

RANCANG BANGUN SMART DOOR LOCK BERBASIS DUAL MIKROKONTROLER DENGAN AUTENTIKASI DUA FAKTOR RFID-OTP BERBASIS TELEGRAM

Ridho Nurhadi Pratama, Jonatan Perez Immanuel Siburian, Ramdan Haerullah, Ibrahim Lammada

Teknik Elektro, Universitas Singaperbangsa Karawang

Jl. HS.Ronggo Waluyo Puseurjaya, Telukjambe Timur, Karawang 41361, Indonesia

2210631160066@student.unsika.ac.id

ABSTRAK

Keamanan akses pintu merupakan aspek penting dalam menjaga aset fisik pada lingkungan rumah, perkantoran, maupun fasilitas industri di era modern ini. Sistem konvensional berbasis kunci mekanik dan autentikasi satu faktor masih memiliki kelemahan terhadap risiko duplikasi dan kehilangan kredensial. Selain itu, penggunaan satu mikrokontroler yang menangani proses kontrol perangkat keras dan komunikasi jaringan secara bersamaan berpotensi menurunkan kinerja dan stabilitas sistem. Penelitian ini bertujuan merancang dan membangun sistem *smart door lock* berbasis autentikasi dua faktor menggunakan RFID dan *One-Time Password* (OTP) dengan arsitektur dual mikrokontroler. Sistem dirancang menggunakan metode rancang bangun dengan Arduino Mega 2560 sebagai pengendali utama perangkat keras dan NodeMCU ESP8266 sebagai modul komunikasi untuk pengiriman OTP melalui aplikasi Telegram. Pengujian dilakukan terhadap lima parameter, yaitu akurasi pembacaan RFID, waktu respons sistem, waktu aktuasi servo, waktu komunikasi OTP, dan keberhasilan sistem secara *end-to-end*. Hasil pengujian menunjukkan akurasi pembacaan RFID sebesar 100% pada jarak 1–6 cm, waktu respons rata-rata 9,44 detik, waktu aktuasi servo 0,81 detik, waktu komunikasi OTP 3,81 detik, dan tingkat keberhasilan sistem sebesar 100%. Arsitektur dual mikrokontroler terbukti mampu memisahkan beban kerja secara efektif sehingga sistem berjalan stabil dan responsif.

Kata kunci : dual mikrokontroler; smart door lock; RFID-OTP; autentikasi dua faktor; Telegram bot

1. PENDAHULUAN

Keamanan akses pintu merupakan salah satu aspek fundamental dalam menjaga aset fisik, baik pada lingkungan rumah, perkantoran, maupun fasilitas industri. Seiring perkembangan teknologi, kebutuhan akan sistem keamanan yang lebih andal dan responsif semakin meningkat. Sistem keamanan berbasis elektronik mulai banyak dikembangkan sebagai alternatif dari kunci mekanik konvensional, yang masih memiliki sejumlah keterbatasan seperti risiko kehilangan, duplikasi tanpa izin, serta kerentanan terhadap pembobolan secara fisik [1].

Salah satu teknologi yang banyak diadopsi pada sistem keamanan akses pintu adalah *Radio Frequency Identification* (RFID), yang memungkinkan proses identifikasi pengguna dilakukan secara cepat dan tanpa kontak langsung [2].

Implementasi RFID pada sistem akses pintu terbukti mampu meningkatkan kemudahan operasional [3].

Namun, sistem autentikasi yang hanya bergantung pada satu faktor verifikasi memiliki kelemahan mendasar, yaitu rentan terhadap akses tidak sah apabila kartu RFID hilang, dicuri, atau berhasil diduplikasi oleh pihak yang tidak berwenang [4].

Di sisi lain, sebagian besar penelitian terdahulu yang mengembangkan sistem *smart door lock* masih menggunakan satu mikrokontroler untuk menangani seluruh proses sistem, mulai dari pembacaan sensor, pengolahan data, hingga komunikasi jaringan [5], sehingga berpotensi menimbulkan keterbatasan kinerja ketika harus menangani komunikasi jaringan

yang bersifat non-deterministik secara bersamaan [6]. Selain itu, pengendalian satu faktor autentikasi yang masih banyak digunakan belum sepenuhnya menjamin keamanan akses [7][8].

Berdasarkan permasalahan tersebut, penelitian ini bertujuan merancang dan membangun sistem *smart door lock* yang mampu: (1) menerapkan autentikasi dua faktor berbasis RFID dan *One-Time Password* (OTP) untuk meningkatkan keamanan akses; dan (2) mengimplementasikan arsitektur dual mikrokontroler yang memisahkan proses kontrol perangkat keras dan komunikasi jaringan guna meningkatkan kinerja dan stabilitas sistem.

Untuk mencapai tujuan tersebut, pendekatan autentikasi dua faktor (*two-factor authentication*) diterapkan dengan mengombinasikan RFID sebagai faktor kepemilikan dan OTP sebagai faktor verifikasi dinamis [9].

Kode OTP dibangkitkan secara acak dan dikirimkan kepada pengguna melalui aplikasi Telegram menggunakan modul NodeMCU ESP8266 [10][11].

Sementara itu, Arduino Mega 2560 berperan sebagai pengendali utama yang menangani seluruh proses kontrol perangkat keras secara deterministik, terpisah dari proses komunikasi jaringan yang bersifat non-deterministik. Pendekatan arsitektur dual mikrokontroler ini diharapkan mampu mengatasi keterbatasan kinerja yang ditemukan pada penelitian-penelitian sebelumnya, sekaligus menghadirkan sistem keamanan akses pintu yang lebih andal, responsif, dan aman. Kontribusi utama penelitian ini

meliputi: (1) implementasi pembagian beban kerja antara dua mikrokontroler; (2) integrasi RFID dan OTP berbasis Telegram sebagai autentikasi dua faktor; serta (3) evaluasi kuantitatif kinerja sistem melalui lima parameter pengujian sebagai indikator keandalan.

