

Prototype Sistem Smart Door Lock untuk Keamanan Ruang Laboratorium dengan Alarm Buzzer dan Audit Logging

Fajar Septian^{1*}, Dwi Ermawati², Andika Riyadi Jasril³, Chairul Fikri⁴, Asep Taufik Muharram⁵

^{1,4,5}Teknik Informatika, Politeknik Negeri Jakarta, Jl. Prof. DR. G.A. Siwabessy Kampus Universitas Indonesia Depok, Indonesia, 16425

e-mail: ¹fajar.septian@lecturer.pnj.ac.id, ⁴chairul.fikri@lecturer.pnj.ac.id,

⁵asep.muhammad@tik.pnj.ac.id,

^{2,3}Teknik Multimedia Jaringan, Politeknik Negeri Jakarta, Jl. Prof. DR. G.A. Siwabessy Kampus Universitas Indonesia Depok, Indonesia, 16425

e-mail: ²dwi.ermawati@lecturer.pnj.ac.id, ³andika.riyadijasril@lecturer.pnj.ac.id

*Corresponding author

Submitted Date: January 20th, 2026

Revised Date: March 10th, 2026

Reviewed Date: February 2nd, 2026

Accepted Date: April 25th, 2026

Abstract

This study addresses the security vulnerabilities of university laboratory rooms due to conventional mechanical keys. The purpose of this research is to design and implement a cost-effective, microcontroller-based smart door lock system integrated with real-time audit logging and an alarm mechanism. The system was developed using the prototyping method, encompassing requirements analysis, electronic circuit design, hardware assembly, software development via Arduino IDE, and quantitative performance evaluation. The prototype integrates an Arduino Uno, a 3x4 keypad, an SG90 servo motor, a DS1307 Real-Time Clock (RTC), a buzzer, and an LCD. Performance tests demonstrate high reliability with a 0.00 system error rate. The system achieves a fast total response time ranging from 191 ms to 212 ms for user validation and physical access execution. Power consumption analysis shows the prototype operates efficiently, requiring 0.65 Watts during idle states and peaking at 0.80 Watts when active. Every access attempt is systematically recorded into the local EEPROM with an average write speed of 44 μ s. The primary contribution of this research is the successful integration of localized, real-time audit logging, multi-stage password validation, and automated lockout alarms into a single, low-cost microcontroller architecture without internet dependency. This provides a highly functional, secure, and easily adoptable reference for institutional laboratory access control.

Keywords: Smart Door Lock; Arduino; Alarm Buzzer; Audit Logging; Laboratory Security

Abstrak

Penelitian ini dilatarbelakangi oleh kerentanan keamanan pada ruang laboratorium universitas akibat penggunaan kunci mekanik konvensional. Tujuan dari penelitian ini adalah merancang dan mengimplementasikan sistem *smart door lock* berbasis mikrokontroler berbiaya rendah yang terintegrasi dengan audit *logging real-time* dan mekanisme alarm. Metode pengembangan yang digunakan adalah metode *prototyping*, yang meliputi analisis kebutuhan, perancangan rangkaian, perakitan perangkat keras, pengkodean sistem melalui Arduino IDE, serta evaluasi performa kuantitatif. Purwarupa yang dibangun mengintegrasikan Arduino Uno, keypad 3x4, motor servo SG90, Real-Time Clock (RTC) DS1307, buzzer, dan LCD. Hasil pengujian performa menunjukkan keandalan tinggi dengan tingkat *error* sistem sebesar 0,00. Sistem menghasilkan waktu respons total yang cepat berkisar antara 191 ms hingga 212 ms untuk proses validasi pengguna hingga eksekusi pembukaan pintu. Analisis konsumsi daya menunjukkan efisiensi operasional sebesar 0,65 Watt pada kondisi idle dan meningkat menjadi 0,80 Watt saat



komponen aktif bekerja. Setiap upaya akses tercatat secara sistematis pada EEPROM lokal dengan kecepatan penulisan rata-rata 44 μ s. Kontribusi utama dari penelitian ini adalah keberhasilan integrasi fitur audit *logging* lokal *real-time*, validasi kata sandi bertingkat, dan alarm penguncian otomatis (*lockout*) ke dalam satu arsitektur mikrokontroler sederhana tanpa ketergantungan internet. Sistem ini menyediakan referensi *access control* yang fungsional, aman, dan mudah diimplementasikan untuk kebutuhan laboratorium institusi.

Kata kunci: *Smart Door Lock*; Arduino; Alarm Buzzer; Audit *Logging*; Keamanan Laboratorium

1. Pendahuluan

Keamanan rumah dan bangunan menjadi salah satu aspek penting dalam kehidupan modern (Dewi & Fikri, 2023). Seiring berkembangnya teknologi, sistem pengamanan ruangan menggunakan kunci mekanik dianggap kurang memadai karena mudah diduplikasi, hilang, atau rusak (Juliansyah et al., 2025). Hal ini mendorong inovasi sistem penguncian pintu yang lebih cerdas, praktis, dan aman berupa sistem *smart door lock*. Penggunaan *smart door lock* dapat mengurangi risiko kejahatan terhadap akses rumah atau bangunan yang ditinggal pemiliknya (Rizky et al., 2023). Perkembangan penelitian *smart door lock* saat ini tidak hanya berfokus pada autentikasi akses, tetapi juga integrasi sistem monitoring dan *access control* berbasis mikrokontroler maupun *Internet of Things* (IoT). Penelitian internasional menunjukkan bahwa sistem *smart lock* berbasis Arduino dan RFID mampu meningkatkan keamanan akses ruangan melalui autentikasi digital yang lebih fleksibel dibandingkan kunci mekanik konvensional (Kanagamalliga et al., 2026). Selain itu, implementasi *audit logging* dan monitoring aktivitas pengguna juga menjadi bagian penting dalam sistem keamanan *modern* untuk mendukung pelacakan aktivitas akses serta evaluasi keamanan sistem *access control* secara *real-time*. Penelitian lain juga menekankan bahwa aspek keamanan dan privasi menjadi tantangan utama dalam implementasi *smart lock* berbasis IoT, sehingga sistem *access control modern* perlu memiliki mekanisme autentikasi dan monitoring aktivitas pengguna yang andal untuk mencegah akses tidak sah (Sonamoni et al., 2024).

