.



Gambar 1. Perancangan Sistem

1) Perancangan Sistem (System Design)

Tahap pertama dalam perancangan sistem adalah merancang keseluruhan konsep sistem yang akan dikembangkan. Pada tahap ini, dilakukan identifikasi kebutuhan, spesifikasi teknis, serta fungsi-fungsi utama yang harus dimiliki oleh sistem. Perancangan ini mencakup pemilihan teknologi yang akan digunakan, seperti modul IoT, sensor sidik jari, dan mekanisme penguncian pintu[4], [5]. Semua elemen ini dirancang untuk bekerja secara terpadu dalam rangka mencapai tujuan sistem keamanan yang diinginkan.



Gambar 2. Block Diagram

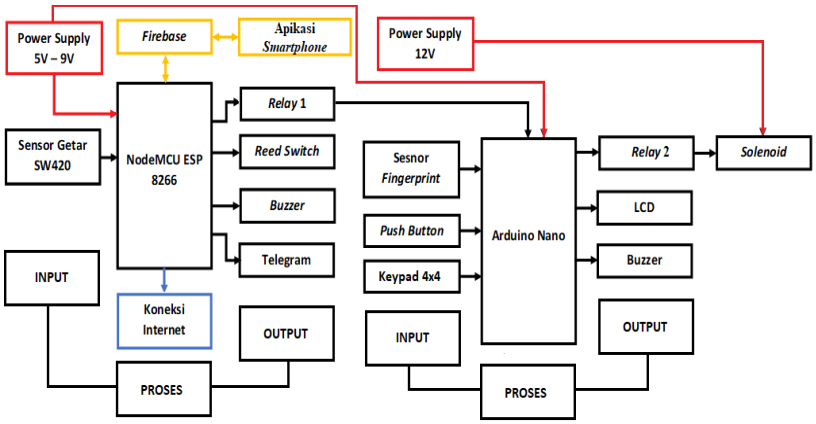
Gambar tersebut menggambarkan arsitektur sistem yang dirancang untuk mengamankan pintu menggunakan teknologi Internet of Things (IoT) dengan autentikasi sidik jari dan kata sandi[6][7]. Sistem ini terdiri dari beberapa komponen utama yang saling terhubung untuk menyediakan layanan keamanan yang dapat diakses secara real-time melalui perangkat mobile.

Komponen-komponen Utama:

a) Firebase Realtime Database: Firebase Realtime Database digunakan sebagai basis data untuk menyimpan dan menyinkronkan data antara perangkat pengguna (smartphone) dan sistem keamanan pintu (smart lock). Basis data ini bekerja secara real-time, memungkinkan perubahan status keamanan pintu untuk segera diperbarui dan diakses oleh pengguna melalui aplikasi yang terhubung.
b) MIT App Inventor: MIT App Inventor digunakan untuk mengembangkan aplikasi mobile yang menjadi antarmuka antara pengguna dan sistem keamanan[8]. Aplikasi ini memungkinkan pengguna untuk memantau status pintu, mengirim perintah untuk mengunci atau membuka pintu, serta menerima notifikasi keamanan secara langsung melalui smartphone.
c) Smart Lock: Smart Lock adalah perangkat kunci pintar yang terhubung ke internet dan dikendalikan melalui aplikasi. Perangkat ini dilengkapi dengan sensor sidik jari dan keypad untuk autentikasi pengguna. Ketika pengguna memasukkan sidik jari atau kata sandi yang benar, smart lock akan membuka pintu dan memperbarui statusnya di Firebase Realtime Database.
d) Telegram: Telegram digunakan sebagai platform untuk mengirim notifikasi keamanan kepada pengguna. Setiap kali ada aktivitas mencurigakan, seperti upaya membuka pintu tanpa izin, sistem akan mengirim pesan notifikasi ke aplikasi Telegram yang terhubung dengan akun pengguna. Hal ini memungkinkan pengguna untuk segera mengambil tindakan jika terjadi ancaman keamanan.
e) Smartphone: Smartphone berfungsi sebagai perangkat yang digunakan oleh pengguna untuk mengakses aplikasi mobile yang dikembangkan dengan MIT App Inventor. Melalui aplikasi ini, pengguna dapat memantau status pintu, mengontrol akses pintu, dan menerima notifikasi keamanan dari smart lock. Smartphone terhubung ke internet untuk memastikan komunikasi yang lancar dengan Firebase dan perangkat smart lock.

2. Alur Kerja Sistem:

Sistem keamanan yang dirancang terdiri dari beberapa komponen utama yang saling terhubung untuk menyediakan keamanan real-time berbasis Internet of Things (IoT). Gambar di bawah ini menunjukkan diagram alur dari seluruh sistem yang mencakup proses input, pemrosesan data, dan output.

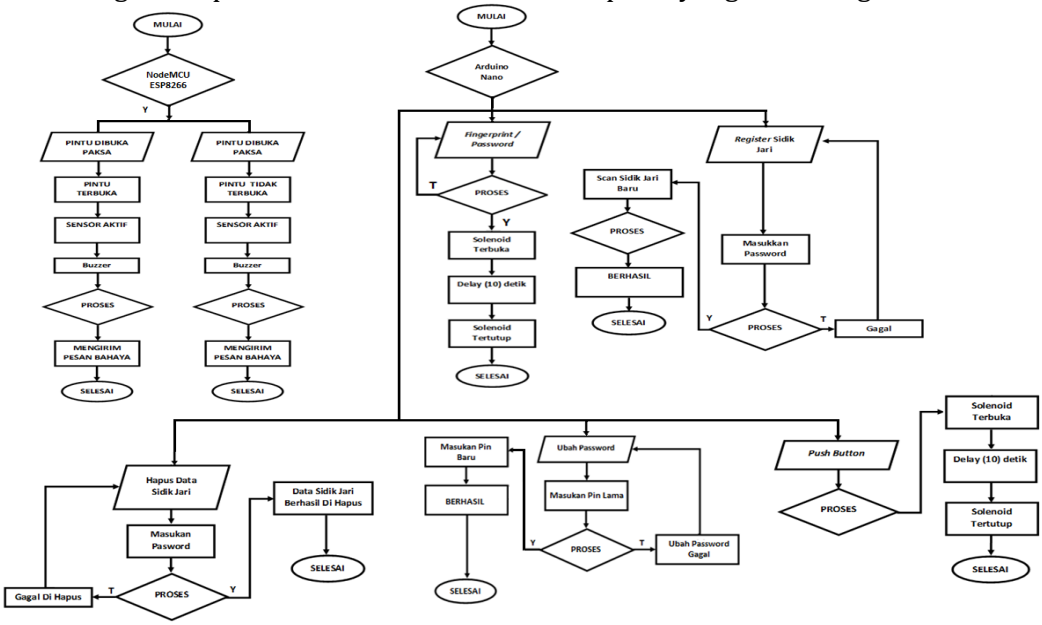


Gambar 3. Alur Kerja Sistem

dalam gambar ini, sistem dibagi menjadi beberapa bagian utama:

a) Input: Sensor-sensor seperti Sensor Getar SW-420 dan Reed Switch mendeteksi adanya aktivitas fisik atau upaya pembobolan pintu.
b) Pemrosesan: Data dari sensor dikirimkan ke NodeMCU ESP8266, yang kemudian mengelola koneksi internet melalui Firebase dan berkomunikasi dengan aplikasi di smartphone pengguna. Selain itu, data juga diproses oleh Arduino Nano untuk memvalidasi autentikasi sidik jari dan kata sandi melalui sensor fingerprint dan keypad 4x4.
c) Output: Berdasarkan input yang diterima dan proses autentikasi, sistem mengaktifkan atau menonaktifkan relay yang mengontrol solenoid untuk membuka atau mengunci pintu. Notifikasi dikirimkan ke smartphone pengguna melalui aplikasi jika terdeteksi ancaman..

Setelah perancangan sistem dan arsitektur keseluruhan dijelaskan, penting untuk memahami bagaimana sistem ini bekerja secara rinci dalam praktiknya. Diagram alur kerja di atas memberikan gambaran lebih spesifik mengenai logika operasi dan interaksi antara berbagai komponen dalam sistem keamanan pintu yang dirancang.



Gambar 4. Flowchart System

Penjelasan Flowchart Alur Kerja Sistem:

a) **NodeMCU ESP8266 dan Arduino Nano**: Sistem dimulai dari inisialisasi dua komponen utama, yaitu NodeMCU ESP8266 dan Arduino Nano. NodeMCU bertanggung jawab untuk mengelola konektivitas IoT, mengontrol notifikasi, dan memproses input dari sensor keamanan seperti sensor getar dan reed switch. Di sisi lain, Arduino Nano mengelola proses autentikasi pengguna, baik melalui sidik jari maupun kata sandi.

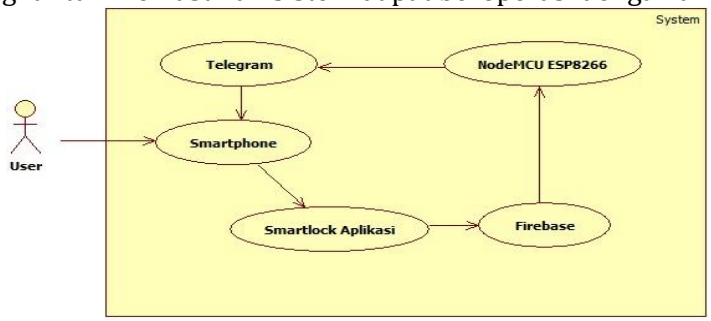
b) **Autentikasi dan Kontrol Akses**: Proses autentikasi dimulai ketika pengguna mencoba mengakses pintu dengan menggunakan sidik jari atau memasukkan kata sandi. Jika autentikasi berhasil (ditandai dengan verifikasi yang benar dari sidik jari atau kata sandi), maka sistem akan membuka solenoid pintu, yang berarti pintu terbuka. Setelah pintu terbuka, sistem akan menunggu selama beberapa detik sebelum menutup kembali solenoid, memastikan pintu terkunci secara otomatis. Jika autentikasi gagal, baik karena sidik jari tidak terdaftar atau kata sandi yang dimasukkan salah, sistem tidak akan membuka pintu dan akan menampilkan pesan kesalahan yang sesuai.

c) **Fitur Tambahan dan Keamanan**: Sistem juga memiliki fitur untuk menghapus data sidik jari dan mengubah kata sandi. Proses ini dilindungi oleh verifikasi awal, di mana pengguna harus memasukkan kata sandi lama sebelum dapat mendaftar sidik jari baru atau mengubah kata sandi. Ini memastikan bahwa hanya pengguna yang berwenang yang dapat melakukan perubahan pada data autentikasi. Selain itu, sistem memiliki kemampuan untuk mendeteksi ancaman melalui sensor getar (SW420) dan reed switch. Jika ada upaya untuk merusak pintu atau membukanya secara paksa, sistem akan segera mengaktifkan buzzer dan mengirimkan notifikasi ke pengguna melalui Telegram, memberi tahu mereka tentang potensi ancaman keamanan.

d) **Pengendalian Manual melalui Push Button**: Pengguna juga diberikan opsi untuk membuka pintu dari dalam menggunakan push button. Proses ini juga diatur oleh Arduino Nano dan hanya memungkinkan pintu untuk dibuka jika push button ditekan.