2. TINJAUAN PUSTAKA

Perancangan sistem *smart door lock* berbasis autentikasi dua faktor memerlukan pemahaman terhadap beberapa konsep dasar yang saling terkait. Landasan teori yang dikaji pada bagian ini meliputi sistem keamanan akses pintu, *embedded system*, arsitektur multi mikrokontroler, teknologi RFID, serta konsep *two-factor authentication* dengan *One-Time Password* (OTP). Selain itu, kajian terhadap penelitian terdahulu juga disertakan untuk menunjukkan posisi dan kebaruan penelitian ini di antara studi yang telah dilakukan sebelumnya.

2.1. Sistem Keamanan Akses Pintu

Sistem keamanan akses pintu merupakan komponen penting dalam perlindungan aset fisik, khususnya pada lingkungan yang membutuhkan kontrol akses secara otomatis dan *real-time* [8].

Perkembangan teknologi telah mendorong peralihan sistem keamanan dari berbasis mekanik menuju berbasis elektronik, dengan memanfaatkan mikrokontroler dan sensor sebagai komponen utama [1].

Secara umum, metode autentikasi pengguna pada sistem keamanan diklasifikasikan menjadi tiga kategori, yaitu berbasis pengetahuan (PIN atau kata sandi), berbasis kepemilikan (kartu akses atau token), dan berbasis karakteristik biometrik [4].

Sistem autentikasi satu faktor memiliki keterbatasan karena hanya bergantung pada satu elemen verifikasi, sehingga risiko akses tidak sah meningkat apabila faktor tersebut berhasil dikompromikan [7].

Untuk itu, pendekatan autentikasi yang lebih kuat diperlukan dengan mengombinasikan dua kategori berbeda guna memberikan lapisan perlindungan tambahan [9].

2.2. Embedded System

Embedded system merupakan sistem berbasis mikrokontroler yang dirancang untuk menjalankan fungsi spesifik dalam suatu perangkat dengan keterbatasan sumber daya, seperti kapasitas memori, kecepatan pemrosesan, dan konsumsi daya [12].

Karakteristik tersebut menuntut perancangan sistem yang efisien dan terstruktur agar setiap proses dapat berjalan secara optimal sesuai dengan kebutuhan aplikasi.

Pada sistem keamanan akses pintu, *embedded system* berperan dalam memproses input dari sensor, mengolah data, dan menggerakkan aktuator secara *real-time*, sehingga aspek waktu respons dan keandalan menjadi parameter penting dalam perancangannya [13].

Namun, ketika kompleksitas fungsi sistem meningkat, penggunaan satu mikrokontroler untuk menangani pembacaan sensor, komunikasi data, dan pengendalian aktuator secara bersamaan dapat menyebabkan beban pemrosesan yang tinggi serta menurunkan stabilitas operasional sistem [6].

Kondisi ini menjadi dasar pengembangan pendekatan arsitektur yang mampu mendistribusikan beban kerja sistem secara lebih efisien, yang akan dijelaskan lebih lanjut pada sub-bab berikutnya

2.3. Arsitektur Multi Kontroler

Arsitektur multi mikrokontroler merupakan pendekatan perancangan sistem *embedded* yang menggunakan lebih dari satu unit pengendali untuk menangani fungsi yang berbeda secara terpisah, dengan tujuan mendistribusikan beban kerja sistem agar setiap mikrokontroler dapat bekerja optimal sesuai tugasnya [14].

Pendekatan ini umum diterapkan pada sistem yang memiliki kombinasi proses bersifat deterministik, seperti pembacaan sensor dan pengendalian aktuator, dengan proses non-deterministik, seperti komunikasi jaringan [15].

Pemisahan fungsi antar mikrokontroler memungkinkan pengendali utama tetap berfokus pada proses kontrol perangkat keras tanpa terganggu oleh latensi yang ditimbulkan oleh proses komunikasi jaringan. Komunikasi antar mikrokontroler umumnya dilakukan melalui antarmuka serial seperti UART, I2C, atau SPI, yang memungkinkan pertukaran data secara *real-time* dengan kompleksitas implementasi yang relatif rendah [16].

Selain meningkatkan stabilitas dan responsivitas sistem, pendekatan ini juga memberikan fleksibilitas pengembangan karena setiap modul dapat dimodifikasi secara independen tanpa memengaruhi keseluruhan sistem [14].

2.4. Radio Frequency Identification (RFID)

Radio Frequency Identification (RFID) merupakan teknologi identifikasi otomatis yang memanfaatkan gelombang radio untuk membaca dan mengirimkan data dari sebuah *tag* ke perangkat pembaca (*reader*) tanpa memerlukan kontak langsung [2].

Sistem RFID umumnya terdiri dari tiga komponen utama, yaitu *tag*, *reader*, dan antena, yang bekerja secara terintegrasi dalam proses identifikasi pengguna [3].

Pada penerapannya, *tag* RFID menyimpan informasi identitas unik (UID) yang dapat dibaca oleh *reader* ketika berada dalam jangkauan tertentu, sehingga proses autentikasi dapat dilakukan secara cepat dan praktis [17].

Karakteristik tersebut menjadikan RFID banyak digunakan pada sistem kontrol akses karena kemampuannya memberikan identifikasi yang akurat dengan waktu respons yang singkat [3][17]

Dalam penelitian ini, RFID berperan sebagai faktor kepemilikan (*something you have*) yang menjadi tahap awal proses autentikasi sebelum dilanjutkan dengan verifikasi faktor kedua.

2.5. Two Factor Authentication

Two-Factor Authentication (2FA) merupakan metode autentikasi yang memverifikasi identitas pengguna dengan mengombinasikan dua kategori faktor verifikasi yang berbeda, misalnya kepemilikan dan pengetahuan dinamis [9].

Pendekatan ini memberikan lapisan keamanan tambahan karena akses tidak dapat diperoleh hanya dengan menguasai satu jenis kredensial, sehingga risiko akses tidak sah akibat pencurian atau penyalahgunaan satu faktor dapat diminimalkan [4].

Salah satu metode yang umum digunakan sebagai faktor kedua dalam 2FA adalah *One-Time Password* (OTP), yaitu kode verifikasi yang bersifat sementara dan hanya berlaku untuk satu sesi atau periode waktu tertentu [10].