Ruang laboratorium memiliki tingkat kebutuhan keamanan yang lebih tinggi dibandingkan ruangan biasa karena di dalamnya terdapat berbagai aset penting seperti perangkat komputer, alat praktikum, dokumen penelitian, serta data akademik yang bersifat penting dan terbatas. Akses yang tidak terkontrol terhadap ruang laboratorium dapat menimbulkan risiko kerusakan perangkat, kehilangan data, maupun penyalahgunaan fasilitas laboratorium. Selain itu, penggunaan kunci mekanik konvensional masih memiliki kelemahan karena mudah dipinjamkan, diduplikasi, atau hilang sehingga pengawasan terhadap aktivitas keluar masuk ruangan menjadi sulit dilakukan. Oleh karena itu, diperlukan sistem keamanan pintu yang mampu melakukan autentikasi akses sekaligus mencatat aktivitas pengguna secara otomatis untuk meningkatkan keamanan dan monitoring ruang laboratorium.

Smart door lock berbasis *keypad* menawarkan solusi dengan akses menggunakan PIN tanpa kunci fisik (Putri & Agung, 2025). Kode PIN dapat diganti kapan saja dan hanya diketahui oleh pengguna tertentu (Romadon et al., 2022). *Buzzer* digunakan untuk memberikan *alarm* peringatan keamanan jika terjadi percobaan akses mencurigakan atau entri PIN yang tidak cocok dengan yang terdaftar pada sistem (Wakhid et al., 2026). Setiap data percobaan akses ke sistem dicatat ke dalam *audit logging* sebagai bukti jika terdapat anomali atau kemungkinan penyalahgunaan akses mencurigakan (Pratama et al., 2026). Kombinasi *keypad* sebagai autentikasi, *buzzer* sebagai sistem peringatan, dan *audit logging* sebagai sistem pencatat aktivitas, sistem *smart door lock* ini diharapkan mampu menjadi solusi keamanan ruang laboratorium yang efektif, mudah digunakan, dan dapat diterapkan pada ruangan terbatas lainnya.

Beberapa penelitian sebelumnya telah mengembangkan sistem *smart door lock* dengan pendekatan yang berbeda. Penelitian berbasis *keypad* dan PIN umumnya hanya berfokus pada autentikasi akses tanpa menyediakan fitur *audit logging* sehingga aktivitas pengguna tidak dapat dipantau secara historis. Penelitian lain telah menerapkan *audit logging*, namun belum dilengkapi dengan alarm keamanan sebagai peringatan terhadap percobaan akses tidak sah. Selain itu, beberapa sistem *smart door lock* berbasis IoT menggunakan mikrokontroler seperti ESP32 dengan konektivitas internet yang menawarkan pemantauan jarak jauh, tetapi memerlukan konfigurasi jaringan yang lebih kompleks serta biaya implementasi yang lebih tinggi. Penelitian pada sistem keamanan *smart home* juga menunjukkan bahwa mekanisme *authorization* dan monitoring aktivitas pengguna menjadi bagian penting dalam pengembangan *access*



control modern, namun sebagian besar implementasi masih memerlukan arsitektur jaringan dan konfigurasi perangkat yang relatif kompleks (Mubarakali et al., 2026). Dibandingkan dengan penelitian tersebut, penelitian ini mengembangkan sistem *smart door lock* berbasis Arduino Uno yang lebih sederhana, terjangkau, dan mampu mengintegrasikan autentikasi PIN, alarm *buzzer*, serta *audit logging* dalam satu sistem keamanan untuk kebutuhan ruang laboratorium.

Berdasarkan penelitian terdahulu, masih terdapat *research gap* berupa belum tersedianya sistem *smart door lock* berbasis mikrokontroler yang mampu mengintegrasikan autentikasi *keypad*, alarm keamanan, dan *audit logging* dalam satu sistem sederhana yang mudah diterapkan pada lingkungan laboratorium. Selain itu, beberapa penelitian menggunakan perangkat dengan spesifikasi tinggi yang meningkatkan kompleksitas implementasi dan biaya pengembangan. Oleh karena itu, penelitian ini dikembangkan untuk menyediakan prototipe *smart door lock* yang lebih terjangkau, mudah diterapkan, serta mampu menyediakan fitur pencatatan aktivitas akses (*audit logging*) sebagai bentuk *monitoring* keamanan pada ruang laboratorium atau ruangan terbatas lainnya. Kontribusi utama penelitian ini adalah pengembangan sistem keamanan pintu berbasis Arduino Uno yang mengintegrasikan autentikasi PIN, alarm *buzzer*, serta *audit logging* secara *real-time* dalam satu prototipe sederhana dan berbiaya rendah sebagai solusi keamanan ruang laboratorium berbasis mikrokontroler. Penelitian ini bertujuan untuk merancang dan mengimplementasikan prototipe *smart door lock* berbasis Arduino Uno yang mampu meningkatkan keamanan akses ruang laboratorium melalui autentikasi PIN, alarm *buzzer*, dan *audit logging* secara *real-time*.

Berdasarkan kajian penelitian terdahulu, masih terdapat celah penelitian berupa belum adanya implementasi *smart door lock* sederhana berbasis mikrokontroler yang secara terintegrasi menggabungkan autentikasi *keypad*, alarm keamanan, dan *audit logging* untuk kebutuhan keamanan ruang laboratorium. Oleh karena itu, penelitian ini berkontribusi dalam pengembangan sistem keamanan berbasis mikrokontroler dengan menghadirkan prototipe *smart door lock* yang memiliki biaya implementasi rendah, mudah diterapkan, serta mampu mendukung monitoring aktivitas akses secara *real-time* melalui fitur *audit logging*.

