

SISTEM SMART DOOR LOCK MENGGUNAKAN METODE AUTENTIKASI INTEGRASI MULTIFAKTOR BERBASIS ESP32

**Muhammad Yusril Maulana¹, Lusiarakhmawati², Endryansyah³,
Raden Roro Hapsari Peni Agustin Tjahyaningtijas⁴**

S1 Teknik Elektro, Fakultas Teknik, Universitas Negeri Surabaya

muhammadyusril.22103@mhs.unesa.ac.id, lusiarakhmawati@unesa.ac.id, endryansyah@unesa.ac.id,
hapsaripeni@unesa.ac.id

Abstract (English)

The low level of security in conventional door locking systems has become one of the common problems caused by the risk of lost keys, key forgery or duplication, and burglary attempts. To overcome these problems, this research implements the concept of multi-factor authentication as a layered security system. This study aims to design and implement a smart door lock system using an ESP32-based multi-factor authentication integration method to improve door access security. The system integrates several authentication methods, namely fingerprint sensors, RFID, and a keypad as a backup method, and is also equipped with monitoring features through the Telegram application and a 16x2 LCD display. Testing was conducted on the accuracy level of sensor readings, system response time, and monitoring notification capabilities. The results showed that the multi-factor authentication-based smart door lock system was able to function properly in controlling door access. The system also successfully sent notifications through Telegram when access was granted, authentication errors occurred, or indications of door break-in attempts were detected. Therefore, this ESP32-based smart door lock system can serve as an alternative solution for improving the security of rooms or valuable storage areas.

Article History

Submitted: 27 June 2026

Accepted: 6 July 2026

Published: 7 July 2026

Key Words

Smart Door Lock, Multi-factor Authentication, ESP32, Internet of Things (IoT).

Abstrak (Indonesia)

Rendahnya tingkat keamanan pada sistem penguncian konvensional menjadi salah satu permasalahan yang sering terjadi akibat risiko kehilangan kunci, pemalsuan atau duplikasi kunci, serta tindakan pembobolan. Untuk mengatasi permasalahan tersebut, penelitian ini menerapkan konsep multi-factor authentication sebagai sistem keamanan berlapis. Penelitian ini bertujuan untuk merancang dan mengimplementasikan sistem smart door lock menggunakan metode autentikasi integrasi multifaktor berbasis ESP32 guna meningkatkan keamanan akses pintu. Sistem ini mengintegrasikan beberapa metode autentikasi, yaitu sensor fingerprint, RFID, dan keypad sebagai metode cadangan, serta dilengkapi fitur monitoring melalui aplikasi Telegram dan tampilan LCD 16x2. Pengujian dilakukan terhadap tingkat akurasi pembacaan sensor, waktu respons sistem, serta kemampuan notifikasi monitoring. Hasil penelitian menunjukkan bahwa sistem smart door lock berbasis autentikasi multifaktor mampu bekerja dengan baik dalam mengontrol akses pintu. Sistem juga berhasil mengirimkan notifikasi melalui Telegram ketika terjadi akses berhasil, kesalahan autentikasi, maupun indikasi pembobolan pintu. Dengan demikian, sistem smart door lock berbasis ESP32 ini dapat menjadi solusi alternatif dalam meningkatkan keamanan ruangan atau tempat penyimpanan barang berharga.

Sejarah Artikel

Submitted: 27 June 2026

Accepted: 6 July 2026

Published: 7 July 2026

Kata Kunci

Smart Door Lock, Autentikasi Multifaktor, ESP32, Internet of Things (IoT).