Karakteristik dinamis pada OTP membuatnya sulit untuk diprediksi atau digunakan ulang oleh pihak yang tidak berwenang, sehingga lapisan keamanan menjadi lebih kuat dibandingkan kata sandi statis [10].

OTP umumnya didistribusikan melalui kanal komunikasi terpisah seperti SMS, email, atau aplikasi pesan instan berbasis internet, untuk memastikan kode hanya dapat diakses oleh pengguna yang sah [11].

Dengan kombinasi RFID sebagai faktor kepemilikan dan OTP sebagai faktor verifikasi dinamis, sistem *smart door lock* yang dikembangkan dalam penelitian ini menerapkan konsep 2FA secara terintegrasi untuk meningkatkan keamanan akses pintu.

2.6. Penelitian Terdahulu

Beberapa penelitian terdahulu telah dikembangkan untuk meningkatkan keamanan akses pintu menggunakan teknologi RFID, OTP, maupun kombinasi keduanya. Penelitian Tamam dan Romadhoni [13] mengembangkan sistem pengaman pintu otomatis berbasis NodeMCU dengan E-KTP sebagai *tag* RFID dan notifikasi WhatsApp, namun masih menggunakan satu mikrokontroler untuk menangani seluruh proses sistem dan hanya mengandalkan satu faktor autentikasi.

Penelitian Wibawa et al. [17] memanfaatkan RFID MFRC522 sebagai sistem pemantauan akses ruangan dengan basis data, yang juga masih bergantung pada single factor authentication.

Pada aspek autentikasi dua faktor, penelitian Ilham et al. [9] mengimplementasikan kombinasi RFID dan OTP berbasis NodeMCU sebagai sistem keamanan pintu, di mana seluruh proses pembacaan sensor dan komunikasi jaringan ditangani oleh satu unit pengendali. Pendekatan ini berhasil meningkatkan keamanan, tetapi penggunaan satu mikrokontroler

untuk menangani seluruh fungsi berpotensi menambah beban pemrosesan terutama saat berlangsung komunikasi jaringan yang bersifat non-deterministik. Perbandingan beberapa penelitian terdahulu dengan penelitian ini disajikan pada Tabel 1.

Tabel 1. Perbandingan penelitian terdahulu dengan penelitian ini

Peneliti	Metode Autentikasi	Arsitektur Mikronkontroler	Media Notifikasi
Tamam & Romadhoni [13]	RFID E-KTP (single factor)	Single (NodeMCU)	WhatsApp
Wibawa et al. [17]	RFID E-KTP (single factor)	Single (NodeMCU)	Database
Ilham et al. [9]	RFID (single factor)	Single (NodeMCU)	-
Penelitian ini	RFID + OTP (two factor)	Dual (Arduino Mega 2560 + NodeMCU ESP8266)	Telegram

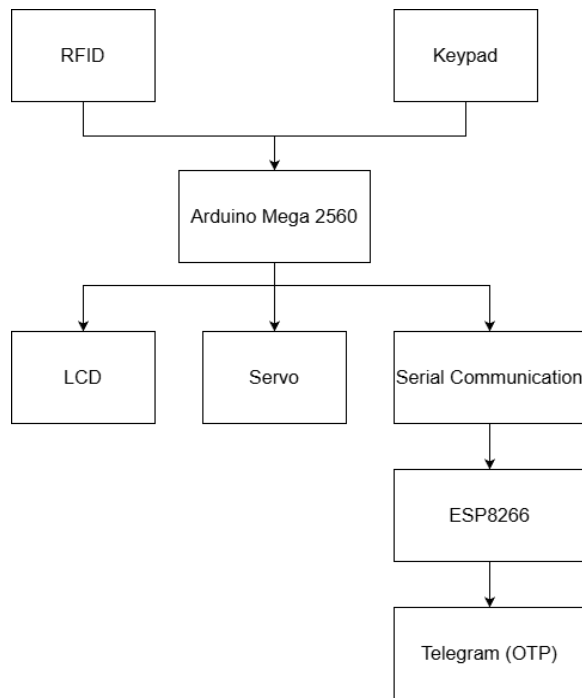
Berdasarkan perbandingan tersebut, terlihat bahwa kebaruan penelitian ini terletak pada penerapan arsitektur dual mikrokontroler yang memisahkan proses kontrol perangkat keras dan komunikasi jaringan, sehingga sistem tidak hanya menerapkan autentikasi dua faktor tetapi juga mendistribusikan beban kerja secara lebih efisien dibandingkan penelitian sebelumnya.

3. METODE PENELITIAN

Metode Penelitian ini menggunakan pendekatan rancang bangun (*research and development*) yang dilaksanakan secara sistematis melalui tiga tahapan utama, yaitu perancangan sistem, perancangan perangkat keras, dan perancangan perangkat lunak. Setiap tahapan saling berkaitan untuk memastikan integrasi antar komponen berjalan sesuai fungsi yang diharapkan, dengan tahap perancangan sistem menjadi landasan pengembangan keseluruhan perangkat.

3.1. Perancangan Sistem

Sistem *smart door lock* pada penelitian ini dirancang dengan arsitektur dual mikrokontroler yang menerapkan autentikasi dua faktor melalui RFID dan OTP. Komponen utama sistem terdiri atas modul RFID sebagai pembaca kartu, *keypad* sebagai media input OTP, Arduino Mega 2560 sebagai pengendali utama perangkat keras, NodeMCU ESP8266 sebagai modul komunikasi jaringan, LCD sebagai antarmuka informasi, dan motor servo sebagai aktuator kunci pintu. Hubungan antar komponen ditunjukkan pada Gambar 1.



Gambar 1. Diagram blok sistem smart door lock

Proses kerja sistem dimulai ketika pengguna menempelkan kartu RFID pada modul pembaca, sehingga UID kartu terbaca dan dikirim ke Arduino Mega 2560 untuk verifikasi awal. Apabila UID terdaftar, Arduino mengirimkan perintah ke NodeMCU ESP8266 melalui antarmuka serial untuk membangkitkan dan mengirimkan kode OTP kepada pengguna melalui layanan Telegram. Pengguna kemudian memasukkan kode OTP melalui *keypad* untuk diverifikasi oleh Arduino. Jika OTP sesuai, Arduino mengaktifkan motor servo untuk membuka kunci pintu, sedangkan jika verifikasi gagal, sistem menolak akses dan tetap berada pada kondisi terkunci. Status sistem dan instruksi pengguna ditampilkan secara *real-time* melalui LCD selama seluruh proses berlangsung.