2. Metodologi Penelitian

Metode *prototyping* digunakan dalam pengembangan sistem pada penelitian ini, metode *prototyping* adalah teknik pengembangan sistem purwarupa sebagai gambaran umum tentang sistem yang akan diimplementasikan kepada pengguna (Wulandari et al., 2021). Metode ini meliputi tahapan analisa kebutuhan sistem, desain purwarupa, evaluasi purwarupa, analisis dan perbaikan, iterasi, pengkodean sistem, dan implementasi sistem (Kustanto et al., 2024). Pada tahap evaluasi purwarupa, dilakukan pengujian bertahap terhadap setiap komponen sistem seperti *keypad*, servo motor, RTC, LCD, dan *buzzer* untuk memastikan seluruh fungsi berjalan sesuai rancangan. Hasil evaluasi digunakan sebagai dasar perbaikan terhadap logika program, pengaturan *delay* servo, sensitivitas pembacaan input *keypad*, serta sinkronisasi pencatatan waktu pada RTC. Proses evaluasi dan perbaikan dilakukan secara iteratif hingga sistem mampu memberikan respon yang stabil dan konsisten pada setiap skenario pengujian.

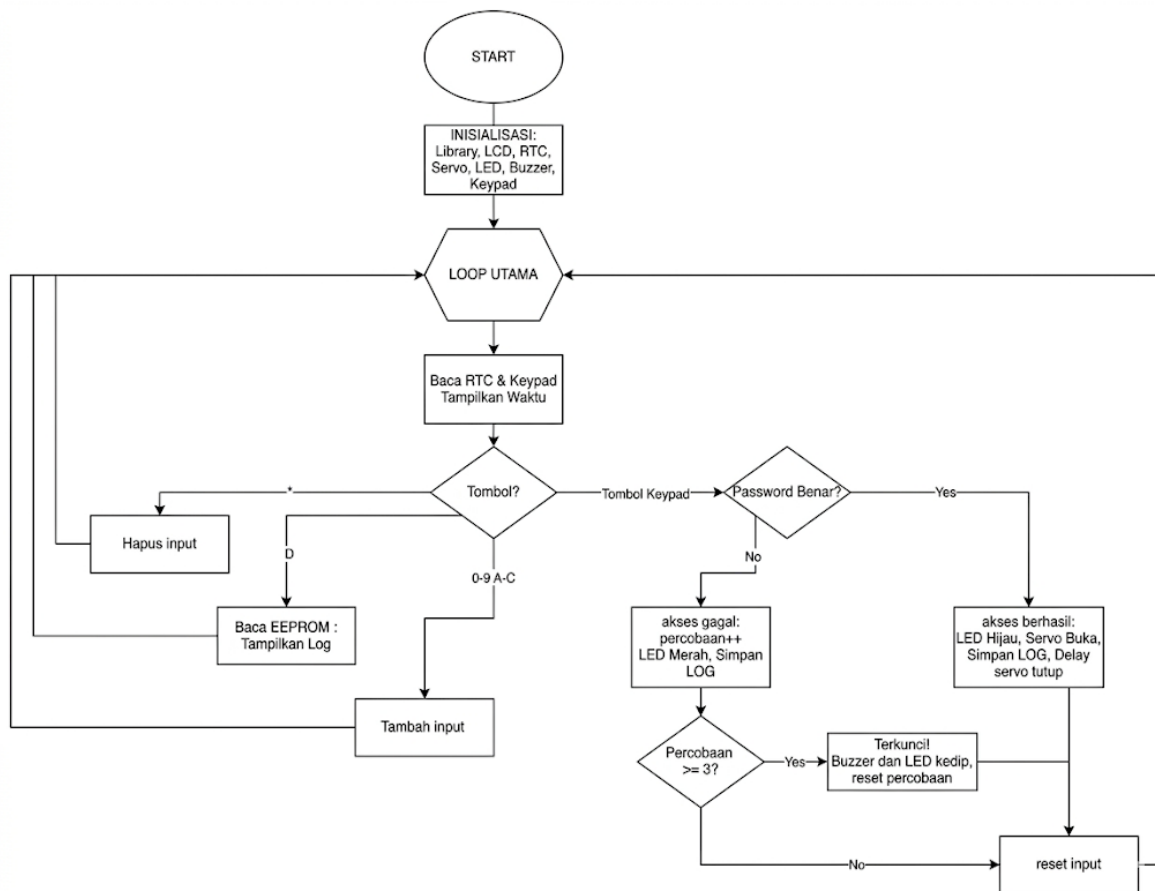
Proses pengembangan dimulai dengan analisis kebutuhan, meliputi identifikasi *hardware* (perangkat keras) dan *software* (perangkat lunak) yang diperlukan serta perancangan fungsi utama sistem. Selanjutnya dilakukan desain *prototype*, yang mencakup desain *flowchart* sistem, desain rangkaian elektronik, serta struktur program pada Arduino. Arduino merupakan *mini circuit board* dengan teknik komputasi fisik yang memiliki mikrokontroler Atmel dan diprogram menggunakan bahasa pemrograman C. Jenis arduino yang digunakan adalah Arduino Uno Atmega328P, *Integrated Circuit* yang memiliki 14 *input/output* digital (6 *output* untuk PWM), *resonator* kristal keramik 16 Mhz, 6 analog *input*, soket adaptor, pin header ICSP, koneksi USB, dan tombol *reset* (Sifaunajah et al., 2023). Tahap berikutnya adalah implementasi, yaitu perakitan komponen seperti *keypad*, *solenoid door lock*, *buzzer*, LED, dan modul penyimpanan *log*, kemudian diikuti dengan penulisan kode program untuk mengatur interaksi antar komponen tersebut.

Arduino Uno dipilih dalam penelitian ini karena memiliki kemudahan implementasi, biaya yang relatif rendah, serta kompatibilitas yang baik dengan berbagai modul perangkat keras seperti *keypad*, RTC, LCD, *buzzer*, dan servo motor. Selain itu, penggunaan Arduino Uno dinilai cukup memadai untuk

kebutuhan sistem yang masih bersifat lokal tanpa konektivitas internet. Dibandingkan mikrokontroler lain seperti ESP32 yang telah mendukung Wi-Fi, Arduino Uno lebih sederhana dalam proses konfigurasi sehingga sesuai untuk pengembangan prototipe awal dan kebutuhan pembelajaran di lingkungan laboratorium.