3. Perancangan Sistem Aplikasi

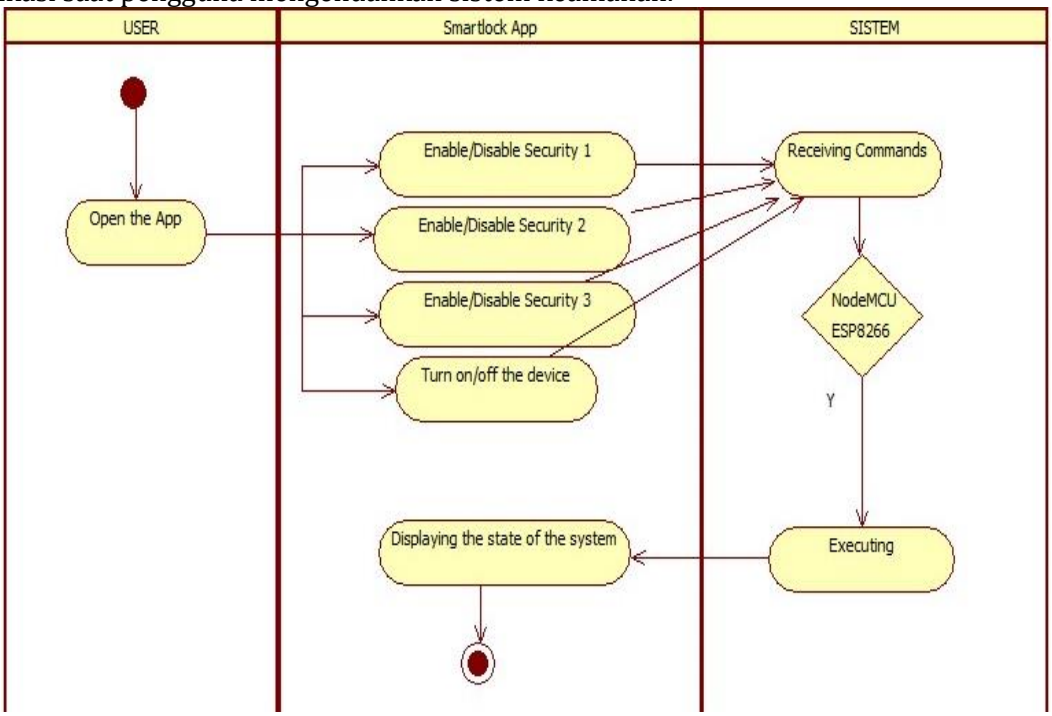
Pada tahap ini, aplikasi yang menjadi antarmuka utama antara pengguna dan sistem keamanan pintu berbasis IoT dirancang untuk memungkinkan akses, kontrol, dan pemantauan pintu secara jarak jauh melalui smartphone. Diagram use case di bawah ini menggambarkan interaksi pengguna dengan berbagai komponen sistem, seperti aplikasi smart lock, Firebase, NodeMCU ESP8266, dan Telegram, serta menunjukkan bagaimana aplikasi ini dirancang untuk memfasilitasi komunikasi yang efektif antara pengguna dan sistem keamanan. Perancangan ini mencakup pengembangan antarmuka yang intuitif dan integrasi teknologi untuk memastikan sistem dapat beroperasi dengan aman dan efisien.



Gambar 5. *Use Case* Sistem Aplikasi

Diagram use case ini menggambarkan interaksi antara pengguna dengan sistem keamanan pintu berbasis IoT melalui aplikasi di smartphone. Pengguna dapat mengontrol dan memantau status pintu, mengirim perintah melalui aplikasi yang terhubung dengan Firebase untuk sinkronisasi data secara real-time, dan mengendalikan smart lock melalui NodeMCU ESP8266. Selain itu, sistem ini juga dilengkapi dengan fitur notifikasi keamanan yang dikirim melalui Telegram, yang akan segera memberi tahu pengguna jika ada aktivitas mencurigakan atau ancaman terhadap keamanan pintu. Diagram ini menunjukkan alur komunikasi dan interaksi antara komponen-komponen utama dalam sistem untuk memastikan bahwa pengguna dapat mengelola keamanan pintu secara efisien dan responsif.

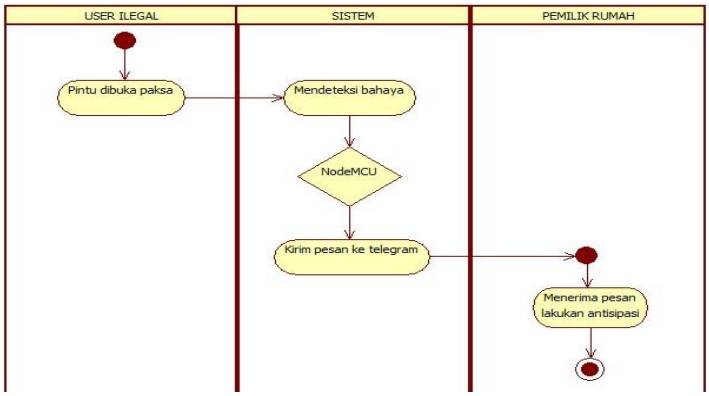
Setelah memahami interaksi umum antara pengguna dan komponen sistem melalui diagram use case, penting untuk melihat lebih dekat bagaimana aplikasi smart lock beroperasi secara internal. Diagram berikut menjelaskan alur kerja spesifik dalam aplikasi saat pengguna mengendalikan sistem keamanan.



Gambar 6. *Activity Diagram* Sistem Monitoring

Diagram ini menggambarkan langkah-langkah yang terjadi saat pengguna membuka aplikasi smart lock di smartphone mereka. Setelah aplikasi dibuka, pengguna dapat mengaktifkan atau menonaktifkan beberapa tingkat keamanan (Security 1, Security 2, Security 3) dan mengontrol perangkat lainnya melalui opsi untuk menyalakan atau mematikan perangkat. Setiap tindakan yang dipilih oleh pengguna akan mengirimkan perintah ke sistem melalui NodeMCU ESP8266, yang kemudian akan memproses dan mengeksekusi perintah tersebut. Selain itu, aplikasi juga menampilkan status terkini dari sistem, memberikan pengguna informasi real-time tentang kondisi keamanan pintu. Diagram ini menyoroti bagaimana aplikasi dan sistem saling berinteraksi untuk memberikan kontrol penuh kepada pengguna atas sistem keamanan rumah mereka.

Setelah menjelaskan bagaimana pengguna dapat berinteraksi dengan aplikasi untuk mengontrol sistem keamanan, penting juga untuk memahami bagaimana sistem bereaksi terhadap potensi ancaman keamanan. Diagram berikut menggambarkan alur kerja ketika terjadi upaya pembukaan pintu secara paksa oleh pengguna yang tidak sah.