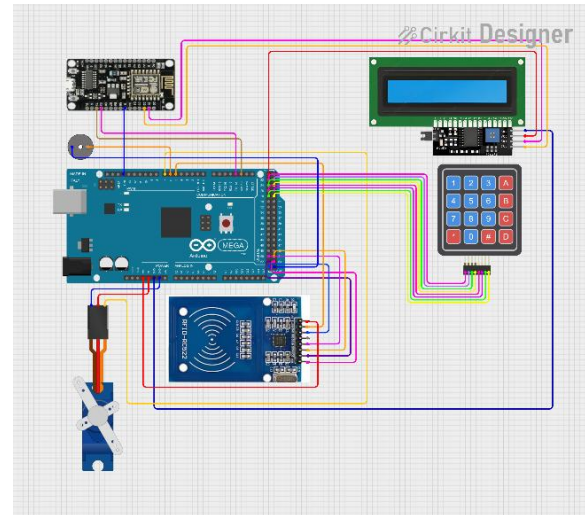
3.2. Perancangan Perangkat Keras

Tabel 2. Komponen perangkat keras

Komponen	Fungsi	Antarmuka
Arduino Mega 2560	Pengendali utama perangkat keras	-
NodeMCU ESP8266	Modul komunikasi jaringan (Telegram)	UART (serial)
RFID RC522	Pembaca UID kartu (faktor pertama)	SPI
Keypad 4×4	Input kode OTP (faktor kedua)	Digital I/O
LCD 16×2 (I2C)	Tampilan status & instruksi	I2C
Motor Servo SG90	Aktuator kunci pintu	PWM
Buzzer	Indikator audio	Digital I/O

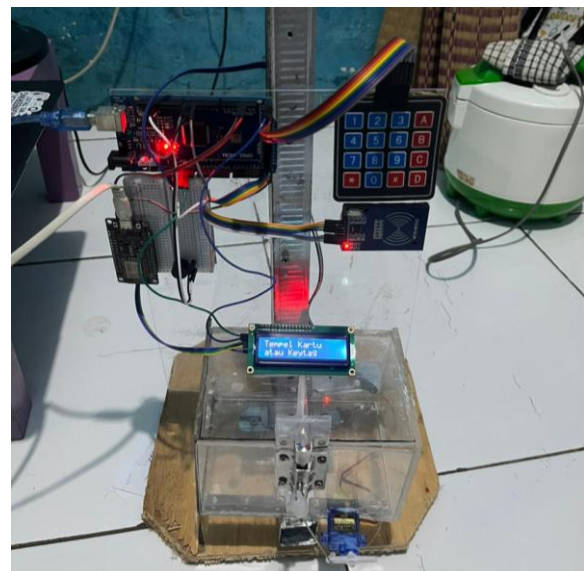
Perancangan perangkat keras dilakukan dengan mengintegrasikan modul-modul utama yang saling

terhubung melalui Arduino Mega 2560 sebagai pengendali pusat. Daftar komponen utama beserta fungsi dan antarmuka komunikasinya ditunjukkan pada Tabel 2, sedangkan skematik rangkaian, implementasi perangkat keras, dan desain mekanik sistem ditampilkan masing-masing pada Gambar 2, Gambar 3, dan Gambar 4.



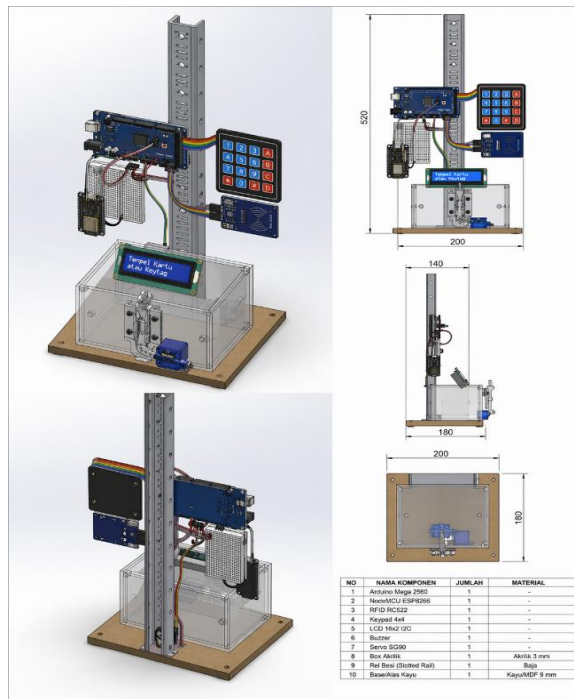
Gambar 2. Skematik rangkaian sistem

Gambar 2 menunjukkan skematik rangkaian sistem secara keseluruhan. Modul RFID RC522 dihubungkan ke Arduino Mega 2560 melalui antarmuka SPI menggunakan pin SS (pin 53), SCK, MOSI, dan MISO. Keypad 4×4 dihubungkan melalui delapan pin digital Arduino. LCD 16×2 terhubung melalui modul I2C pada pin SDA dan SCL. Motor servo SG90 mendapat sinyal PWM dari pin 9 Arduino, sedangkan buzzer terhubung ke pin digital sebagai indikator audio. NodeMCU ESP8266 terhubung ke Arduino melalui komunikasi serial (UART) pada pin TX/RX untuk pertukaran data OTP secara *real-time*.



Gambar 3. Implementasi perangkat keras

Gambar 3 menampilkan implementasi perangkat keras sistem yang telah dirakit. Seluruh komponen elektronik dipasang pada struktur rangka baja ringan dengan papan akrilik bening. Arduino Mega 2560 dan NodeMCU ESP8266 diposisikan di bagian atas rangka, sementara modul RFID RC522 dan keypad 4×4 ditempatkan pada sisi yang mudah dijangkau pengguna. LCD 16×2 dipasang di bagian tengah untuk memudahkan pembacaan status sistem, dan motor servo SG90 dipasang di bagian bawah sebagai aktuator yang menggerakkan mekanisme kunci pintu..