2.1 Desain Flowchart Sistem

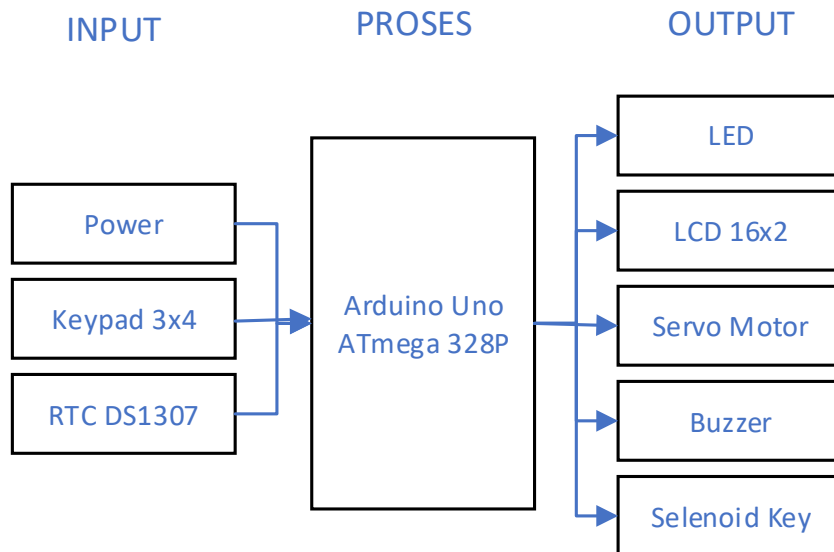
Alur proses sistem digambarkan dalam bentuk diagram *flowchart* untuk menunjukkan tahapan inisialisasi, pembacaan sensor, pengambilan keputusan, serta keluaran sistem secara sistematis (Listyoningrum et al., 2023). Berikut ditampilkan *flowchart* yang merepresentasikan keseluruhan rangkaian dan logika kerja sistem.



Gambar 1. Flowchart sistem

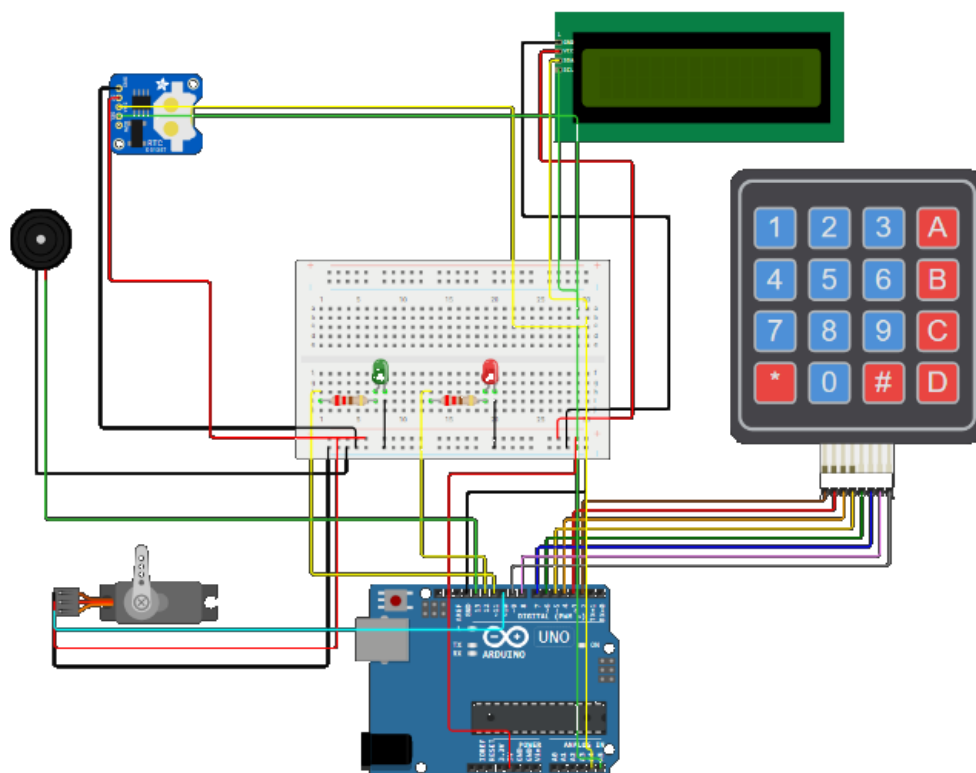
2.2 Desain Rangkaian Elektronik

Desain rangkaian elektronik menggambarkan hubungan antar komponen elektronik yang digunakan untuk prototipe perangkat (KH & Pernando, 2022). Komponen yang digunakan di antaranya adalah Arduino Uno ATmega328P, Keypad 3x4, Liquid Crystal Display 16x2, RTC DS1307 (Real-Time Clock), Servo Motor SG90, Alarm Buzzer, LED, Breadboard dan Kabel Jumper. Desain ini dirancang untuk memastikan seluruh komponen terintegrasi dengan benar serta meminimalkan potensi kesalahan saat perakitan prototipe. Blok diagram sebagai gambaran dari komponen yang akan digunakan pada sistem *smart door lock* dengan *personal identification number* dari keypad (Romadon et al., 2022).



Gambar 2. Diagram blok sistem

Berikut adalah gambar desain rangkaian elektronik untuk sistem *smart door lock*.



Gambar 3. Desain rangkaian elektronik

Tabel 1. Sambungan Pin

Komponen	Pin Komponen	Pin Arduino
LCD 16x2	VCC	5V
	GND	GND
	SDA	A4
	SCL	A5
Keypad 3x4	R1	D2
	R2	D3
	R3	D4
	R4	D5
	C1	D6
	C2	D7
	C3	D8
	C4	D9
Servo Motor	VCC (+5)	5V
	GND	GND
	Signal	D10
LED Merah	Anoda (+)	D11
	Katoda (-)	GND Arduino
LED Hijau	Anoda (+)	D12
	Katoda (-)	GND Arduino
Buzzer	Anoda (+)	D13
	Katoda (-)	GND
RTC DS1307	VCC	5V
	GND	GND
	SDA	A4
	SCL	A5

2.3 Perancangan Perangkat Keras

Komponen elektronik dirakit sesuai skema rangkaian yang telah disusun. Proses ini mencakup pemasangan *keypad* sebagai perangkat *input* utama, penyambungan *servo motor* sebagai aktuator mekanis untuk membuka dan menutup *solenoid key*, serta pemasangan *buzzer* dan LED sebagai indikator kondisi sistem. Selain itu, dilakukan pengujian kelistrikan untuk memastikan bahwa suplai daya 5V dari Arduino mampu mendukung seluruh komponen seperti servo, LCD I2C, RTC, dan *keypad* secara stabil. Perancangan perangkat keras juga mempertimbangkan penempatan fisik komponen agar sistem aman digunakan, pergerakan servo tidak terhalang, serta rangkaian mudah dipelihara maupun dipasang ke pintu prototipe.

