TRANSMISI: JURNAL ILMIAH TEKNIK ELEKTRO, 28, (4), OKTOBER 2026
p-ISSN 1411-0814 e-ISSN 2407-6422

RANCANG BANGUN SISTEM KEAMANAN PINTU RUMAH DENGAN OTENTIKASI GANDA BERBASIS *INTERNET OF THINGS*

Muhammad Naufal Farras dan Aryo Baskoro Utomo*)

Teknik Elektro, Universitas Negeri Semarang, Semarang, Indonesia

*)*E-mail: aryobaskoro@mail.unnes.ac.id*

Abstrak

Pintu merupakan akses utama untuk masuk ke dalam rumah. Sistem keamanan dari pintu penting untuk diterapkan. Untuk meningkatkan keamanan pada sistem keamanan pintu rumah salah satunya dapat menerapkan penggunaan teknologi biometrik seperti sidik jari. Penggunaan mekanisme otentikasi ganda juga dapat meningkatkan keamanan pintu di mana tidak hanya mengandalkan satu *input* saja untuk membuka kunci pintu. Teknologi *Internet of Things* (IoT) juga dapat dikolaborasikan untuk dapat mengendalikan pintu rumah secara jarak jauh. Penelitian ini bertujuan membangun sistem keamanan pintu rumah menggunakan mekanisme otentikasi ganda yang dilengkapi dengan pengendalian jarak jauh berbasis IoT. Pada mekanisme otentikasi ganda *input* yang digunakan adalah sensor sidik jari dan nomor *pin* yang menggunakan *keypad*. Pada pengendalian jarak jauh menggunakan aplikasi yang berbasis *website*. Alat sistem keamanan pintu rumah pada penelitian ini dapat berjalan dengan baik sesuai dengan perancangan yang telah dilakukan. Otentikasi ganda dan pengendalian jarak jauh berbasis IoT menggunakan aplikasi juga telah berhasil diterapkan. Rata-rata jeda waktu untuk membuka kunci pintu menggunakan otentikasi ganda adalah sebesar 0,59 detik.

Kata kunci: sistem keamanan pintu rumah, otentikasi ganda, biometrik, internet of things

Abstract

The door is the main access to enter the house. It is important to implement a security system for the door. One way to improve the security of a home door security system is to use biometric technology such as fingerprint. The use of dual authentication mechanisms can also improve door security, as it does not rely on a single input to unlock the door. Internet of Things (IoT) technology can also be used to control the home door remotely. This research study aims to develop a home door security system using a dual authentication mechanism equipped with IoT-based remote control. In the dual authentication mechanism, the inputs used are a fingerprint sensor and a pin numbers using a keypad. For remote control, a web-based application is used. The home door security system developed in this research study operates effectively according to the design specifications. The dual authentication and IoT-based remote control using application have been successfully implemented. The average time delay to unlock the door using dual authentication is 0,59 seconds.

Keywords: home door security system, dual authentication, biometric, internet of things

1. Pendahuluan

Rumah menjadi tempat bagi manusia untuk istirahat, berkumpul, dan menjalani kehidupan sehari-hari. Kenyamanan dan keamanan rumah sangat penting untuk diperhatikan. Salah satu komponen utama pada rumah adalah pintu. Pintu berfungsi sebagai akses utama keluar dan masuk serta pengaman rumah agar pihak yang tidak berkepentingan tidak dapat masuk ke dalam rumah [1]. Sistem keamanan pintu rumah umumnya masih mengandalkan kunci berbentuk fisik, namun penggunaan kunci seperti ini masih memiliki sejumlah kelemahan seperti kehilangan, kerusakan, pencurian, dan kerentanan terhadap pembobolan [2].

Teknologi otentikasi biometrik dikombinasikan dengan *Internet of Things* (IoT) menjadi salah satu solusi untuk keterbatasan penggunaan kunci fisik. Teknologi biometrik digunakan untuk menganalisis fisik dan sikap manusia untuk proses otentikasi seperti pengenalan pola wajah, pengenalan sidik jari, tanda tangan, dan cara mengetik [3]. IoT memungkinkan perangkat jaringan untuk mengumpulkan dan mengirimkan data dengan bantuan sensor dan aktuator [4], termasuk memungkinkan pengendalian pintu rumah secara jarak jauh menggunakan gawai atau *smartphone* melalui jaringan internet [5].

Berbagai penelitian sebelumnya telah mengembangkan sistem keamanan pintu rumah dengan berbagai pendekatan otentikasi, seperti penggunaan *face recognition* atau pengenalan wajah [2], penggunaan sensor sidik jari [6][7][8][9] penggunaan nomor *pin* menggunakan *keypad* [8], dan penggunaan *Near Field Communication* (NFC) [9]. Pada beberapa penelitian juga telah menerapkan

penggunaan teknologi IoT seperti pengendalian jarak dekat menggunakan modul *bluetooth* [6], dan pemberitahuan status keamanan kepada pemilik rumah melalui *Short Message Service* (SMS) [10].

Sebagian besar penelitian terdahulu masih hanya menerapkan satu metode otentikasi dalam sistem keamanannya[2][7][8][9]. Hal tersebut menimbulkan celah keamanan di mana jika satu otentikasi gagal atau dibobol maka sistem menjadi rentan. Belum banyak penelitian yang secara khusus membahas tentang mengintegrasikan otentikasi ganda (*multi-factor authentication*) berbasis biometrik dan nomor *pin* secara bersamaan dalam satu sistem keamanan pintu rumah berbasis IoT. Salah satu penelitian ditemukan membahas sistem keamanan pintu dengan kombinasi penggunaan sensor sidik jari dan *keypad* berbasis IoT [11], namun belum menerapkan mekanisme otentikasi ganda. Penggunaan otentikasi ganda dinilai efektif dalam meningkatkan keamanan karena memerlukan verifikasi lebih dari satu mekanisme *input* sebelum membuka kunci pintu rumah [12]. Selain itu, minimnya fitur seperti pengendalian pintu secara jarak jauh melalui *website*, pengambilan gambar melalui kamera, serta notifikasi *real-time* ke pemilik rumah juga menjadi keterbatasan pada penelitian sebelumnya.