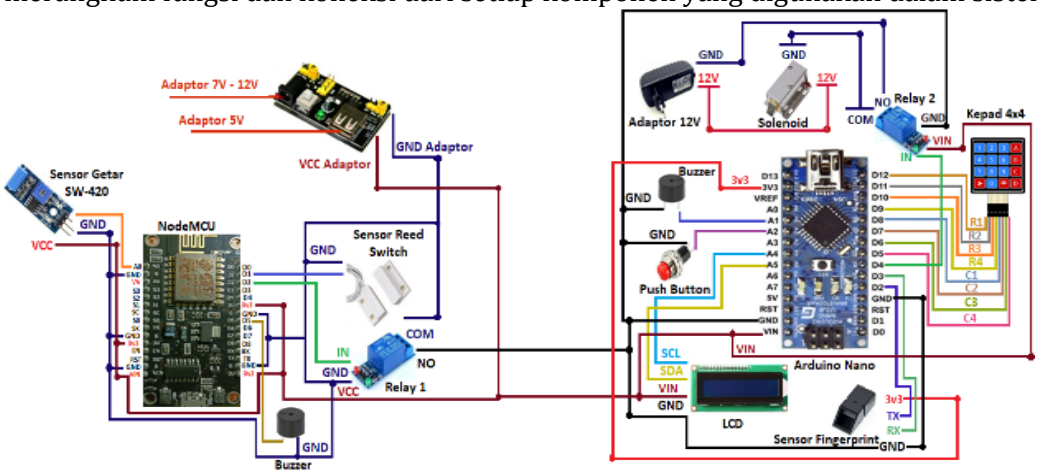


Gambar 7. *Activity Diagram* Sistem Notifikasi

Dalam skenario ini, jika pintu dibuka secara paksa oleh pihak yang tidak berwenang, sistem akan segera mendeteksi adanya ancaman melalui sensor yang terhubung dengan NodeMCU. Setelah ancaman terdeteksi, NodeMCU akan mengirimkan peringatan ke pemilik rumah melalui pesan yang dikirim ke aplikasi Telegram. Pemilik rumah kemudian akan menerima pesan tersebut dan dapat segera mengambil tindakan antisipatif untuk mengamankan properti mereka. Diagram ini menunjukkan bagaimana sistem secara otomatis merespons ancaman dengan cepat dan efektif, memastikan bahwa pemilik rumah selalu mendapatkan notifikasi real-time tentang potensi bahaya yang mengancam keamanan rumah mereka.

4. Implementasi Sistem

Setelah perancangan sistem selesai, langkah berikutnya adalah implementasi fisik dari sistem ini, yang mencakup perakitan semua komponen elektronik dan pengujian integrasi sistem[1], [9], [10]. Gambar di bawah ini menunjukkan diagram rangkaian lengkap dari sistem keamanan pintu berbasis IoT yang dikembangkan. Untuk memberikan pemahaman yang lebih jelas tentang fungsi masing-masing komponen, berikut ini adalah tabel yang merangkum fungsi dan koneksi dari setiap komponen yang digunakan dalam sistem ini.



Gambar 8. Skema Sirkuit Komponen

Diagram di atas menunjukkan implementasi sistem keamanan pintu ganda yang terdiri dari berbagai komponen elektronik utama yang terhubung secara terpadu. Setiap komponen memiliki peran penting dalam menjalankan fungsi sistem keamanan ini, yang memadukan autentikasi biometrik (sidik jari) dan kata sandi untuk meningkatkan keamanan pintu[11].

TABEL 1. Daftar Komponen

Komponen	Jumlah
NodeMCU ESP8266	1
Arduino Nano	1
Sensor Getar SW-420	1
Reed Switch	1
Relay 1 Channel	2
Solenoid Door Lock	1
Keypad 4x4	1
Sensor Sidik Jari	1
Buzzer	1
Push Button	1
Adaptor 5V	1
Adaptor 12V	1
LCD	1
Breadboard	1
Kabel Jumper	Sesuai kebutuhan

4. HASIL DAN PEMBAHASAN

Pada bagian ini akan dijelaskan hasil-hasil dari penelitian yang telah dilakukan serta analisis terhadap setiap hasil yang diperoleh. Penelitian ini bertujuan untuk mengembangkan sistem keamanan pintu ganda berbasis Internet of Things (IoT) yang mengintegrasikan autentikasi sidik jari dan kata sandi. Sistem ini diuji untuk mengevaluasi efektivitas dalam memberikan keamanan yang lebih baik bagi rumah dan bangunan. Uji coba dilakukan pada beberapa skenario, seperti keberhasilan autentikasi sidik jari dan kata sandi, waktu respon sistem dalam mengunci dan membuka pintu, serta kecepatan pengiriman notifikasi kepada pengguna saat terdeteksi ancaman. Selain itu, sistem juga diuji kemampuannya dalam memberikan informasi real-time melalui notifikasi kepada pengguna menggunakan platform Telegram. Pembahasan hasil uji coba ini akan mencakup aspek keandalan, kecepatan, serta potensi perbaikan pada sistem keamanan yang dikembangkan. Hasil pengujian tersebut akan disajikan dalam bentuk tabel, grafik, dan visualisasi untuk memberikan gambaran yang lebih komprehensif mengenai performa sistem.

a. Hasil Pengujian Autentikasi

Pengujian autentikasi dilakukan untuk memastikan keandalan sistem keamanan dalam mengenali dan memverifikasi identitas pengguna. Sistem yang dirancang menggunakan dua metode autentikasi, yaitu **autentikasi sidik jari** dan **autentikasi kata sandi** melalui keypad 4x4. Pengujian ini dilakukan untuk memastikan bahwa hanya pengguna yang memiliki akses sah yang dapat membuka pintu, serta mengukur waktu respon dari sistem.

Pengujian ini dilakukan pada beberapa skenario sebagai berikut:

1. **Pengujian Autentikasi Sidik Jari**:
   - Pengguna yang terdaftar menempatkan jari pada sensor fingerprint. Hasil menunjukkan bahwa sistem dapat mengenali sidik jari yang terdaftar dengan waktu respon rata-rata 1,7 detik.
   - Saat pengguna yang tidak terdaftar mencoba membuka pintu, sistem menolak akses dengan hasil yang konsisten.
2. **Pengujian Autentikasi Kata Sandi**:
   - Pengguna memasukkan kata sandi yang benar melalui keypad 4x4, dan sistem membuka pintu dengan waktu respon rata-rata 1,5 detik.
   - Pengujian dengan memasukkan kata sandi yang salah menghasilkan penolakan akses yang tepat tanpa membuka kunci pintu.