Gambar 4. Desain mekanik sistem

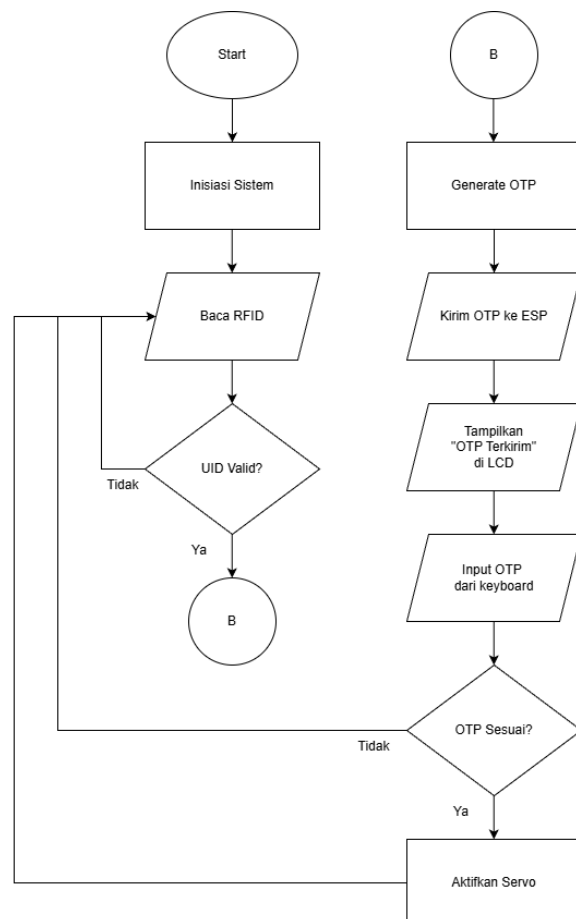
Gambar 4 menunjukkan desain mekanik sistem dengan dimensi keseluruhan 200 × 180 × 520 mm. Rangka utama menggunakan baja ringan berukuran 55 × 5 cm sebagai penopang, dengan alas berbahan kayu/MDF tebal 9 mm sebagai dudukan. Kotak komponen berbahan akrilik bening tebal 3 mm berukuran 200 × 180 mm digunakan sebagai wadah mekanisme pengunci. Desain ini memungkinkan komponen elektronik terlindungi sekaligus mekanisme kunci servo tetap terlihat untuk keperluan demonstrasi dan pengujian sistem.

Modul RFID RC522 dihubungkan ke Arduino melalui antarmuka SPI untuk pembacaan UID kartu, sedangkan keypad digunakan sebagai media input OTP melalui pin digital. LCD menampilkan informasi status sistem melalui antarmuka I2C, dan motor servo dikendalikan melalui sinyal PWM dari Arduino untuk pengaturan posisi sudut pengunci pintu. NodeMCU ESP8266 berfungsi sebagai media komunikasi yang terhubung dengan Arduino melalui antarmuka serial, sehingga pertukaran data OTP berlangsung secara *real-time* tanpa membebani proses utama mikrokontroler [16].

3.3. Perancangan Perangkat Lunak

Perangkat lunak sistem dirancang untuk mengatur alur kerja autentikasi dua faktor dengan pembagian peran antara dua mikrokontroler. Arduino Mega 2560 bertanggung jawab atas proses identifikasi RFID, penerimaan input OTP melalui keypad, serta pengendalian aktuator motor servo dan LCD, sedangkan NodeMCU ESP8266 menangani konektivitas jaringan dan pengiriman OTP melalui Telegram secara independen.

Alur kerja perangkat lunak pada Arduino Mega 2560 ditunjukkan pada Gambar 5. Proses dimulai dengan inisialisasi perangkat, dilanjutkan dengan pembacaan kartu RFID dan verifikasi UID. Apabila UID valid, Arduino membangkitkan kode OTP enam digit dan mengirimkannya ke NodeMCU melalui komunikasi serial. Selanjutnya, pengguna memasukkan kode OTP melalui keypad untuk diverifikasi. Jika OTP sesuai dan belum kedaluwarsa, Arduino mengaktifkan motor servo untuk membuka kunci pintu; jika tidak, sistem menolak akses dan kembali ke kondisi awal.

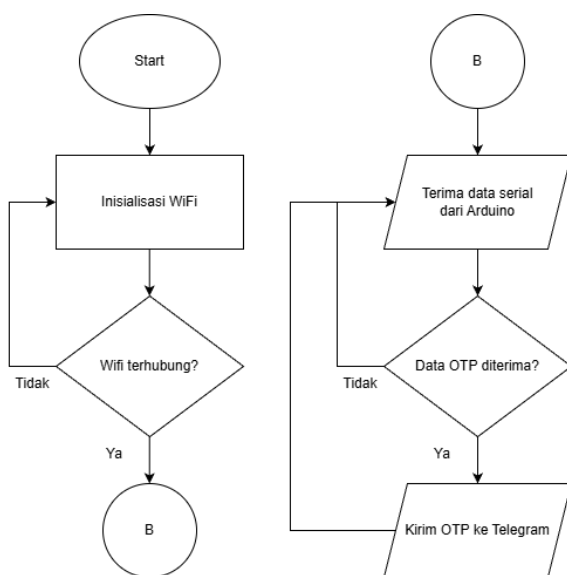


Gambar 5. Flowchart sistem pada Arduino Mega2560

Pada Gambar 5, terlihat bahwa sistem memiliki dua jalur keputusan utama: jalur penolakan akses (apabila UID tidak dikenali atau OTP tidak valid) dan jalur penerimaan akses (apabila kedua faktor terverifikasi). Terdapat pula mekanisme reset OTP

menggunakan tombol * pada keypad dan konfirmasi input OTP menggunakan tombol #, sehingga pengguna memiliki fleksibilitas dalam proses pemasukan kode sebelum diverifikasi oleh sistem.