2.4 Perancangan Perangkat Lunak

Proses ini mencakup pengaturan kerja sistem *smart door lock* mulai dari *input* melalui *keypad*, pembacaan waktu RTC, hingga *output* pada LCD, *buzzer*, LED, dan servo. Program dikembangkan menggunakan Arduino IDE dengan logika yang menentukan respons terhadap setiap kondisi (Ratama et al., 2025). Ketika pengguna memasukkan kode PIN melalui *keypad*, sistem menampilkan *input* data di LCD, memvalidasi data, dan memberikan respon: jika benar maka servo membuka *solenoid key* dan LED hijau menyala; jika salah maka *alarm buzzer* berbunyi dan LED merah menyala. Setiap aktivitas dicatat melalui serial monitor dengan waktu dari RTC. Pengujian dilakukan menggunakan *Wokwi Simulator* untuk memastikan seluruh fungsi berjalan sesuai rancangan sebelum diterapkan pada perangkat sebenarnya (Suhaeb et al., 2024).

2.5 Metode Pengujian dan Evaluasi Sistem

Pengujian sistem dilakukan untuk mengevaluasi performa dan keandalan prototipe *smart door lock* berdasarkan beberapa parameter kuantitatif. Evaluasi dilakukan terhadap waktu respons sistem, tingkat keberhasilan autentikasi PIN, respon alarm *buzzer*, serta akurasi pencatatan *audit logging*. Waktu respons sistem diukur sejak pengguna menekan tombol konfirmasi pada *keypad* hingga servomotor bergerak

membuka atau menutup kunci. Pengujian dilakukan sebanyak beberapa kali pada kondisi input benar maupun salah untuk memastikan konsistensi respon sistem.

Selain itu, tingkat *error* sistem dianalisis berdasarkan jumlah kegagalan pembacaan input *keypad*, kesalahan pencatatan log, dan ketidaksesuaian respon output terhadap kondisi yang diberikan. Pengujian *audit logging* dilakukan dengan membandingkan waktu yang tercatat pada serial monitor dengan waktu aktual dari modul RTC DS1307. Sistem juga diuji pada beberapa kondisi waktu berbeda, yaitu pagi, siang, dan malam, untuk memastikan kestabilan operasional prototipe dalam penggunaan berkelanjutan.

Konsumsi daya listrik (*watt*) diukur dengan menggunakan formula:

$$P = V \times I$$

P = Daya listrik Watt (W)

V = Tegangan listrik Volt (V)

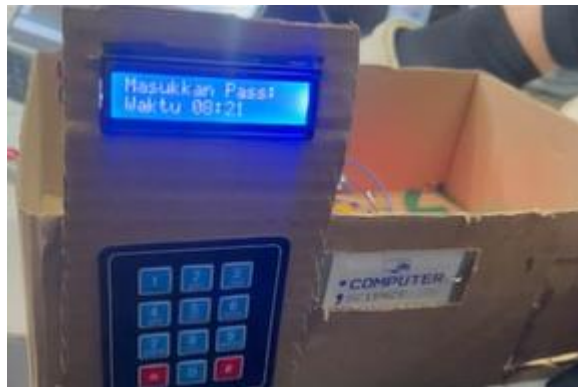
I = Arus listrik Ampere (A)

Hasil pengujian kemudian dianalisis untuk mengetahui tingkat keberhasilan sistem dalam menjalankan fungsi autentikasi, keamanan alarm, dan pencatatan aktivitas akses secara *real-time* sebagai bagian dari evaluasi performa prototipe *smart door lock* berbasis mikrokontroler.

3. Hasil dan Pembahasan

3.1 Hasil Perancangan Sistem

Hasil perancangan sistem *smart door lock* menunjukkan bahwa seluruh komponen *hardware* dan *software* dapat berfungsi dan terintegrasi dengan baik. *Keypad* berhasil digunakan sebagai *input* PIN, LCD menampilkan status sistem, RTC mencatat waktu akses, LED dan *buzzer* memberikan indikator visual dan audio, sementara servo motor bekerja sebagai penggerak *solenoid key*. Program arduino telah mengimplementasikan verifikasi PIN, kontrol servo, alarm, dan pencatatan *audit logging* secara *real-time*. Secara keseluruhan, sistem berjalan stabil dan mampu merespon setiap *input* sesuai yang dirancang.



Gambar 4. Prototipe sistem *smart door lock*

3.2 Hasil Pengujian Sistem

Pada tahap pengujian, dilakukan proses pengambilan data untuk memastikan setiap bagian dari sistem *smart door lock* bekerja sesuai dengan fungsi yang telah dirancang. Pengambilan data ini dilakukan melalui beberapa format pencatatan. Setiap format digunakan untuk menguji komponen tertentu secara terstruktur.

Tabel 2. Hasil pengujian *keypad*

No.	Skenario Uji	Input/ Kondisi	Hasil yang Diharapkan	Hasil Uji
1	Password benar	Input: 1234, Klik #	LED hijau menyala, servo membuka, LCD menampilkan "Akses Diterima", log tersimpan	Berhasil Waktu respon 191 ms Tingkat error 0,00
2	Password salah 1×	Input acak	LED merah berkedip, LCD "Akses Ditolak", log gagal tersimpan	Berhasil Waktu respon 200 ms Tingkat error 0,00
3	Password salah 3×	Input acak salah 3 kali berturut-turut	Buzzer berbunyi, LED merah berkedip, sistem <i>lockout</i> , percobaan reset	Berhasil Waktu respon 212 ms Tingkat error 0,00

Tabel 3. Hasil Pengujian Servo Motor

No.	Skenario Uji	Input/ Kondisi	Hasil yang Diharapkan	Hasil Uji
1	Perintah buka	Password benar	Servo berputar 90° membuka kunci	Berhasil Waktu respon 150 ms Tingkat error 0,00
2	Perintah tutup otomatis	Setelah delay 7 detik	Servo kembali ke 0° (kunci tertutup)	Berhasil Waktu respon 150 ms Tingkat error 0,00