Tabel berikut merangkum hasil dari pengujian autentikasi:

TABEL 2. Hasil Pengujian Autentikasi

Skenario Pengujian	Hasil Autentikasi	Waktu Respon
Sidik jari terdaftar	Berhasil	1,7 detik
Sidik jari tidak terdaftar	Gagal	1,7 detik
Kata sandi benar	Berhasil	1,5 detik
Kata sandi salah	Gagal	1,5 detik

Hasil pengujian menunjukkan bahwa sistem autentikasi bekerja dengan baik dan mampu memberikan akses hanya kepada pengguna yang terdaftar, baik melalui sidik jari maupun kata sandi. Waktu respon sistem juga memadai untuk aplikasi keamanan pintu, dengan respon yang cepat dan konsisten.

Gambar 9. Implementasi Fingerprint

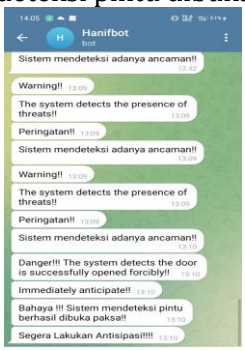
Gambar di atas menunjukkan implementasi fisik dari sistem autentikasi menggunakan keypad 4x4 dan sensor sidik jari. Terdapat dua tampilan yang menunjukkan hasil dari proses autentikasi, yaitu:

1. **Tampilan kiri:** Menunjukkan autentikasi yang berhasil, di mana pengguna memasukkan sidik jari yang sudah terdaftar. Indikator LED berwarna hijau menyala, dan layar menampilkan pesan "Berhasil...!!" sebagai tanda bahwa akses diizinkan, dan pintu dapat dibuka.

2. **Tampilan kanan:** Menunjukkan autentikasi yang gagal, di mana pengguna mungkin memasukkan sidik jari yang tidak terdaftar atau kata sandi yang salah. Layar menampilkan pesan "Akses Ditolak" sebagai tanda bahwa akses tidak diizinkan, dan pintu tetap terkunci.

b. Hasil Pengujian Notifikasi Real-Time

Pengujian notifikasi real-time dilakukan untuk mengevaluasi kecepatan dan keandalan sistem dalam memberikan peringatan kepada pengguna melalui aplikasi Telegram ketika terdeteksi ancaman keamanan. Sistem mengirimkan notifikasi ketika Sensor Getar SW-420 mendeteksi adanya getaran yang menandakan percobaan perusakan pintu, atau ketika Reed Switch mendeteksi pintu dibuka secara paksa.



Gambar 10. Implementasi Notifikasi

Pengujian ini dilakukan pada beberapa skenario dengan berbagai jarak antara pengguna dan perangkat untuk menguji kecepatan pengiriman notifikasi:

1. **Deteksi Getaran pada Pintu:**Ketika pintu menerima getaran yang signifikan, sistem langsung mengirimkan notifikasi ke pengguna melalui aplikasi Telegram. Notifikasi ini diterima dengan waktu pengiriman rata-rata antara 3 hingga 5 detik, tergantung pada jarak pengguna dari perangkat.
2. **Deteksi Pintu Dibuka Paksa:**Sistem berhasil mendeteksi pintu yang dibuka secara paksa melalui Reed Switch dan mengirimkan notifikasi real-time. Pengguna menerima notifikasi dalam waktu kurang dari 5 detik, memastikan adanya respons yang cepat terhadap ancaman.

Tabel berikut merangkum hasil pengujian notifikasi real-time pada berbagai skenarioBagian Hasil dan Pembahasan memuat hasil-hasil dari penelitian serta pembahasan menyeluruh dari masing-masing hasil yang didapatkan dari penelitian yang dibahas.

TABEL 3. Hasil Pengujian Notifikasi Real-Time

Skenario Deteksi Ancaman	Jarak Pengguna	Waktu Pengiriman Notifikasi
Deteksi getaran di pintu	50 meter	3 detik
Deteksi pintu terbuka paksa	120 meter	4 detik
Deteksi getaran di pintu	280 meter	4 detik
Deteksi pintu terbuka paksa	11 kilometer	5 detik

Hasil pengujian menunjukkan bahwa sistem mampu memberikan notifikasi kepada pengguna dengan waktu pengiriman yang cepat, bahkan ketika pengguna berada jauh dari perangkat. Penggunaan Firebase Realtime Database memungkinkan data dikirim dan

disinkronkan secara real-time, sehingga pengguna dapat segera mengambil tindakan jika terjadi ancaman.

Secara keseluruhan, hasil pengujian notifikasi real-time menunjukkan bahwa sistem ini efektif dalam memberikan peringatan kepada pengguna ketika terjadi ancaman, serta memiliki keandalan yang baik dalam hal kecepatan pengiriman notifikasi.

c. Hasil Pengujian Sistem Monitoring

Pengujian sistem monitoring dilakukan untuk mengevaluasi kemampuan pengguna dalam memantau dan mengendalikan sistem keamanan pintu secara jarak jauh menggunakan aplikasi smartphone. Sistem ini memanfaatkan Firebase Realtime Database sebagai media untuk sinkronisasi data antara perangkat dan aplikasi yang digunakan oleh pengguna. Pengguna dapat memonitor status pintu, mengunci dan membuka pintu, serta menerima notifikasi keamanan secara real-time melalui aplikasi yang terhubung dengan internet.

Gambar 11. Aplikasi Monitoring Yang Digunakan

Gambar ini menunjukkan tampilan utama aplikasi monitoring dan kontrol sistem keamanan pintu berbasis IoT. Gambar ini paling sesuai untuk dimasukkan dalam Bab 4.3 Hasil Pengujian Sistem Monitoring, karena aplikasi ini berfungsi untuk memantau status pintu dan mengendalikan akses pintu dari jarak jauh.