Adapun alur kerja NodeMCU ESP8266 ditunjukkan pada Gambar 6, yang dimulai dengan inisialisasi koneksi WiFi dan komunikasi serial. NodeMCU secara kontinu memantau data masuk dari Arduino, dan ketika kode OTP diterima, NodeMCU langsung mengirimkannya ke pengguna melalui Telegram Bot API. Pemisahan tugas antar mikrokontroler memungkinkan proses kontrol perangkat keras yang bersifat deterministik berjalan tanpa terganggu oleh latensi komunikasi jaringan yang bersifat non-deterministik [15], sehingga sistem mampu beroperasi secara stabil dan responsif.



Gambar 6. Flowchart sistem pada NodeMCU ESP8266

Pada Gambar 6, terlihat bahwa NodeMCU beroperasi secara independen dari Arduino, ia hanya menunggu dan memproses data yang masuk melalui komunikasi serial. Apabila data yang diterima diawali dengan prefiks "OTP:", NodeMCU akan segera mengirimkan kode OTP tersebut ke pengguna melalui Telegram Bot API. Pemisahan proses komunikasi ini memastikan bahwa latensi jaringan internet tidak memengaruhi proses kontrol perangkat keras pada Arduino Mega 2560.

4. HASIL DAN PEMBAHASAN

Pengujian sistem *smart door lock* dilakukan untuk mengevaluasi kinerja sistem yang telah dirancang melalui empat parameter utama, yaitu akurasi pembacaan RFID, waktu respons sistem, waktu aktuasi servo, dan waktu komunikasi OTP. Setiap parameter diuji secara berulang dengan jumlah percobaan yang konsisten untuk memperoleh data yang representatif, kemudian dianalisis untuk menilai tingkat keandalan dan stabilitas sistem secara menyeluruh.

4.1. Hasil Pengujian Akurasi RFID

Pengujian akurasi pembacaan RFID dilakukan untuk mengetahui kemampuan sistem dalam mendeteksi kartu pada berbagai variasi jarak antara *tag* dan *reader*. Setiap variasi jarak diuji sebanyak 10 kali percobaan untuk memperoleh hasil yang konsisten. Hasil pengujian ditunjukkan pada Tabel 3.

Tabel 3. Hasil pengujian akurasi pembacaan RFID

Jarak (cm)	Jumlah Percobaan	Berhasil	Gagal	Persentase (%)
1 cm	10	10	0	100%
2 cm	10	10	0	100%
3 cm	10	10	0	100%
4 cm	10	10	0	100%
5 cm	10	10	0	100%
6 cm	10	10	0	100%
7 cm	10	7	3	70%
8 cm	10	0	10	0%

Berdasarkan Tabel 3, sistem menunjukkan tingkat keberhasilan pembacaan RFID sebesar 100% pada jarak 1–6 cm, yang menandakan bahwa modul RC522 bekerja optimal dengan stabilitas pembacaan tinggi pada rentang jarak dekat. Pada jarak 7 cm, tingkat keberhasilan menurun menjadi 70%, dan pada jarak 8 cm sistem tidak mampu membaca kartu sama sekali. Penurunan kinerja tersebut disebabkan oleh keterbatasan jangkauan efektif modul RC522 yang bekerja pada frekuensi 13,56 MHz, di mana kekuatan medan elektromagnetik melemah seiring bertambahnya jarak [17].

Dengan demikian, jarak optimal pengoperasian sistem berada pada rentang ≤ 6 cm, yang masih sesuai dengan kebutuhan sistem keamanan akses pintu karena meminimalkan risiko pembacaan tidak sah dari jarak jauh.

4.2. Hasil Pengujian Waktu Respons Sistem

Pengujian waktu respons sistem dilakukan untuk mengetahui kecepatan sistem dalam memproses data sejak kartu RFID terdeteksi hingga sistem meminta input OTP. Hasil pengujian dari 10 kali percobaan ditunjukkan pada Tabel 4.

Tabel 4. Hasil pengukuran waktu respons sistem

Percobaan ke-	Waktu Respons (detik)
1	9,45
2	9,47
3	9,40
4	9,50
5	9,47
6	9,58
7	9,46
8	9,31
9	9,31
10	9,50
Rata-rata	9,44

Berdasarkan Tabel 4, waktu respons sistem berada pada rentang 9,31–9,58 detik dengan nilai rata-rata 9,44 detik. Variasi waktu yang relatif kecil menunjukkan bahwa sistem bekerja secara deterministik dan konsisten dalam memproses data dari pembacaan RFID hingga permintaan input OTP. Nilai waktu respons yang relatif tinggi tersebut tidak hanya dipengaruhi oleh proses pembangkitan dan pengiriman OTP melalui komunikasi serial antara Arduino Mega 2560 dan NodeMCU ESP8266, tetapi juga oleh alur pemrosesan tampilan LCD yang berjalan secara berurutan dari instruksi "*Tempelkan Kartu*", "*OTP Terkirim*", hingga "*Masukkan OTP*". Akumulasi proses tersebut menyebabkan terjadinya jeda waktu yang signifikan, meskipun kestabilannya tetap terjaga sehingga masih dapat diterima dalam konteks aplikasi *smart door lock*.

4.3. Hasil Pengujian Waktu Aktuasi Servo

Pengujian waktu aktuasi servo dilakukan untuk mengetahui kecepatan respons aktuator dalam membuka kunci pintu setelah proses autentikasi dinyatakan berhasil. Hasil pengujian dari 10 kali percobaan ditampilkan pada Tabel 5.

Tabel 5. Hasil pengujian waktu aktuasi servo

Percobaan ke-	Waktu Aktuasi Servo (detik)
1	0,82
2	0,81
3	0,73
4	0,82
5	0,84
6	0,79
7	0,97
8	0,82
9	0,76
10	0,69
Rata-rata	0,81

Berdasarkan Tabel 5, waktu aktuasi servo berada pada rentang 0,69–0,97 detik dengan nilai rata-rata 0,81 detik. Variasi waktu yang relatif kecil menunjukkan bahwa aktuator memiliki kestabilan yang baik dalam pengendalian. Perbedaan waktu yang muncul kemungkinan dipengaruhi oleh karakteristik mekanis servo SG90 serta variasi tegangan suplai saat aktuasi berlangsung. Secara keseluruhan, waktu aktuasi yang berada di bawah 1 detik membuktikan bahwa sistem telah memenuhi kebutuhan respons *real-time* dalam proses pembukaan kunci pintu.