Tabel 4. Hasil Pengujian Audit Logging

No.	Skenario Uji	Input/ Kondisi	Hasil yang Diharapkan	Hasil Uji
1	Log akses berhasil	Password benar	Log berisi timestamp + status “BERHASI L”	Berhasil Waktu respon 44 ms Tingkat error 0,00
2	Log akses gagal	Password salah	Log berisi timestamp + status “GAGAL”	Berhasil Waktu respon 44 ms Tingkat error 0,00
3	Menampil kan log	Tombol “0” ditekan	Serial monitor menampilkan riwayat log	Berhasil Waktu respon 240 ms Tingkat error 0,00

Tabel 5. Hasil Pengujian Buzzer

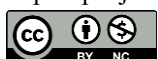
No.	Skenario Uji	Input/ Kondisi	Hasil yang Diharapkan	Hasil Uji
1	Alarm	Jika 3 kali gagal masuk	Buzzer beep panjang & LED merah kedip	Berhasil Waktu respon 50 ms Tingkat error 0,00

Tabel 6. Hasil Pengujian Keadaan IDLE (*Baseline Test*)

No.	Fungsi	Waktu Eksekusi	Keterangan
1	Loop Eksekusi (loop())	312–320 μ s	Stabil dan ringan
2	Pembacaan RTC DS1307	1072–1088 μ s	Tidak berubah signifikan
3	Free SRAM	383 bytes	Menjadi <i>baseline</i> untuk perbandingan
4	Keypad scan	<i>Timeout</i>	Tidak ada tombol ditekan; sistem merespons timeout dengan benar.
5	LCD <i>update</i>	41,352 μ s (41.3 ms)	Waktu terbesar; normal untuk LCD I2C 16×2
6	RTC <i>read</i>	1,068 μ s	Konsisten dengan <i>baseline</i>
7	Servo Command Exec	52 μ s	Perintah servo dieksekusi sangat cepat
8	Servo Move Duration	150,056 μ s (150 ms)	Memiliki durasi eksekusi terbesar
9	EEPROM <i>read</i>	240 μ s	Pembacaan data lebih lambat dari tulis, namun normal
10	Buzzer tone() Exec	64 μ s	Eksekusi fungsi buzzer sangat ringan
11	Buzzer Active	50,016 μ s (50 ms)	Durasi buzzer aktif sesuai program
12	LED Command Exec	8 μ s	Waktu eksekusi digital Write sangat cepat
13	LED ON duration	30,002 μ s (30 ms)	Durasi LED menyala selama benchmark
14	Free SRAM	361 bytes	Memori menurun 22 bytes setelah seluruh komponen aktif

Tabel 7. Hasil Pengujian Waktu Respon

No.	Jenis Pengujian	Waktu (ms)	Keterangan
1	Waktu Respons Logika (Input ke Validasi PIN)	40–60 ms	Proses validasi PIN. Sangat cepat dan stabil
2	Waktu Eksekusi Perintah Servo	0.05 ms (52 μ s)	Waktu mikrokontroler mengirim perintah ke servo
3	Waktu Pergerakan Servo (<i>Servo Move Duration</i>)	150 ms	Durasi servo bergerak dari posisi terkunci ke posisi Terbuka
4	Waktu Pembacaan RTC	1.06 ms (1068 μ s)	Lama pembacaan waktu dari RTC DS1307 untuk keperluan audit log
5	Waktu Respons Total	191–212 ms	Total waktu dari input pengguna sampai pintu terbuka



Tabel 8. Hasil Pengujian Penggunaan SRAM

No.	Kondisi	Free SRAM (bytes)	Keterangan
1	IDLE (<i>baseline</i>)	383	Sistem hanya menjalankan proses dasar (<i>keypad scan</i> dan <i>RTC read</i>)
2	Setelah <i>Benchmark</i>	361	Memori berkurang 22 bytes akibat buffer LCD, EEPROM, dan proses benchmark

Tabel 9. Hasil Pengujian Penggunaan EEPROM

No.	Kondisi	Waktu Eksekusi	Keterangan
1	EEPROM <i>write</i>	44 μ s	Proses penulisan audit log cepat dan stabil
2	EEPROM <i>read</i>	240 μ s	Pembacaan lebih lambat namun tetap dalam batas normal

Tabel 10. Hasil Pengujian Konsumsi Daya

No.	Kondisi	Tegangan (V)	Arus (mA)
1	Normal (IDLE)	5 v	130 mA
2	Komponen bekerja	5 v	160 mA

Perhitungan daya normal:

$$P = V \times I$$

$$P = 5 \times 0,13$$

$$P = 0,65 \text{ watt}$$

Perhitungan daya saat komponen bekerja:

$$P = V \times I$$

$$P = 5 \times 0,16$$

$$P = 0,80 \text{ watt}$$

3.3 Pembahasan

Sistem *smart door lock* menunjukkan kinerja yang sesuai dengan rancangan perangkat lunak dan logika sistem yang telah dirancang. Setiap skenario uji berhasil dijalankan dengan hasil yang konsisten terhadap kondisi *input* yang diberikan. Pada pengujian dengan *input* PIN benar, sistem merespon dengan LED hijau menyala, servo motor bergerak membuka kunci pintu, serta LCD menampilkan pesan “Akses Diterima”. Selain itu, sistem mencatat aktivitas akses tersebut ke dalam *log* melalui serial monitor lengkap dengan *timestamp* dari modul RTC. Sedangkan pengujian dengan *input* PIN salah, sistem menampilkan pesan “Akses Ditolak” pada LCD, diikuti LED merah berkedip sebagai indikator kesalahan *input*, dan data percobaan disimpan dalam *log* sebagai akses gagal. Apabila PIN yang dimasukkan tiga kali salah berturut-turut, maka sistem memasuki mode penguncian (*lockout*) dan *alarm buzzer* berbunyi panjang berulang, LED merah terus berkedip, dan sistem menolak akses lebih lanjut hingga dilakukan *reset*. Hal ini menunjukkan bahwa fitur keamanan terhadap percobaan akses berulang bekerja sebagaimana mestinya.