Penggunaan IoT merupakan langkah tepat untuk mengatasi keterbatasan pada penelitian sebelumnya. Penggunaan IoT memungkinkan sistem keamanan pintu rumah dapat terhubung langsung ke jaringan internet, sehingga pemilik rumah dapat memantau, mengendalikan, dan menerima notifikasi dari jarak jauh secara *real-time* [13]. Integrasi IoT dengan mekanisme otentikasi ganda juga dapat meningkatkan fleksibilitas dan keamanan karena proses otentikasi dapat berjalan otomatis dan setiap pengguna yang melakukan otentikasi tercatat dalam basis data yang telah terhubung dengan sistem. Dengan demikian, penggunaan IoT dapat memberikan solusi terhadap kebutuhan keamanan sekaligus menutup celah keamanan sistem pada penelitian sebelumnya.

Penelitian ini bertujuan untuk merancang dan membuat sistem keamanan pintu rumah berbasis IoT dengan otentikasi ganda yang mengombinasikan penggunaan sensor sidik jari dan *input* nomor *pin*. Sidik jari dipilih karena sidik jari memiliki tingkat keunikan yang tinggi dan tidak mudah untuk dipalsukan, sementara nomor *pin* digunakan sebagai lapisan verifikasi tambahan yang mudah untuk diingat dan bersifat fleksibel. Otentikasi ganda digunakan sebagai keamanan ganda pada pintu rumah sebelum kunci pintu terbuka dengan menggunakan 2 jenis *input* berbeda yang mengharuskan kedua *input* memberikan hasil verifikasi yang valid. Sistem ini memungkinkan pengguna untuk mengendalikan pintu rumah secara jarak jauh dengan IoT melalui aplikasi berbasis *website* untuk melakukan membuka atau mengunci pintu, mengambil gambar, dan pengiriman notifikasi.

2. Metode

Penelitian ini dilakukan dengan merancang dan membangun sistem keamanan pintu rumah berbasis IoT dengan menerapkan mekanisme otentikasi ganda. Sistem ini menggunakan dua jenis *input* sebagai verifikasi keamanan, yaitu sensor sidik jari dan nomor *pin* 6 digit angka. Perangkat utama yang digunakan dalam sistem ini adalah mikrokontroler ESP32 yang terintegrasi dengan kamera ESP32-CAM. ESP32 digunakan sebagai pengendali utama untuk mengontrol logika, komunikasi jaringan, serta pemrosesan data *input*. Kamera ESP32-CAM digunakan untuk mengambil gambar aktivitas otentikasi sistem.

Teknologi IoT diterapkan dalam bentuk aplikasi berbasis *website* yang dibangun menggunakan React.js dan Next.js. *Website* ini memungkinkan pengguna mengendalikan sistem secara jarak jauh menggunakan jaringan internet dengan fitur seperti membuka kunci pintu, melihat hasil tangkapan kamera, serta menerima notifikasi status dari sistem. Untuk penyimpanan data dan otentikasi pengguna pada aplikasi menggunakan basis data Firebase.

Metode pengujian yang digunakan dalam penelitian ini adalah pengujian *black box*, yaitu metode yang berfokus pada spesifikasi fungsional sistem. Pengujian *black box* hanya memeriksa kesesuaian antara *input* dan *output* sistem sesuai dengan kebutuhan yang telah dilakukan [14]. Fokus utama dari pengujian *black box* dalah memastikan bahwa setiap fungsi dalam perangkat bekerja sebagaimana mestinya, dengan validasi terhadap masukan dan keluaran yang ditentukan oleh spesifikasi [15]. Tujuan dari pengujian ini adalah untuk memastikan bahwa sistem merespons secara benar terhadap *input* yang vaild maupun tidak valid sesuai dengan rancangan sistem.

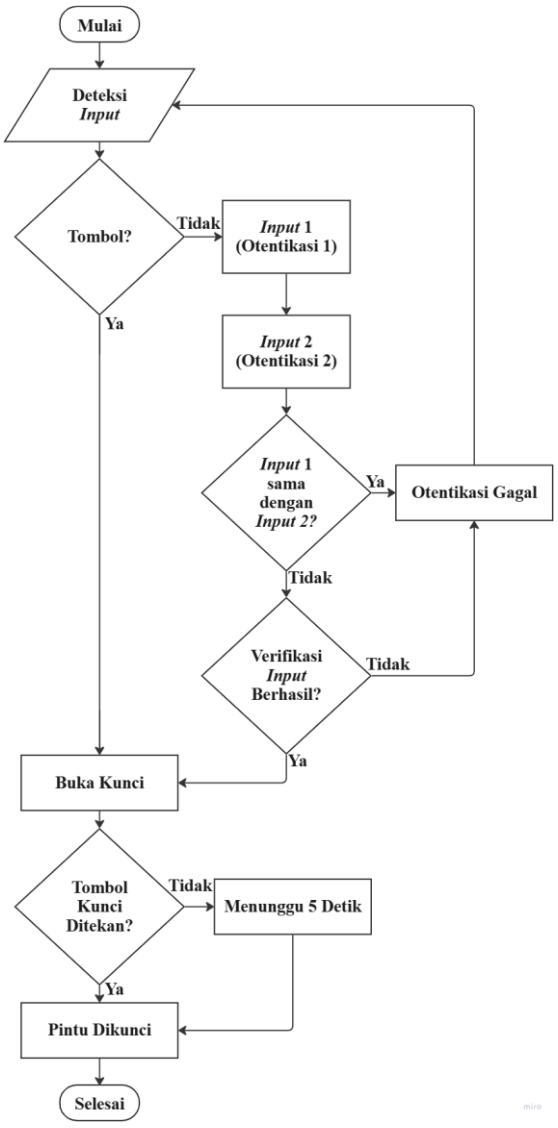
2.1. *Flowchart* Sistem

Gambar 1 menunjukkan *flowchart* sistem yang menjelaskan bagaimana sistem bekerja. Pada langkah awal, sistem akan mendeteksi *input* yang masuk. Jika *input* adalah tombol untuk membuka kunci pintu maka kunci pintu akan langsung terbuka. Selain tombol, *input* seperti sidik jari dan *pin* akan melalui tahapan otentikasi ganda. Antara sidik jari dan nomor *pin* dapat digunakan bergantian pada *input* 1 dan *input* 2. Namun, pada tahapan *input* 1 dan 2 tidak dapat menggunakan *input* yang sama atau otentikasi akan dinyatakan gagal. Pada proses verifikasi *input*, apabila terjadi kesalahan verifikasi seperti sidik jari yang salah atau nomor *pin* yang salah akan ada kesempatan sebanyak 3 kali. Jika salah lebih dari 3 kali maka otentikasi dinyatakan gagal dan mengharuskan mengulang dari awal proses otentikasi.