Penjelasan Aplikasi:

Aplikasi ini memiliki beberapa fitur utama yang dapat dilihat dari tampilan di gambar:

1. Tampilan Utama (Main Page):Pada layar aplikasi, terlihat status sistem keamanan pintu dengan indikator apakah sistem dalam keadaan "Aktif" atau "Non-Aktif." Aplikasi ini memungkinkan pengguna untuk memantau keamanan pintu secara real-time melalui konektivitas IoT.
2. Fitur Deteksi Ancaman:Aplikasi memiliki dua fitur utama untuk mendeteksi ancaman, yaitu mendeteksi jika pintu dibuka paksa atau didobrak. Ketika ancaman terdeteksi, status pada aplikasi akan berubah menjadi "Aktif" dengan alarm peringatan menyala. Pengguna dapat mengaktifkan atau menonaktifkan fitur alarm dan deteksi ancaman ini melalui aplikasi secara langsung.
3. Kondisi Fingerprint:Pada bagian bawah layar aplikasi, terdapat status kondisi sensor sidik jari yang menampilkan apakah sensor dalam keadaan hidup dan siap untuk digunakan. Ini memastikan bahwa pengguna dapat memeriksa status sensor sebelum melakukan autentikasi.
4. Kontrol Pintu:Pengguna juga dapat membuka atau mengunci pintu melalui aplikasi, sehingga memudahkan pengendalian pintu dari jarak jauh tanpa perlu berada di lokasi fisik.

Pengujian ini mencakup beberapa aspek, yaitu:

1. Kecepatan Respon Saat Memantau Status Pintu: Pengguna dapat memantau status pintu (terkunci atau terbuka) melalui aplikasi smartphone. Hasil pengujian menunjukkan bahwa status pintu diperbarui dalam waktu kurang dari 1 detik, baik saat pengguna berada dalam jarak dekat maupun jauh dari perangkat.
2. Kecepatan Respon Saat Mengontrol Pintu: Pengguna dapat membuka atau menutup pintu melalui aplikasi mobile. Sistem merespons perintah pengguna dalam waktu yang sangat cepat, dengan rata-rata waktu respon 1 detik, bahkan ketika pengguna berada pada jarak hingga 43 kilometer dari perangkat.
3. Stabilitas Koneksi: Sistem diuji untuk melihat apakah tetap stabil dalam kondisi jarak jauh, baik pada jaringan internet dengan kecepatan yang berbeda. Hasil menunjukkan bahwa tidak ada gangguan signifikan pada koneksi antara perangkat dan aplikasi selama pengujian.

Tabel berikut merangkum hasil pengujian sistem monitoring:

TABEL 4. Hasil Pengujian Sistem Monitoring

Aksi	Jarak Pengguna	Waktu Respon
Membuka pintu melalui aplikasi	43 kilometer	1 detik
Menutup pintu melalui aplikasi	43 kilometer	1 detik
Membuka pintu melalui aplikasi	280 meter	1 detik
Menutup pintu melalui aplikasi	280 meter	1 detik

Hasil pengujian ini menunjukkan bahwa sistem monitoring berfungsi dengan baik, memungkinkan pengguna untuk mengontrol akses pintu secara jarak jauh dengan waktu respon yang cepat dan koneksi yang stabil. Firebase Realtime Database memastikan bahwa setiap perubahan status pintu disinkronkan dengan aplikasi mobile secara real-time, memberikan kemudahan bagi pengguna untuk memantau dan mengontrol sistem kapan saja dan dari mana saja.

d. Hasil Implementasi Sistem

Setelah tahap perancangan dan pengujian sistem selesai, sistem keamanan pintu berbasis Internet of Things (IoT) yang dirancang berhasil diimplementasikan dalam bentuk fisik. Implementasi ini mencakup integrasi seluruh komponen elektronik, perangkat keras, dan perangkat lunak, termasuk NodeMCU, Arduino Nano, sensor sidik jari, keypad, solenoid, dan relay. Gambar berikut menunjukkan hasil implementasi fisik sistem:

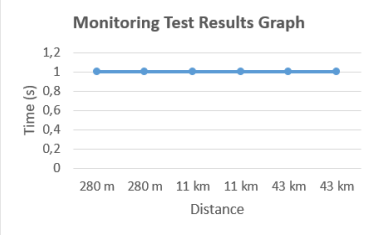
Gambar 12. Implementasi Alat

Gambar di atas menunjukkan implementasi fisik dari sistem keamanan pintu berbasis Internet of Things (IoT). Gambar ini memperlihatkan dua sudut pandang perangkat yang telah dirakit, yaitu tampilan bagian depan dan bagian belakang perangkat:

1. Tampilan Kiri (Bagian Depan): Pada bagian ini terlihat keypad 4x4 yang digunakan untuk memasukkan kata sandi, serta sensor sidik jari yang terletak di bawahnya. Kedua komponen ini merupakan metode autentikasi yang digunakan untuk membuka pintu. Di bawah keypad, terlihat juga indikator LED yang akan menyala hijau ketika akses berhasil diberikan. Tampilan ini menunjukkan sistem siap digunakan oleh pengguna untuk membuka pintu dengan autentikasi sidik jari atau kata sandi
2. Tampilan Kanan (Bagian Belakang):Pada bagian belakang, terlihat susunan komponen elektronik yang terhubung dalam sistem, seperti NodeMCU, Arduino Nano, relay, solenoid, dan kabel penghubung. Komponen-komponen ini terintegrasi untuk mengontrol sistem keamanan pintu, termasuk deteksi ancaman melalui sensor dan pengiriman notifikasi real-time. Tampilan ini menunjukkan bagaimana semua komponen terhubung dan bekerja sama untuk menjalankan fungsi keamanan.

Sistem ini juga diuji dalam kondisi nyata untuk memverifikasi apakah setiap komponen bekerja dengan baik. Implementasi ini mencakup pengujian autentikasi pengguna menggunakan sidik jari dan kata sandi, penguncian dan pembukaan kunci pintu, serta pengiriman notifikasi real-time ke pengguna melalui aplikasi mobile. Berdasarkan hasil pengujian, sistem dapat berfungsi sesuai dengan perancangan dan mampu memberikan tingkat keamanan yang lebih baik dibandingkan dengan sistem kunci konvensional.