4.4. Hasil Pengujian Waktu Komunikasi OTP

Pengujian waktu komunikasi OTP dilakukan untuk mengukur durasi pengiriman kode OTP dari sistem hingga diterima pengguna melalui platform Telegram. Pengukuran dihitung dari saat sistem menampilkan notifikasi "*OTP Terkirim*" pada LCD hingga kode diterima oleh pengguna. Hasil pengujian dari 10 kali percobaan ditunjukkan pada Tabel 6.

Tabel 6. Hasil pengujian waktu pengiriman OTP

Percobaan ke-	Delay OTP (detik)
1	03,38
2	03,93
3	03,81
4	04,03
5	03,74
6	03,94
7	03,83
8	03,81
9	03,81
10	03,84

Berdasarkan Tabel 6, waktu komunikasi OTP berada pada rentang 3,38–4,03 detik dengan nilai rata-rata 3,81 detik. Variasi tersebut dipengaruhi oleh kondisi jaringan internet yang digunakan oleh NodeMCU ESP8266 serta waktu respons server Telegram dalam memproses dan mengirimkan pesan. Berbeda dengan proses pada Arduino Mega 2560 yang bersifat deterministik, komunikasi jaringan memiliki sifat non-deterministik sehingga waktu yang dibutuhkan dapat berfluktuasi [6]. Meskipun demikian, waktu pengiriman 3–4 detik masih tergolong cepat dan berada dalam batas wajar untuk sistem berbasis komunikasi jaringan, sehingga tidak mengganggu pengalaman pengguna dalam proses autentikasi.

4.5. Hasil Pengujian Keberhasilan Sistem

Pengujian keberhasilan sistem dilakukan secara *end-to-end* untuk memvalidasi bahwa seluruh tahapan autentikasi dua faktor dapat berjalan secara terintegrasi. Pengujian mencakup empat tahapan utama, yaitu pembacaan kartu RFID, pengiriman OTP melalui Telegram, verifikasi OTP melalui *keypad*, dan aktuasi motor servo untuk membuka kunci pintu. Sebanyak 10 kali percobaan dilakukan menggunakan kartu RFID terdaftar dan kode OTP yang valid. Hasil pengujian ditampilkan pada Tabel 7.

Tabel 7. Hasil pengujian keberhasilan sistem

Percobaan ke-	Tahapan Berhasil	Total Tahapan	Status
1	4	4	Berhasil
2	4	4	Berhasil
3	4	4	Berhasil
4	4	4	Berhasil
5	4	4	Berhasil
6	4	4	Berhasil
7	4	4	Berhasil
8	4	4	Berhasil
9	4	4	Berhasil
10	4	4	Berhasil
Tingkat Keberhasilan		100%	

Berdasarkan Tabel 7, sistem menunjukkan tingkat keberhasilan 100% pada seluruh tahapan pengujian *end-to-end*. Hasil ini membuktikan bahwa keempat proses utama sistem berjalan secara terintegrasi tanpa mengalami kegagalan pada satu pun percobaan. Konsistensi keberhasilan tersebut juga

mengindikasikan bahwa pembagian beban kerja antara Arduino Mega 2560 dan NodeMCU ESP8266 berjalan secara stabil, sehingga proses kontrol perangkat keras dan komunikasi jaringan tidak saling mengganggu satu sama lain. Dengan demikian, sistem *smart door lock* yang dirancang telah memenuhi fungsi utama autentikasi dua faktor secara menyeluruh dan dapat diandalkan untuk diterapkan pada lingkungan keamanan akses pintu.

5. KESIMPULAN DAN SARAN

5.1. Kesimpulan

Berdasarkan hasil perancangan, implementasi, dan pengujian sistem *smart door lock* berbasis autentikasi dua faktor RFID dan OTP dengan arsitektur dual mikrokontroler, dapat ditarik beberapa kesimpulan sebagai berikut:

Pertama, sistem berhasil menerapkan autentikasi dua faktor secara terintegrasi dengan tingkat keberhasilan *end-to-end* sebesar 100% pada seluruh tahapan pengujian, mulai dari pembacaan RFID, pengiriman OTP, verifikasi OTP, hingga aktuasi servo. Modul RFID menunjukkan tingkat akurasi pembacaan 100% pada jarak 1–6 cm, dengan penurunan kinerja pada jarak di atasnya akibat keterbatasan jangkauan medan elektromagnetik modul RC522. Kedua, arsitektur dual mikrokontroler terbukti mampu memisahkan proses kontrol perangkat keras dan komunikasi jaringan secara efektif, ditunjukkan oleh waktu aktuasi servo yang konsisten di bawah 1 detik (rata-rata 0,81 detik) dan waktu komunikasi OTP rata-rata 3,81 detik yang masih berada dalam batas wajar untuk sistem berbasis jaringan. Ketiga, waktu respons sistem secara keseluruhan tercatat rata-rata 9,44 detik, yang dipengaruhi oleh proses pembangkitan OTP, komunikasi serial antar mikrokontroler, dan alur sequential pada tampilan LCD. Meskipun nilai tersebut relatif tinggi, kestabilan waktu respons menunjukkan bahwa sistem bekerja secara deterministik tanpa fluktuasi yang signifikan.

5.2. Saran

Berdasarkan hasil yang diperoleh, terdapat beberapa saran untuk pengembangan penelitian selanjutnya. Pertama, optimasi alur pemrosesan tampilan LCD dapat dilakukan dengan menggantikan delay sequential menjadi pendekatan non-blocking agar waktu respons sistem dapat diperpendek. Kedua, fitur keamanan dapat diperkuat dengan menambahkan enkripsi data pada proses pengiriman OTP untuk mencegah potensi penyadapan komunikasi jaringan. Ketiga, sistem dapat dilengkapi dengan fitur pencatatan riwayat akses (*log activity*) dan integrasi dengan aplikasi mobile atau platform IoT lainnya untuk meningkatkan kemudahan kontrol dan monitoring secara *real-time*. Pengembangan lebih lanjut juga dapat diarahkan pada efisiensi konsumsi daya dan desain perangkat yang lebih ringkas agar siap diterapkan secara luas pada lingkungan rumah pintar (*smart home*).