Ketika kunci pintu berhasil terbuka, terdapat dua cara untuk membuat pintu rumah kembali terkunci. Jika menekan tombol kembali, maka pintu rumah akan

langsung terkunci kembali. Namun jika tidak, maka secara otomatis sistem akan menunggu selama 5 detik sebelum pada akhirnya pintu akan kembali terkunci.

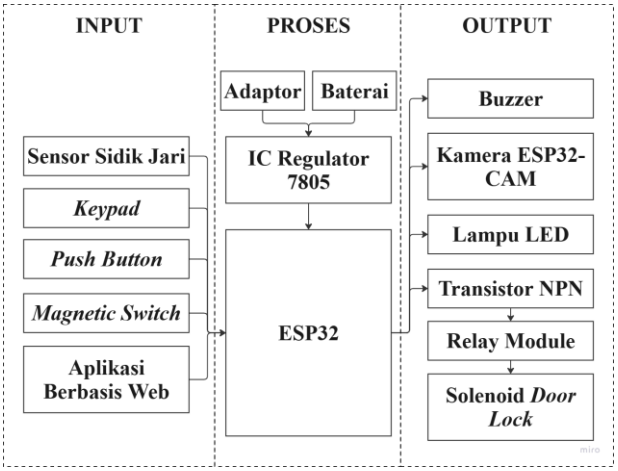
Di dalam sistem terdapat beberapa indikator proses berjalannya sistem, seperti *buzzer* untuk indikator proses verifikasi *input* berhasil atau gagal dan indikator pintu terbuka atau tertutup. Indikator lain adalah lampu LED untuk menandakan kondisi kunci pintu, ketika LED merah menyala maka pintu dalam keadaan terkunci dan ketika LED hijau menyala maka pintu dalam keadaan tidak terkunci.



Gambar 1. *Flowchart* Sistem

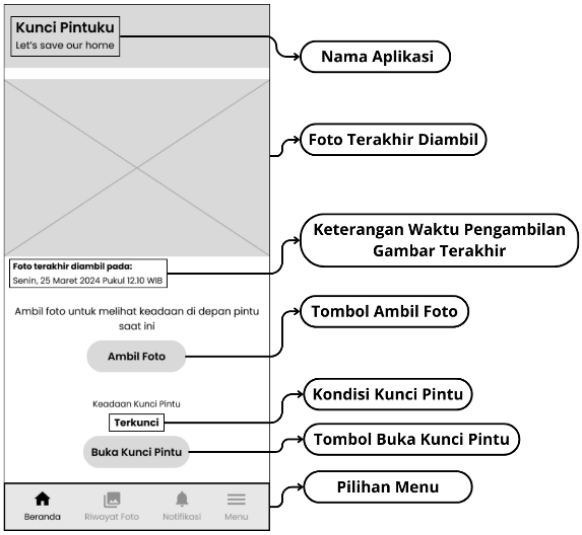
2.2. Diagram Blok

Gambar 2 menunjukkan diagram blok sistem. Alat yang dibuat memilik adaptor dan baterai yang diturunkan tegangannya menjadi 5V oleh IC regulator 7805 sebagai sumber tegangan ESP32. *Input* yang digunakan adalah sensor sidik jari, *keypad*, *push button*, *magnetic switch*, dan aplikasi berbasis *website*. *Output* yang digunakan antara lain *buzzer*, kamera ESP32-CAM, LED, dan solenoid *door lock* dengan bantuan transistor NPN dan *relay module* sebagai pengontrol kerja dari solenoid.



Gambar 2. Diagram Blok

2.3. Perancangan Perangkat Lunak



Gambar 3. Desain Halaman Beranda Aplikasi

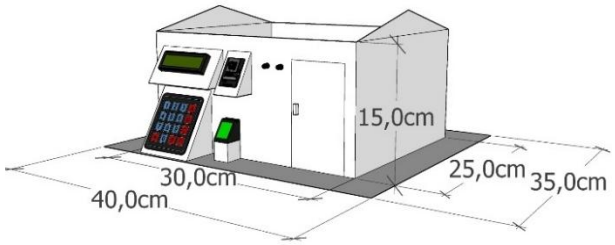
Pada perancangan perangkat lunak, perancangan terdiri dari perancangan aplikasi berbasis *website* untuk pengendalian jarak jauh sistem keamanan rumah dan juga perancangan program untuk ESP32 dan ESP32-CAM. Pada perancangan aplikasi berbasis *website* akan terdapat beberapa halaman seperti halaman *login*, halaman beranda, halaman riwayat foto, halaman notifikasi, halaman menu dan halaman ganti *pin* alat. Proses desain dari halaman-halaman tersebut dibuat sedetail mungkin dengan beberapa keterangan penjelasan yang menunjukkan isi dari halaman-halaman dalam aplikasi tersebut. Gambar 3 menunjukkan desain dari halaman beranda yang akan diterapkan dalam

aplikasi. Selain halaman beranda, terdapat *tab* riwayat foto untuk menyimpan gambar hasil tangkapan kamera yang tersimpan dalam Firebase dan *tab* notifikasi untuk menampilkan riwayat notifikasi dari sistem.

Selain perancangan desain halaman aplikasi, juga dilakukan perancangan untuk program mikrokontroler ESP32 dan ESP32-CAM menggunakan PlatformIO pada aplikasi *desktop* Visual Studio Code. Program akan di *compile* terlebih dahulu sebelum kemudian di *upload* ke dalam ESP32 dan ESP32-CAM. Program ESP32 dan ESP32-CAM yang sudah dirancang pada penelitian ini dapat dilihat dan diunduh pada *link* bit.ly/doorlockesp32 dan bit.ly/doorlockesp32cam.