Sistem juga diuji dalam kondisi waktu yang berbeda berdasarkan pembacaan modul RTC, yaitu pagi, siang, dan malam. Pada kondisi tersebut, sistem tetap beroperasi dengan baik dan menampilkan *timestamp* yang sesuai di setiap pencatatan *log*. Hal ini membuktikan bahwa komponen RTC mampu mencatat waktu secara akurat tanpa memengaruhi fungsi utama sistem. Dengan demikian, dapat disimpulkan bahwa keseluruhan proses mulai dari *input*, pengambilan keputusan, hingga *output* sistem berjalan stabil di berbagai kondisi waktu, dan semua fitur keamanan serta pencatatan aktivitas berfungsi dengan baik sesuai rancangan.

Jika dibandingkan dengan beberapa penelitian sebelumnya, sistem yang dikembangkan pada penelitian ini memiliki pendekatan yang lebih sederhana namun tetap mampu menyediakan fitur keamanan yang terintegrasi. Penelitian *smart door lock* berbasis PIN sebelumnya umumnya hanya menyediakan fungsi autentikasi akses tanpa pencatatan aktivitas pengguna secara otomatis. Sementara itu, beberapa penelitian berbasis IoT telah menyediakan monitoring jarak jauh, namun memerlukan konektivitas internet dan konfigurasi sistem yang lebih kompleks. Pada penelitian ini, integrasi



otentikasi *keypad*, alarm *buzzer*, dan *audit logging* berbasis RTC dalam satu sistem berbasis Arduino Uno memberikan solusi yang lebih sederhana, terjangkau, dan mudah diterapkan untuk kebutuhan keamanan ruang laboratorium. Meskipun belum mendukung monitoring berbasis jaringan, sistem ini tetap mampu menyediakan pencatatan aktivitas akses secara *real-time* sebagai bentuk pengawasan keamanan ruangan.

Waktu respon sistem menjadi aspek penting dalam implementasi keamanan pintu karena keterlambatan respon dapat memengaruhi kenyamanan pengguna maupun efektivitas pengamanan ruangan. Pada prototipe ini, respon servo motor dan tampilan status pada LCD berlangsung secara cepat setelah proses validasi PIN dilakukan, sehingga akses dapat diberikan atau ditolak secara langsung. Selain itu, akurasi modul RTC berperan penting dalam audit logging karena setiap aktivitas akses memerlukan pencatatan waktu yang tepat untuk kebutuhan *monitoring* maupun investigasi keamanan apabila terjadi percobaan akses tidak sah.

Meskipun sistem telah berjalan dengan baik, penelitian ini masih memiliki beberapa keterbatasan yang perlu diperhatikan secara kritis. Sistem masih bergantung pada satu daya utama Arduino sehingga apabila terjadi pemadaman listrik, fungsi keamanan dan pencatatan aktivitas dapat berhenti beroperasi. Selain itu, *audit logging* masih disimpan secara lokal melalui serial monitor sehingga data riwayat akses belum memiliki mekanisme penyimpanan permanen maupun monitoring jarak jauh. Dari sisi keamanan, autentikasi masih menggunakan metode PIN *keypad* yang memiliki potensi risiko seperti pembagian kode akses antar pengguna atau kemungkinan PIN diketahui oleh pihak lain. Sistem juga belum dilengkapi dengan enkripsi data maupun autentikasi multi-faktor yang umumnya digunakan pada sistem keamanan *modern*. Keterbatasan lainnya adalah belum dilakukannya pengujian jangka panjang terhadap ketahanan perangkat keras, terutama pada servo motor yang bekerja secara mekanis dalam proses buka-tutup kunci secara berulang.

Oleh karena itu, pengembangan lebih lanjut diperlukan untuk meningkatkan reliabilitas sistem, seperti penambahan sumber daya cadangan, penyimpanan log berbasis database atau *cloud*, integrasi IoT untuk monitoring *real-time*, serta penerapan metode autentikasi tambahan seperti sidik jari atau pengenalan wajah guna meningkatkan tingkat keamanan sistem.

4. Kesimpulan

Penelitian ini berhasil mengembangkan prototipe *smart door lock* berbasis Arduino Uno yang mampu menjawab kebutuhan sistem keamanan ruang laboratorium yang sederhana, terjangkau, dan dilengkapi fitur *audit logging*. Sistem yang dibangun mampu melakukan autentikasi PIN melalui *keypad*, mengontrol mekanisme penguncian menggunakan servo motor, memberikan peringatan melalui *buzzer* dan LED, serta mencatat seluruh aktivitas akses berdasarkan waktu dari modul RTC.

Hasil pengujian menunjukkan bahwa seluruh fitur utama sistem dapat berjalan secara stabil dan konsisten pada berbagai kondisi pengujian. Keunggulan utama dari sistem ini terletak pada biaya implementasi yang relatif rendah, kemudahan integrasi antar komponen, serta adanya fitur *audit logging* sebagai pendukung *monitoring* keamanan ruang. Namun demikian, sistem masih memiliki keterbatasan karena belum terhubung ke jaringan internet dan penyimpanan log masih bersifat lokal melalui serial monitor. Oleh karena itu, pengembangan lebih lanjut diperlukan untuk meningkatkan keandalan, kapasitas penyimpanan data, serta kemampuan *monitoring* secara *real-time* berbasis IoT.

a. Saran Pengembangan

Pengembangan lebih lanjut sistem *smart door lock* ini dapat ditingkatkan dari sisi keamanan maupun fungsionalitasnya. Salah satu pengembangan yang dapat dilakukan adalah menambahkan metode autentikasi tambahan seperti sensor wajah atau sensor sidik jari sebagai lapisan keamanan kedua. Selain itu, penyimpanan *audit logging* dapat dibuat lebih komprehensif dengan menyimpannya pada media eksternal seperti SD card atau mengirimkannya ke server sehingga data riwayat akses dapat dipantau dalam jangka panjang. Penggunaan modul komunikasi berbasis IoT juga dapat dipertimbangkan agar notifikasi akses atau percobaan pembobolan dapat langsung dikirimkan ke perangkat pengguna secara *real-time*. Dari sisi perangkat keras, desain mekanik untuk pemasangan servo dapat dibuat lebih kokoh agar sistem tetap stabil saat diaplikasikan pada pintu sebenarnya. Dengan pengembangan tersebut, sistem *smart door lock* dapat menjadi lebih aman, modern, dan andal untuk digunakan pada berbagai kebutuhan keamanan ruang.