DAFTAR PUSTAKA

- [1] Z. Zulkarnaen and A. K. Al Koriah, "RANCANG BANGUN SISTEM KEAMANAN PINTU RUMAH DENGAN VOICE RECOGNITION DAN RFID GELANG BERBASIS IOT," *TEKNIMEDIA: Teknologi Informasi dan Multimedia*, vol. 5, no. 2, pp. 249–254, Dec. 2024, doi: 10.46764/teknimedia.v5i2.241.
- [2] N. Amalia and Muhammad, "Rancang Bangun Sistem Keamanan Pintu Menggunakan Modul RFID Berbasis IoT," *Jurnal Sains dan Teknologi* 4.0, vol. 1, no. 2, pp. 1–7, 2024, [Online]. Available: <https://jurnal.komputasi.org/index.php/jst/article/view/20/>
- [3] E. Alfonsius, A. S. Ruitan, and D. Liuw, "Pengembangan Sistem Keamanan Pintu Menggunakan Metode Prototype Berbasis RFID dan Keypad 4x4 dengan Arduino Nano," *Jurnal Ilmiah Informatika dan Ilmu Komputer (JIMA-ILKOM)*, vol. 3, no. 2, pp. 110–123, Sep. 2024, doi: 10.58602/jima-ilkom.v3i2.33.
- [4] C. L. Aldea and R. Bocu, "Authentication Challenges and Solutions in Microservice Architectures," *Applied Sciences (Switzerland)*, vol. 15, no. 22, Nov. 2025, doi: 10.3390/app152212088.
- [5] W. G. R. Putri and I. G. N. W. P. Agung, "IOT SMART DOOR LOCK SYSTEM MENGGUNAKAN DOUBLE SENSOR BERBASIS MIKROKONTROLER ESP32," *Jurnal MNEMONIC*, vol. 8, no. 1, pp. 74–82, Feb. 2025.
- [6] J. S. Sonamoni *et al.*, "IoT-Based Smart Remote Door Lock and Monitoring System Using an Android Application †," *Engineering Proceedings*, vol. 76, no. 1, 2024, doi: 10.3390/engproc2024076085.
- [7] M. Faturrachman and I. Yustiana, "Sistem Keamanan Pintu Rumah dengan Sidik Jari Berbasis Internet of Things (IoT)," *Jurnal Teknik Informatika UNIKA Santo Thomas (JTIUST)*, vol. 6, no. 2, pp. 379–385, Dec. 2021, doi: 10.54367/jtiust.v6i2.1517.
- [8] A. Syahri and Mhd. Basri, "Perancangan Sistem Keamanan untuk Deteksi Pencurian Menggunakan Sensor Magnetic dan RFID Berbasis Internet of Things," *Hello World Jurnal Ilmu Komputer*, vol. 4, no. 3, pp. 163–170, Oct. 2025, doi: 10.56211/helloworld.v4i3.1166.
- [9] A. Ilham, A. Mashudi, and A. Prihanto, "Rancang Bangun Sistem Keamanan Pintu Menggunakan Metode Two-Factor Authentication," *Journal of Informatics and Computer Science (JINACS)*, vol. 6, no. 3, 2024, doi: 10.26740/jinacs.v6n3.
- [10] S. Wibawa and R. Ningsih, "Perlindungan Data Digital Dengan Time-Based One-Time Password (TOTP)," *INSANtek: Jurnal Inovasi dan Sains Teknik Elektro*, vol. 5, no. 1, 2024, [Online].

Available:

<http://jurnal.bsi.ac.id/index.php/insantek>

- [11] H. Wiranto and A. Mufti Salis, "Pengalaman pengguna dan kepercayaan terhadap keamanan OTP dalam sistem autentikasi dompet digital," *Jurnal Pendidikan Informatika dan Sains*, vol. 14, no. 1, pp. 75–83, Jun. 2025, doi: 10.31571/saintek.v14i1.8897.
- [12] W. R. Gusti, M. Zakarijah, and U. Rochayati, "Perancangan Embedded System untuk Kendali Rumah Burung Walet Berbasis ATmega8," *JEPIN (Jurnal Edukasi dan Penelitian Informatika)*, vol. 8, no. 3, pp. 500–507, Dec. 2022, doi: 10.26418/jp.v8i3.57354.
- [13] M. T. Tamam and R. Romadhoni, "Pengaman Pintu Gedung Otomatis Menggunakan E-KTP Berbasis NodeMCU dan RFID-RC522 dengan Notifikasi Whatsapp Application," *Journal of Telecommunication, Electronics, and Control Engineering (JTECE)*, vol. 5, no. 1, pp. 22–30, Jan. 2023, doi: 10.20895/jtece.v5i1.910.
- [14] O. A. Putra and R. Handika, "Rancang Bangun Sistem Keamanan Lalu Lintas Menggunakan Smartphone Dan Esp32Cam Berbasis Arduino Mega 2560," *Jurnal Sains Dan Teknologi (JSIT)*, vol. 2, no. 1, pp. 72–82, 2022, doi: 10.47233/jsit.v2i1.
- [15] L. K. Sari, O. Candra, H. Effendi, and F. Eliza, "Perancang Sistem Otomasi Pada Aquascape Berbasis Internet of Things (IoT)," *JTEIN: Jurnal Teknik Elektro Indonesia*, vol. 4, no. 1, pp. 160–168, May 2023, doi: 10.24036/jtein.v4i1.363.
- [16] N. Septianti and R. Rahmadewi, "Sistem Komunikasi Antar Arduino Menggunakan Protokol RS485," *Journal of Electrical Engineering and Computer (JEECOM)*, vol. 4, no. 2, 2024, doi: 10.33650/jeeecom.v4i2.
- [17] K. Wirawibawa, R. Susana, and F. Hadiatna, "Pemanfaatan RFID MFRC522 dan Sistem Database untuk Pemantauan Akses Ruangan dengan Identifikasi In dan Out," *Power Elektronik: Jurnal Orang Elektro*, vol. 11, no. 1, pp. 36–44, 2022, doi: 10.30591/polektro.v11i1.2889