2.4. Perancangan Perangkat Keras

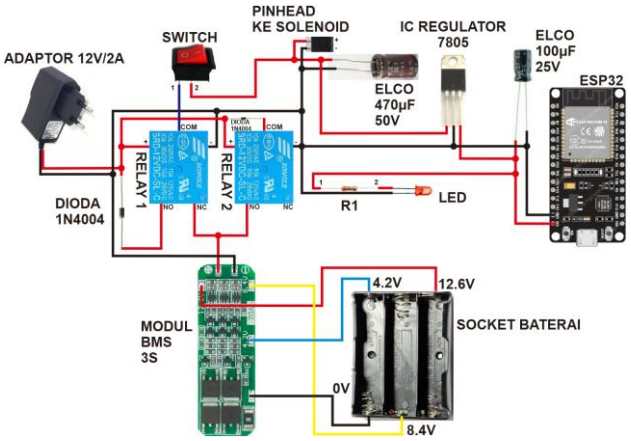
Pada perancangan perangkat keras dilakukan perancangan desain alat dengan bentuk maket rumah. Selain itu juga dilakukan perancangan rangkaian *supply* 12V & 5V sebagai sumber tegangan untuk alat dan juga rangkaian keseluruhan dari sistem keamanan pintu rumah. Beberapa komponen berada di luar maket rumah antara lain *keypad*, LCD, sensor sidik jari, ESP32-CAM, dan LED indikator. Sedangkan komponen sisanya berada di dalam maket rumah. Terdapat pintu pada maket rumah sebagai simulasi untuk membuka dan menutup pintu. Desain maket rumah berukuran panjang 30 cm, lebar 25 cm, dan tinggi 20 cm termasuk dengan atapnya. Alas pada desain maket rumah ini berukuran panjang 40 cm dan lebar 35 cm. Desain maket rumah ini dapat dilihat pada Gambar 4.



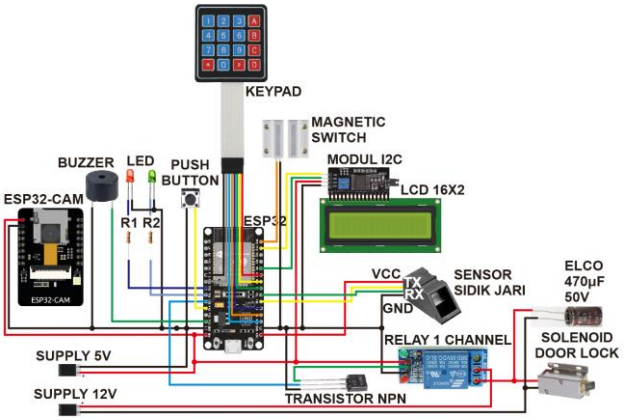
Gambar 4. Desain Maket Rumah

Pada perancangan rangkaian *supply* 12V dan 5V sebagai sumber tegangan alat terdiri dari beberapa komponen seperti *relay*, *switch*, kapasitor elektrolit, IC 7805, LED, dioda, adaptor, modul BMS, dan baterai 3S. Perancangan rangkaian *supply* 12V dan 5V ditunjukkan pada Gambar 5. Modul BMS digunakan sebagai pengisian ulang baterai dan juga sebagai proteksi dari baterai. Selain menyalurkan tegangan untuk alat, adaptor juga menyalurkan tegangannya untuk pengisian ulang baterai ketika baterai tidak digunakan. Baterai akan digunakan otomatis ketika aliran tegangan dari adaptor terputus.

Selain perancangan rangkaian *supply*, juga dilakukan perancangan untuk rangkaian keseluruhan dari sistem keamanan pintu rumah seperti yang ditunjukkan pada Gambar 6. Rangkaian ini terdiri dari seluruh komponen yang dibutuhkan seperti ESP32, ESP32-CAM, *buzzer*, LED, *push button*, *keypad*, *magnetic switch*, LCD, sensor sidik jari, transistor NPN, modul *relay*, kapasitor elektrolit, dan solenoid *door lock*.



Gambar 5. Perancangan Rangkaian *Supply* 12V & 5V



Gambar 6. Perancangan Rangkaian Keseluruhan Sistem

3. Hasil dan Pembahasan

3.1. Perangkat Keras

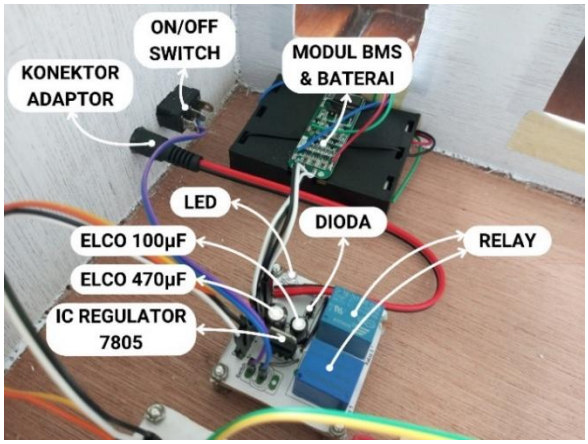
Pembuatan maket rumah sebagai wadah dari alat sistem keamanan pintu rumah dibangun dengan berdasarkan ukuran pada perancangan sebelumnya seperti pada Gambar 7. Penempatan komponen di luar maket rumah disesuaikan dengan desain maket rumah pada perancangan. Untuk penempatan komponen lainnya yang berada di dalam maket rumah disesuaikan dengan ukuran dari maket rumah itu sendiri.

Selain komponen yang berada di luar seperti *keypad*, LCD, ESP32-CAM, sensor sidik jari, dan LED, bagian dalam maket rumah ditempatkan komponen lainnya yang merupakan komponen dari rangkaian *supply* 12V & 5V dan juga rangkaian keseluruhan dari sistem keamanan pintu rumah seperti yang dapat dilihat pada Gambar 8 dan

Gambar 9. Pada kedua rangkaian ini disambungkan antar komponennya menggunakan jalur *layout* PCB dengan ukuran untuk rangkaian *supply* yaitu 5 cm x 5 cm dan untuk rangkaian keseluruhan sistem yaitu 10 cm x 10 cm. Untuk menghubungkan komponen yang berada di luar dengan rangkaian yang berada di dalam maket rumah dengan menggunakan kabel *jumper* dengan ukuran panjang rata-rata 20 cm untuk tiap kabelnya.