Referensi

- Dewi, I. P., & Fikri, R. (2023). Optimalisasi Keamanan Rumah dengan Implementasi Sistem Notifikasi Gerbang Cerdas Berbasis Internet of Things (IoT). *Journal of Computer System and Informatics (JoSYC)*, 4(4), 816–829. <https://doi.org/10.47065/josyc.v4i4.4004>
- Juliansyah, D., Sulaiman, S., Ariandi, M., & Dasmen, R. N. (2025). Perancangan Sistem Kemanan Tempat Penyimpanan Barang Menggunakan Konsep Laser Light Sebagai Alarm dan Notifikasi Berbasis IoT. *Ruang Teknik Journal*, 8(2), 339–348. <https://doi.org/10.31869/rtj.v8i2.6693>
- Kanagamalliga, S., Rajalingam, S., Deepasree, S., & Chrisline, C. J. (2026). Revolutionizing Smart Home Security with an Arduino-Powered RFID Door Access Control System. *Computer Vision and Robotics (CVR 2025)*, 411–420. https://doi.org/10.1007/978-3-032-06250-5_34
- KH, M., & Pernando, Y. (2022). Perancangan Prototype Alat Penghapus Papan Tulis Otomatis Dengan Koneksi Bluetooth. *Journal of Digital Ecosystem for Natural Sustainability*, 2(2), 67–72. <https://doi.org/10.63643/jodens.v2i2.171>
- Kustanto, P., Ramadhan, B. K., & Noe'man, A. (2024). Penerapan Metode Prototype dalam Perancangan Media Pembelajaran Interaktif. *Journal of Students' Research in Computer Science*, 5(1), 83–94. <https://doi.org/10.31599/6x0dfz47>
- Listyoningrum, K. I., Fenida, D. Y., & Hamidi, N. (2023). Inovasi Berkelanjutan dalam Bisnis: Manfaatkan Flowchart untuk Mengoptimalkan Nilai Limbah Perusahaan. *Jurnal Informasi Pengabdian Masyarakat*, 1(4), 100–112. <https://doi.org/10.47861/jipm-nalanda.v1i4.552>
- Mubarakali, A., Sharavanan, S., Elshafie, H., & Changalasetty, S. B. (2026). A secure and scalable home security system using IoT, 6G networks, AI-based hybrid deep learning models, blockchain, and smart contracts. *International Journal of Information Security*, 25(15). <https://doi.org/10.1007/s10207-025-01178-x>
- Pratama, R. I., Kiswanto, D., Butarbutar, L. E., & Silalahi, F. J. (2026). Sistem Logging Jaringan Berbasis Website dengan Implementasi Notifikasi Real-Time untuk Peringatan Akses Mencurigakan. *Jurnal Informatika Dan Teknik Elektro Terapan*, 14(1), 40–49. <https://doi.org/10.23960/jitet.v14i1.8201>
- Putri, W. G. R., & Agung, I. W. P. (2025). Iot Smart Door Lock System Menggunakan Double Sensor Berbasis Mikrokontroler ESP32. *Jurnal MNEMONIC*, 8(1), 74–82. <https://doi.org/10.36040/mnemonic.v8i1.12420>
- Ratama, N., Munawaroh, M., & Zakaria, H. (2025). Sistem Otomatis Monitoring Dan Pengendalian Kekeruhan Air Berbasis Arduino Dengan Metode Fuzzy. *Informatika: Jurnal Teknik Informatika Dan Multimedia*, 5(1), 161–168. <https://doi.org/10.51903/bbzcq642>
- Rizky, R. F., Zy, A. T. Z., & Sunge, A. S. (2023). Sistem Smart Door Lock Menggunakan Voice Recognition Berbasis Arduino. *Bulletin of Information Technology (BIT)*, 4(2), 239–244. <https://doi.org/10.47065/bit.v4i2.696>
- Romadon, A., Pranata, A., & Halim, J. (2022). Smart Lock System Dengan Personal Identification Number Berbasis Internet Of Things. *Jurnal Sistem Komputer Triguna Dharma (JURSIK TGD)*, 1(4), 118–125. <https://doi.org/10.53513/jursik.v1i4.5399>
- Sifaunajah, A., Arifin, M. Z., & Shabet, M. R. A. M. (2023). *Mudah Membangun Jam Digital Berbasis Arduino Atmega*. Lembaga Penelitian dan Pengabdian kepada Masyarakat Universitas KH. A. Wahab Hasbullah.
- Sonamoni, J. S., Sikdar, R., Akib, A. S. M. A. S., Islam, S., Sourov, S., Ahasan, M. A. Al, Islam, M., Habib, M. A., & Mridha, M. F. (2024). IoT-Based Smart Remote Door Lock and Monitoring System Using an Android Application. *1st International Conference on Industrial, Manufacturing, and Process Engineering (ICIMP-2024)*. <https://doi.org/10.3390/engproc2024076085>
- Suhaeb, S., Risal, A., & Wahyudi. (2024). Pemanfaatan Wokwi Simulation untuk Pengujian Mikrokontroler Light Emitting Diode (LED) yang Efisien dan Akurat. *Micronic: Journal of Multidisciplinary Electrical and Electronics Engineering*, 2(1), 1–8. <https://doi.org/10.61220/micronic.v2i1.240>
- Wakhid, A. R., Ilmi, U., Bachri, A., Faroh, R. A., Santoso, E. W., & Erlangga, G. B. (2026). Sistem Keamanan Sepeda Motor menggunakan Modul GPS Neo-7M, Solenoid Key Berbasis ESP8266. *Jurnal Riset Rumpun Ilmu Teknik*, 5(1), 240–252. <https://doi.org/10.55606/jurritek.v5i1.7432>



Wulandari, D. A. N., Bahar, A. A. H., Arfananda, M. G., & Apriyani, H. (2021). Prototyping Model in Information System Development of Al-Ruhamaa' Bogor Yatim Center Foundation. *Jurnal PILAR Nusa Mandiri*, 17(2), 127–136. <https://doi.org/10.33480/pilar.v17i2.2375>