Grafik hasil pengujian sistem monitoring juga menunjukkan bahwa waktu respon tetap stabil di angka 1 detik meskipun jarak antara pengguna dan perangkat bertambah. Hal ini dibuktikan oleh Gambar 8 di bawah ini:



Gambar 13. Grafik Hasil Pengujian Monitoring

Grafik di atas menampilkan hasil pengujian waktu respon sistem monitoring pada jarak yang berbeda. Pengujian dilakukan untuk mengevaluasi kecepatan sistem dalam merespons perintah pengguna untuk membuka atau menutup pintu melalui aplikasi mobile. Pengujian dilakukan pada jarak 280 meter, 11 kilometer, dan 43 kilometer.

e. Pembahasan

Berdasarkan hasil pengujian dan implementasi yang telah dilakukan, sistem keamanan pintu berbasis IoT menunjukkan performa yang memuaskan dalam hal autentikasi, monitoring, dan deteksi ancaman. Pada bagian ini, beberapa aspek penting dari hasil implementasi akan dibahas lebih lanjut untuk memahami kekuatan serta potensi perbaikan dari sistem ini.

1. Keandalan Autentikasi

Sistem autentikasi yang menggunakan sensor sidik jari dan keypad menunjukkan tingkat keandalan yang tinggi. Hasil pengujian memperlihatkan bahwa sensor sidik jari mampu mendeteksi sidik jari terdaftar dengan akurasi tinggi dan waktu respon yang cepat, yaitu rata-rata 1,7 detik. Selain itu, keypad juga memberikan hasil yang konsisten dalam menolak akses ketika pengguna memasukkan kata sandi yang salah.

TABEL 5. Hasil Pengujian Fingerprint

No	Aksi	Sudut	Waktu	Hasil
1	Ibu jari terdaftar (kanan)	0o	1,67s	Terdeteksi
2	Jari telunjuk tidak terdaftar (kiri)	0o	2,01s	Tidak terdeteksi
3	Ibu jari terdaftar (kanan)	45o	1,36s	Terdeteksi
4	Jari telunjuk tidak terdaftar (kiri)	45o	2,03s	Tidak terdeteksi
5	Ibu jari terdaftar (kanan)	90o	1,87s	Terdeteksi
6	Jari telunjuk tidak terdaftar (kiri)	90o	1,68s	Tidak terdeteksi
7	Ibu jari terdaftar (kanan)	135o	1,42s	Terdeteksi
8	Jari telunjuk tidak terdaftar (kiri)	135o	1,3s	Tidak terdeteksi
9	Ibu jari terdaftar (kanan)	180o	1,53s	Terdeteksi
10	Jari telunjuk tidak terdaftar (kiri)	180o	2,01s	Tidak terdeteksi
Rata-rata waktu: 1,7 detik				

Meskipun sistem ini sudah cukup baik, tantangan yang mungkin muncul adalah kepekaan sensor terhadap faktor eksternal, seperti kondisi sidik jari yang basah atau kotor, yang bisa mempengaruhi kemampuan sensor dalam mendeteksi. Oleh karena itu, di masa depan, peningkatan performa sensor sidik jari yang lebih tahan terhadap kondisi lingkungan perlu dipertimbangkan.

2. Notifikasi Real-Time yang Efektif

Penggunaan Firebase Realtime Database memungkinkan sistem ini untuk memberikan notifikasi real-time kepada pengguna ketika ada potensi ancaman. Dari hasil pengujian, notifikasi dikirimkan dalam waktu kurang dari 5 detik, bahkan ketika pengguna berada pada jarak yang jauh dari perangkat. Hal ini menunjukkan bahwa sistem ini mampu menjaga konektivitas dan memberikan informasi yang cepat dan tepat kepada pengguna.

Berikut adalah tabel hasil pengujian kecepatan pengiriman pesan notifikasi

TABEL 6. Hasil Pengujian Kecepatan Pengiriman Pesan Notifikasi

No	Aksi	Jarak	Waktu	Hasil
1	Mendeteksi ketika pintu didobrak	11 km	5s	Terkirim
2	Mendeteksi ketika pintu berhasil dibuka paksa	11 km	4s	Terkirim
3	Mendeteksi ketika pintu didobrak	280 m	4s	Terkirim
4	Mendeteksi ketika pintu berhasil dibuka paksa	280 m	4s	Terkirim
5	Mendeteksi ketika pintu didobrak	120 m	3s	Terkirim
6	Mendeteksi ketika pintu berhasil dibuka paksa	120 m	4s	Terkirim
7	Mendeteksi ketika pintu didobrak	50 m	3s	Terkirim
8	Mendeteksi ketika pintu berhasil dibuka paksa	50 m	3s	Terkirim

Namun, ada potensi ketergantungan terhadap koneksi internet yang perlu diperhatikan. Dalam kondisi jaringan internet yang tidak stabil, waktu pengiriman notifikasi mungkin akan meningkat atau bahkan gagal terkirim. Solusi potensial untuk masalah ini adalah menyediakan sistem notifikasi cadangan menggunakan pesan SMS atau metode alternatif lainnya.

3. Pengendalian Jarak Jauh

Sistem monitoring jarak jauh yang terhubung dengan aplikasi smartphone memungkinkan pengguna untuk mengontrol pintu dari mana saja. Hasil pengujian menunjukkan bahwa perintah pengguna untuk membuka atau menutup pintu dapat dieksekusi dengan waktu respon rata-rata 1 detik, tanpa adanya perbedaan signifikan meskipun jarak pengguna dari perangkat bervariasi. Namun, dalam jangka panjang, perlu dipastikan bahwa sistem ini tetap aman dari potensi serangan siber. Sebagai sistem berbasis IoT, penting untuk memperbarui mekanisme enkripsi dan keamanan data untuk mencegah akses tidak sah dari pihak luar.

4. Keamanan Tambahan dari Deteksi Ancaman

Sistem ini berhasil mendeteksi ancaman fisik melalui sensor getar dan Reed Switch yang diintegrasikan ke dalam perangkat. Deteksi getaran dan upaya membuka pintu secara paksa memberikan perlindungan tambahan kepada pengguna. Notifikasi real-time yang dihasilkan dari deteksi ini sangat membantu pengguna untuk segera mengambil tindakan. Namun, sistem ini belum memiliki mekanisme untuk mencegah perusakan fisik yang lebih lanjut setelah deteksi awal.Untuk meningkatkan keamanan lebih jauh, sistem dapat dilengkapi dengan fitur tambahan seperti kamera pengawas atau pengiriman data ke server pusat untuk mencatat log aktivitas yang lebih rinci.