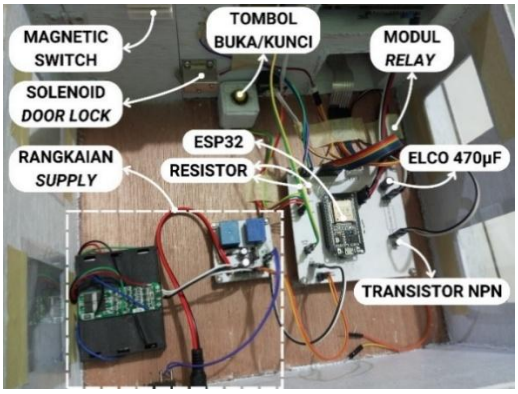


Gambar 7. Maket Rumah



Gambar 8. **Rangkaian *Supply***

Sumber tegangan yang masuk ke dalam rangkaian *supply* 12V & 5V menggunakan adaptor 12V/2A dan baterai 3S. Adaptor digunakan sebagai sumber utama pada alat sistem keamanan pintu rumah yang terhubung langsung dengan listrik PLN. Selain itu, adaptor juga digunakan sebagai pengisian ulang baterai 3S dengan bantuan modul BMS. Ketika listrik PLN terputus, baterai akan langsung menyalurkan tegangannya menggantikan adaptor yang terputus.



Gambar 9. Rangkaian Keseluruhan

3.2. Perangkat Lunak

Program yang dibuat untuk ESP32 dan ESP32-CAM menggunakan PlatformIO berhasil dibuat dan dimasukkan ke dalam ESP32 dan ESP32-CAM. Program yang sudah masuk tersebut berhasil berjalan sesuai dengan cara kerja sistem yang telah disusun sebelumnya pada tahap perancangan.

Untuk komunikasi data, sistem ini memanfaatkan *Firebase Realtime Database* sebagai penghubung antara ESP32 dan ESP32-CAM dengan aplikasi berbasis *website*. Firebase digunakan untuk mengirimkan perintah membuka kunci pintu, mengirimkan perintah mengunci pintu, menerima status kunci pintu, mengirim perintah mengambil gambar dengan ESP32-CAM dan menyimpannya, serta menyimpan riwayat notifikasi aktivitas. Untuk notifikasi aktivitas, seperti proses kunci pintu terbuka, pintu kembali terkunci, dan verifikasi *input* gagal dikelola melalui *Firebase Cloud Messaging* agar notifikasi dapat masuk dalam aplikasi secara *real-time*.

Dalam proses pembuatan aplikasi berbasis *website*, aplikasi *desktop* Visual Studio Code juga digunakan untuk melakukan program membuat setiap halaman untuk aplikasi sistem keamanan pintu rumah. Teknologi yang dipakai dalam pembuatan aplikasi adalah menggunakan React.js dan Next.js dengan bantuan dalam *styling* menggunakan Tailwind CSS. Aplikasi dibuat dengan fokus untuk perangkat *mobile* atau *smartphone* dan diakses dengan menggunakan domain *website* pada umumnya. Untuk dapat menyimpannya sebagai aplikasi pada *smartphone*, aplikasi dapat diunduh langsung pada domain *website* aplikasi tersebut. Gambar 10 menunjukkan halaman beranda aplikasi yang sudah berhasil dibuat. Untuk hasil gambar dan riwayat notifikasi yang tersimpan dalam Firebase juga ditampilkan di aplikasi pada *tab* khusus riwayat foto dan notifikasi.



Gambar 10. Halaman Beranda Aplikasi

3.3. Pengujian dan Analisis Data

Pengujian sistem pada penelitian ini dilakukan dengan 4 buah skenario pengujian, yaitu pengujian sistem dengan *input* nomor *pin* salah hingga 3 kali, pengujian sistem dengan *input* sidik jari salah hingga 3 kali, pengujian sistem dengan kedua *input* yang masuk benar, dan pengujian sistem pemantauan dan pengendalian jarak jauh menggunakan aplikasi berbasis *website*.

Pengujian pertama dilakukan dengan menguji sistem ketika *input* nomor *pin* terdeteksi tidak sesuai atau salah dimasukkan hingga sebanyak 3 kali. Percobaan dilakukan sebanyak 3 kali dengan tiap percobaan terdapat 3 proses kesalahan memasukkan *input* nomor *pin*. Hasil pada pengujian pertama ini tercantum pada Tabel 1. Pada pengujian pertama ini dari 3 kali percobaan seluruhnya menunjukkan hasil yang sesuai dengan cara kerja sistem.

Tabel 1. Pengujian *Input* Nomor *Pin* Salah Hingga 3 Kali

Percobaan ke-	Nomor *Pin*	*Buzzer*	Notifikasi
1	Salah ke-1	Bunyi pendek 3 kali	Tidak terkirim
	Salah ke-2	Bunyi pendek 3 kali	Tidak terkirim
	Salah ke-3	Bunyi pendek 3 kali & panjang 1 kali	Terkirim
2	Salah ke-1	Bunyi pendek 3 kali	Tidak terkirim
	Salah ke-2	Bunyi pendek 3 kali	Tidak terkirim
	Salah ke-3	Bunyi pendek 3 kali & panjang 1 kali	Terkirim
3	Salah ke-1	Bunyi pendek 3 kali	Tidak terkirim
	Salah ke-2	Bunyi pendek 3 kali	Tidak terkirim
	Salah ke-3	Bunyi pendek 3 kali & panjang 1 kali	Terkirim

Pengujian kedua dilakukan dengan menguji sistem ketika *input* sidik jari terdeteksi tidak sesuai atau salah dimasukkan hingga sebanyak 3 kali. Percobaan dilakukan sebanyak 3 kali dengan tiap percobaan terdapat 3 proses kesalahan memasukkan *input* sidik jari. Hasil pada pengujian kedua ini tercantum pada Tabel 2. Pada pengujian kedua ini dari 3 kali percobaan seluruhnya menunjukkan hasil yang sesuai dengan cara kerja sistem.

Tabel 2. Pengujian *Input* Sidik Jari Salah Hingga 3 Kali

Percobaan ke-	Sidik Jari	*Buzzer*	Notifikasi
1	Salah ke-1	Bunyi pendek 3 kali	Tidak terkirim
	Salah ke-2	Bunyi pendek 3 kali	Tidak terkirim
	Salah ke-3	Bunyi pendek 3 kali & panjang 1 kali	Terkirim
2	Salah ke-1	Bunyi pendek 3 kali	Tidak terkirim
	Salah ke-2	Bunyi pendek 3 kali	Tidak terkirim
	Salah ke-3	Bunyi pendek 3 kali & panjang 1 kali	Terkirim
3	Salah ke-1	Bunyi pendek 3 kali	Tidak terkirim
	Salah ke-2	Bunyi pendek 3 kali	Tidak terkirim
	Salah ke-3	Bunyi pendek 3 kali & panjang 1 kali	Terkirim

Pengujian ketiga dilakukan dengan menguji sistem ketika kedua *input* baik sidik jari maupun nomor *pin* yang masuk benar dan sesuai. Percobaan dilakukan sebanyak 4 kali dengan memasukkan *input* bergantian antara sidik jari dan nomor *pin* terlebih dahulu. Hasil pengujian ketiga ini tercantum pada Tabel 3. Pada pengujian ketiga ini, dari 4 kali percobaan seluruhnya menunjukkan hasil yang sesuai dengan yang direncanakan pada *flowchart* sistem.

Tabel 3. Pengujian Kedua *Input* yang Masuk Benar dan Sesuai

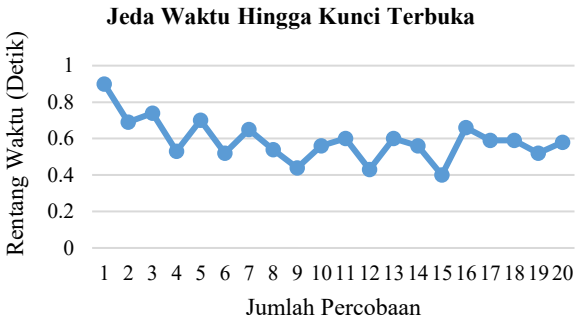
Percobaan ke-	Nomor *Pin*	Sidik Jari	*Buzzer*	Notifikasi	Kunci Pintu	Lampu LED
1	Masuk & sesuai	Belum masuk	Bunyi pendek 3 kali	Belum terkirim	Terkunci	Merah
	Masuk & sesuai	Masuk & sesuai	Bunyi panjang 2 kali	Terkirim	Terbuka	Hijau
2	Masuk & sesuai	Belum masuk	Bunyi pendek 3 kali	Belum terkirim	Terkunci	Merah
	Masuk & sesuai	Masuk & sesuai	Bunyi panjang 2 kali	Terkirim	Terbuka	Hijau
3	Belum masuk	Masuk & sesuai	Bunyi pendek 3 kali	Belum terkirim	Terkunci	Merah
	Masuk & sesuai	Masuk & sesuai	Bunyi panjang 2 kali	Terkirim	Terbuka	Hijau
4	Belum masuk	Masuk & sesuai	Bunyi pendek 3 kali	Belum terkirim	Terkunci	Merah
	Masuk & sesuai	Masuk & sesuai	Bunyi panjang 2 kali	Terkirim	Terbuka	Hijau

Pengujian keempat dilakukan dengan menguji aplikasi berbasis *website* untuk mengendalikan sistem secara jarak jauh menggunakan teknologi IoT. Pengujian dilakukan dengan memberikan beberapa indikator aktivitas pengujian dan harapan pada hasil pengujian. Hasil pengujian keempat ini tercantum pada Tabel 4.

Tabel 4. Pengujian Aplikasi Berbasis *Website*

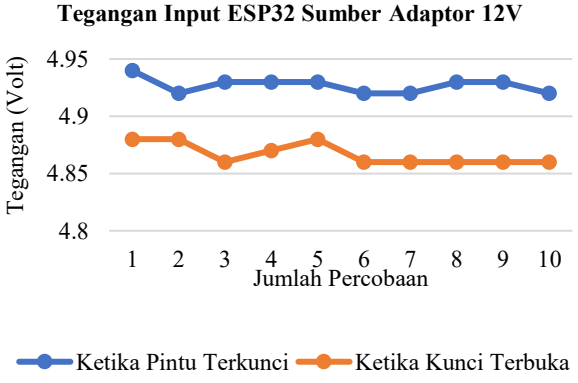
Aktivitas Pengujian	Realisasi yang Diharapkan	Hasil
Masuk halaman *login*	Muncul *form login* untuk masuk ke dalam akun	Sesuai
Masuk dengan akun terdaftar	Jika *email* dan *password* sesuai akan langsung masuk ke halaman beranda, jika tidak muncul peringatan	Sesuai
Masuk halaman beranda	Muncul pengambilan gambar terakhir, tombol ambil gambar, dan tombol membuka kunci pintu rumah	Sesuai
Klik tombol ambil gambar	Ketika gambar berhasil diambil, gambar pada halaman beranda akan *update* otomatis	Sesuai
Klik tombol buka kunci pintu	*Buzzer* akan berbunyi, kunci pintu terbuka, dan notifikasi kunci terbuka terkirim. Ketika pintu kembali terkunci, notifikasi pintu terkunci terkirim	Sesuai
Masuk halaman riwayat foto	Daftar foto akan ditampilkan beserta keterangan waktu pengambilan foto	Sesuai
Masuk halaman notifikasi	Daftar riwayat notifikasi akan ditampilkan	Sesuai
Masuk halaman menu	Muncul tombol ganti nomor *pin* alat dan tombol keluar dari akun	Sesuai
Klik ganti nomor *pin*	Akan muncul *form* mengganti nomor *pin* dengan memasukkan nomor *pin* lama dan nomor *pin* baru	Sesuai
Klik keluar dari akun	Memproses keluar dari akun dan diarahkan kembali ke halaman *login*	Sesuai

Selain pengujian dengan 4 skenario pengujian, juga dilakukan penghitungan jeda waktu ketika kedua *input* yang masuk sesuai hingga kunci terbuka. Penghitungan dilakukan menggunakan alat penghitung waktu *stopwatch*. Gambar 11 menunjukkan grafik dari penghitungan jeda waktu yang diukur melalui 20 kali percobaan pengujian sistem. Dari keseluruhan penghitungan jeda waktu tersebut, jeda waktu rata-rata sistem ketika kedua *input* yang masuk sesuai hingga kunci pintu terbuka sebesar 0,59 detik.