5. Potensi Pengembangan Lebih Lanjut

Meskipun sistem ini telah menunjukkan performa yang sangat baik, masih ada ruang untuk pengembangan lebih lanjut. Salah satu rekomendasi adalah menambahkan fitur backup daya menggunakan baterai atau sumber energi alternatif untuk memastikan sistem tetap berfungsi saat terjadi pemadaman listrik. Selain itu, pengintegrasian sistem dengan teknologi rumah pintar yang lebih luas, seperti pengontrol lampu atau sistem alarm, akan memberikan nilai tambah bagi pengguna.Pengembangan lain yang perlu dipertimbangkan adalah memperluas cakupan autentikasi dengan memasukkan teknologi pengenalan wajah atau suara, yang akan meningkatkan fleksibilitas pengguna dalam memilih metode autentikasi yang lebih nyaman dan aman.

Dari hasil pengujian, terlihat bahwa waktu respon sistem tetap konsisten di angka 1 detik, tanpa adanya penurunan performa meskipun jarak pengguna dari perangkat meningkat. Hal ini menunjukkan bahwa penggunaan Firebase Realtime Database dan konektivitas internet yang stabil mampu menjaga kinerja sistem monitoring tetap optimal, bahkan pada jarak yang jauh.

4. KESIMPULAN

Sistem keamanan pintu berbasis Internet of Things (IoT) yang dirancang telah menunjukkan performa yang baik dalam autentikasi, deteksi ancaman, dan pengiriman notifikasi real-time. Sistem ini berhasil mengintegrasikan sensor sidik jari dan keypad untuk autentikasi, serta sensor getar dan reed switch untuk mendeteksi usaha pembobolan, dengan waktu respon yang cepat dan akurat. Pengujian menunjukkan bahwa waktu pengiriman notifikasi rata-rata adalah 3,75 detik, memastikan pengguna dapat menerima peringatan secara tepat waktu meskipun berada jauh dari lokasi perangkat.

Dengan keandalannya, sistem ini dapat diandalkan untuk meningkatkan keamanan rumah atau bangunan, namun pengembangan lebih lanjut diperlukan untuk meningkatkan daya tahan dan menghadapi kondisi ekstrem..

UCAPAN TERIMAKASIH

Penulis mengucapkan terima kasih yang sebesar-besarnya kepada Fakultas Ilmu Komputer, Universitas Lancang Kuning, atas dukungan dan fasilitas yang telah diberikan sehingga penelitian ini dapat terselenggara dengan baik. Dukungan dalam bentuk sumber daya, bimbingan, dan infrastruktur penelitian sangat membantu dalam penyelesaian proyek ini. Terima kasih juga kepada semua pihak yang telah berkontribusi, baik secara langsung maupun tidak langsung, dalam mendukung keberhasilan penelitian ini.

DAFTAR PUSTAKA

[1] V. Vujović and M. Maksimović, "Raspberry Pi as a Sensor Web node for home automation," *Comput. Electr. Eng.*, vol. 44, pp. 153–171, 2015, doi: 10.1016/j.compeleceng.2015.01.019.

[2] N. Nasution, M. Rizal, D. Setiawan, and M. A. Hasan, "IoT Dalam Agrobisnis Studi Kasus : Tanaman Selada Dalam Green House," *It J. Res. Dev.*, vol. 4, no. 2, pp. 86–93, 2019, doi: 10.25299/itjrd.2020.vol4(2).3357.

[3] N. Nasution, Sri Utami Lestari, and Mhd Arief Hasan, "Penerapan Teknologi Otomatisasi dalam Pertanian Agrotech Farm System," *Din. J. Pengabdi. Kpd. Masy.*, vol. 5, no. 6, pp. 1361–1373, Dec. 2021, doi: 10.31849/dinamisia.v5i6.7752.

[4] N. K. Ningrum and A. Basyir, "Perancangan Sistem Keamanan Pintu Ruangan Otomatis Menggunakan RFID Berbasis Internet of Things (IoT)," *J. Ilm. Matrik*, vol. 24, no. 1, pp. 21–27, 2022.

[5] K. Anggoro, J. Triyono, and S. Raharjo, "Implementasi IoT Sistem Pemantauan dan Kendali Pintu Otomatis Berdasarkan Kedekatan Objek," *J. Scr.*, vol. 9, no. 1, pp. 32–43, 2021.

[6] W. Kurniasih, A. Rakhman, and I. Salamah, "Sistem Keamanan Pintu dan Jendela Rumah Berbasih IoT," *Jurasik (Jurnal Ris. Sist. Inf. dan Tek. Inform.*, vol. 5, no. 2, pp. 266–274, 2020.

[7] R. Zulfikar, S. Sukardi, R. Mukhaiyar, and D. E. Myori, "Rancang Bangun Keamanan Pintu Otomatis Menggunakan Face Recognition Berbasis Internet Of Things (IoT)," *JTEIN J. Tek. Elektro Indones.*, vol. 4, no. 2, pp. 445–453, 2023.

[8] M. A. Hasan, N. Nasution, and D. Setiawan, "Game Bola Tangkis Berbasis Android Menggunakan App Inventor," 2017.

[9] A. I. G. M. Luigi Atzory, "The internet of things: a survey," *Inf. Syst. Front.*, vol. 17, no. 2, pp. 243–259, 2015, doi: 10.1007/s10796-014-9492-7.

[10] A. Satish, "Arduino based smart irrigation system using iot," no. December, 2017.

[11] M. Angelia, K. Setiono, Y. Setevannus, and J. Andry, "Audit Sistem Informasi Absensi Pada Pt Sinar Pratama Agung Menggunakan Kerangka Kerja Cobit 4.1," vol. Vol. 4, No, no. 2, pp. 163–171, 2018, [Online]. Available: http://ejournal.uin-suska.ac.id/index.php/RMSI/article/view/5690