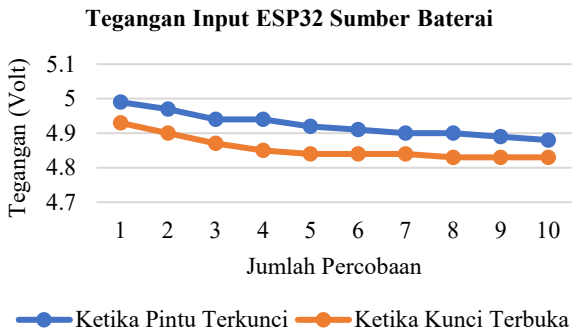
Gambar 11. Grafik Jeda Waktu Hingga Kunci Terbuka

Pada pengujian sistem ini juga dilakukan pengukuran tegangan *input* pada ESP32. Pengukuran ini dilakukan secara manual menggunakan alat ukur multimeter. Pengukuran dilakukan pada 2 kondisi yaitu saat menggunakan sumber tegangan adaptor 12V dan saat menggunakan sumber tegangan baterai. Untuk mengetahui lebih detail pengukuran dilakukan ketika pintu masih terkunci dan ketika kunci pintu terbuka. Gambar 12 dan Gambar 13 menunjukkan grafik hasil dari pengukuran tegangan *input* pada ESP32.



Gambar 12. Grafik Pengukuran Tegangan *Input* ESP32 dengan Sumber Tegangan Adaptor 12V

Dari pengukuran tegangan *input* pada ESP32, ketika menggunakan adaptor 12V rata-rata tegangan *input* saat pintu terkunci sebesar 4,92V dan saat kunci pintu terbuka sebesar 4,87V. Ketika menggunakan baterai, rata-rata tegangan *input* saat pintu terkunci sebesar 4,92V dan saat kunci pintu terbuka sebesar 4,86V. Terjadi perbedaan besarnya tegangan *input* dikarenakan pada saat menggunakan sumber tegangan adaptor 12V, selain untuk menyalurkan tegangan menuju ESP32 adaptor juga menyalurkan tegangan untuk mengisi ulang baterai. Selain itu setelah beberapa kali percobaan, sumber tegangan dari baterai semakin menurun. Hal ini dikarenakan kapasitas baterai yang terus menurun seiring waktu.



Gambar 13. Grafik Pengukuran Tegangan *Input* ESP32 dengan Sumber Tegangan Baterai

3.4. Pembahasan

Pada penelitian ini, hasil pengujian menunjukkan bahwa sistem keamanan pintu rumah berbasis IoT yang dibangun pada penelitian ini dapat bekerja dengan baik. Pengujian skenario 1 hingga skenario 4, seluruhnya menunjukkan hasil pengujian dengan tingkat keberhasilan rata-rata 100%. Hal ini mengindikasikan bahwa sistem keamanan pintu rumah dapat berjalan sesuai dengan perancangan.

Penelitian ini telah menerapkan beberapa saran yang diberikan dari penelitian terdahulu, seperti penerapan teknologi IoT dengan penambahan kamera di depan pintu rumah [7] dan penggunaan ESP32-CAM dengan pengendalian pintu rumah secara jarak jauh menggunakan *smartphone* [8]. Penelitian ini juga memiliki kemiripan dengan salah satu penelitian sebelumnya yang juga menerapkan otentikasi ganda dengan biometrik sidik jari [10]. Perbedaan utamanya terletak pada *input* pendamping, penelitian [10] menggunakan *input* NFC sedangkan pada penelitian ini menggunakan *input* nomor *pin*. Pemilihan penggunaan nomor *pin* dilakukan dengan pertimbangan mudah untuk diingat, tidak memerlukan perangkat tambahan seperti kartu NFC, serta lebih ekonomis karena dapat diimplementasikan pada *keypad* sederhana tanpa tambahan perangkat khusus [16]. Pada penelitian ini memanfaatkan Firebase sebagai media komunikasi antara ESP32 dan ESP32-CAM dengan *server* untuk membuka pintu, mengunci pintu, serta mengambil gambar. Selain itu Firebase juga digunakan untuk menyimpan gambar dan notifikasi yang ditampilkan pada khusus di aplikasi berbasis *website*.

Meskipun demikian, tingkat keberhasilan 100% yang diperoleh masih terbatas pada pengujian menggunakan maket rumah dengan kondisi pencahayaan dan jaringan internet yang stabil. Pengujian pada kondisi lapangan yang lebih kompleks masih diperlukan untuk mengetahui keandalan sistem. Keterbatasan pada penelitian ini meliputi pengujian hanya dilakukan pada *prototipe* bukan pintu rumah sebenarnya, sistem belum diuji pada kondisi lingkungan yang bervariasi, sistem belum dianalisis keandalannya terhadap serangan keamanan digital seperti *brute force*, dan aspek konsumsi daya untuk penggunaan dalam jangka panjang belum dievaluasi.

4. Kesimpulan

Penelitian ini telah berhasil membangun alat sistem keamanan pintu rumah dengan otentikasi ganda berbasis IoT. Alat yang dibangun berbentuk maket rumah dan dapat dikendalikan secara jarak jauh menggunakan aplikasi yang berbasis *website* dengan bantuan teknologi IoT. Beberapa saran yang dapat dipertimbangkan untuk penelitian selanjutnya adalah produk jadi tidak hanya berupa *prototipe*, pengkajian ulang variasi sumber tegangan cadangan, *auto-connect WiFi*, melakukan ujicoba pada kondisi lapangan yang bervariasi dan disarankan menambahkan pengujian keamanan data dari aplikasi berbasis *website*.

Referensi

[1]. A. Ipanhar, T. K. Wijaya, dan P. Gunoto, "Perancangan Sistem Monitoring Pintu Otomatis Berbasis IoT Menggunakan ESP32-CAM," *Sigma Teknika*, vol. 5, no. 2, hlm. 333–350, 2022.

[2]. S. Yedulapuram, R. Arabelli, K. Mahender, dan C. Sidhardha, "Automatic Door Lock System by Face Recognition," *IOP Conf Ser Mater Sci Eng*, vol. 981, no. 3, 2020, doi: 10.1088/1757-899X/981/3/032036.

[3]. M. Iqbal, R. H. Hardyanto, dan P. W. Ciptadi, "Sistem Keamanan Ganda Menggunakan Fingerprint dan Keypad pada Pintu Rumah (Smart Security System)," *Seminar Nasional Dinamika Informatika*, hlm. 175–178, 2021, [Daring]. Tersedia pada: http://senadi.upy.ac.id/prosiding/index.php/senadi/article/view/225

[4]. M. Baláž, K. Kováčiková, A. Novák, dan J. Vaculík, "The Application of Internet of Things in Air Transport," *Transportation Research Procedia*, vol. 75, hlm. 60–67, 2023, doi: 10.1016/j.trpro.2023.12.008.

[5]. A. Rahman dan M. Bagus, "Sistem Kendali Peralatan Elektronik Rumah Tangga Berbasis Internet of Things (IoT) Menggunakan NodeMCU," *Ubiquitous: Computers and its Applications Journal*, vol. 2, hlm. 99–104, 2019, doi: 10.51804/ucaiaj.v2i2.99-104.

[6]. T. Sutikno, M. A. F. Ubaidillah, W. Arsadiando, dan H. S. Purnama, "Fingerprint Based Smart Door Lock System Using Arduino and Smartphone Application," *Computer Science and Information Technologies*, vol. 5, no. 1, hlm. 91–98, Mar 2024, doi: 10.11591/csit.v5i1.pp91-98.

[7]. R. Veliyanti, D. Sasmoko, dan R. Hadi, "Rancang Bangun Sistem Keamanan Pintu Rumah Menggunakan Sidik Jari Sensor dan Arduino," *Seminar Nasional Teknologi dan Multidisiplin Ilmu (SEMNASTEKMU)*, vol. 3, no. 1, hlm. 53–63, Okt 2023, doi: 10.51903/semnastekmu.v3i1.203.

[8]. A. H. P. Yuniarto, Y. Lestiyanti, M. F. Asrori, N. Laela, dan A. Nurcholis, "Perancangan Smart Door Lock System dengan Multi Sensor untuk Sistem Keamanan Rumah," *Techné: Jurnal Ilmiah Elektroteknika*, vol. 22, no. 2, hlm. 333–342, Nov 2023.

[9]. M. Rahayu dan A. I. Irawan, "Autentikasi Ganda pada Sistem Smart Security Home Menggunakan Sidik Jari dan Near Field Communication," *Jurnal Teknologi Rekayasa (JTERA)*, vol. 5, no. 2, hlm. 287, Des 2020, doi: 10.31544/jtera.v5.i2.2020.287-294.

[10]. J. Arifin dan J. Frenando, "Sistem Keamanan Pintu Rumah Berbasis Internet of Things via Pesan Telegram Home Door Security System Based on Internet of Things Through Telegram Message," *TELKA: Jurnal Telekomunikasi, Elektronika, Komputasi dan Kontrol*, vol. 8, no. 1, hlm. 49–59, 2022.

[11]. F. Zaenaldi, A. Subki, A. Akbar, dan L. D. Samsumar, "Sistem Keamanan Pintu Rumah Menggunakan Sidik Jari dan Keypad Berbasis Internet of Things," *Journal of Data Analytics, Information, and Computer Science (JDAICS)*, vol. 1, no. 4, hlm. 215–222, Okt 2024.

[12]. T. Wira dan E. Suryawijaya, "Memperkuat Keamanan Data melalui Teknologi Blockchain: Mengeksplorasi Implementasi Sukses dalam Transformasi Digital di Indonesia Strengthening Data Security through Blockchain Technology: Exploring Successful Implementations in Digital Transformation in Indonesia," *JSKP: Jurnal Studi Kebijakan Publik*, vol. 2, no. 1, hlm. 55–67, 2023, doi: 10.21787/jskp.2.2023.55-67.

[13]. Y. D. Mukin dan P. Noviyanti, "Simulasi Jaringan Smart Home dengan Sistem Berbasis IoT," *Jurnal Komunikasi Sains dan Teknologi*, vol. 2, no. 1, hlm. 63–72, 2023, [Daring]. Tersedia pada: https://journal.proletargroup.org/index.php/JKST

[14]. S. D. Pratama dan M. N. Dadaprawira, "Pengujian Black Box Testing pada Aplikasi Edu Digital Berbasis Website Menggunakan Metode Equivalence dan Boundary Value," *Jurnal Teknologi Sistem Informasi dan Sistem Komputer TGD*, vol. 6, no. 2, hlm. 560–569, Jul 2023, [Daring]. Tersedia pada: https://ojs.trigunadharma.ac.id/index.php/jsk/index

[15]. M. T. Abdillah, I. Kurniastuti, F. A. Susanto, dan F. Yudianto, "Implementasi Black box Testing dan Usability Testing pada Website Sekolah MI Miftahul Ulum Warugunung Surabaya," *Jurnal Ilmu Komputer dan Desain Komunikasi Visual*, vol. 8, no. 1, hlm. 234–242, Jul 2023.

[16]. F. Wadly, "Design Smart Door Locks With Internet Of Things Based On Pin Security Features," *International Journal of Computer Sciences and Mathematics Engineering*, vol. 2, no. 2, hlm. 176–186, Nov 2023, doi: https://doi.org/10.61306/ijecom.v2i2.40.