PENDAHULUAN

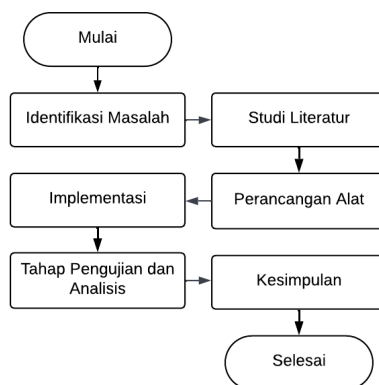
Keamanan rumah dan bangunan merupakan aspek penting yang terus berkembang seiring meningkatnya kebutuhan akan sistem pengamanan yang praktis dan andal. Sistem penguncian konvensional masih memiliki berbagai kelemahan, seperti risiko kehilangan kunci, duplikasi kunci, maupun pembobolan secara paksa. Tindak kejahatan atau kriminal saat ini menjadi bentuk ancaman nyata dan selalu melekat dalam lingkungan masyarakat. Adanya perilaku kejahatan ini secara tidak langsung menimbulkan ketegangan sosial dan juga dapat merusak aturan yang digunakan sebagai pedoman untuk menciptakan ketertiban sosial. Salah satu kejahatan yang sering terjadi di masyarakat adalah tindak pencurian terhadap harta benda (Suharsoyo, 2015).

Banyaknya jumlah perkara kasus tindak pidana pencurian dapat menjadi bukti bahwa kejahatan ini merupakan fenomena sosial yang senantiasa dihadapi dan selalu diusahakan oleh berbagai pihak untuk mengurangi intensitas atau kualitas kejahatan yang terjadi (R. P. Saputra, 2019). Oleh karena itu, diperlukan sistem keamanan pintu yang mampu memberikan perlindungan sekaligus proses pemantauan secara real-time. Perkembangan teknologi Internet of Things (IoT) memungkinkan pengembangan sistem smart door lock yang tidak hanya berfungsi sebagai pengunci pintu, tetapi juga mampu melakukan autentikasi pengguna dan monitoring jarak jauh. Beberapa penelitian tentang smart door lock sudah dilakukan, seperti perancangan smart door lock dengan menggunakan sensor fingerprint (Febriyanto et al., 2019). Kemudian perancangan smart lock system dengan menggunakan Personal Identification Number (PIN) (Romadon et al., 2022). Selain itu terdapat juga perancangan sistem pengamanan pintu dengan menggunakan sensor Radio Frequency Identification (RFID) (Simanjuntak et al., 2020).

Berdasarkan permasalahan tersebut, penelitian ini mengusulkan sistem smart door lock berbasis ESP32 dengan metode autentikasi integrasi multifaktor yang menggabungkan fingerprint, RFID, dan keypad sebagai metode cadangan. Sistem juga dilengkapi fitur monitoring melalui aplikasi Telegram dan tampilan LCD untuk memberikan informasi kondisi pintu secara real-time.

METODE PENELITIAN

Diagram alur penelitian menunjukkan tahapan penelitian dari awal hingga akhir, mulai dari identifikasi masalah sampai dengan penyusunan kesimpulan. Diagram alur penelitian yang digunakan dalam penelitian ini disajikan pada Gambar 1.

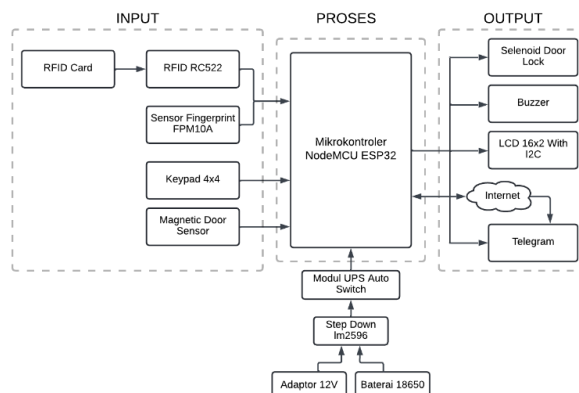


Gambar 1. Diagram Alur Penelitian

Perancangan hardware pada penelitian ini terbagi menjadi 3 yaitu blok diagram, desain perancangan teknis, dan desain alat.

A. Blok Diagram

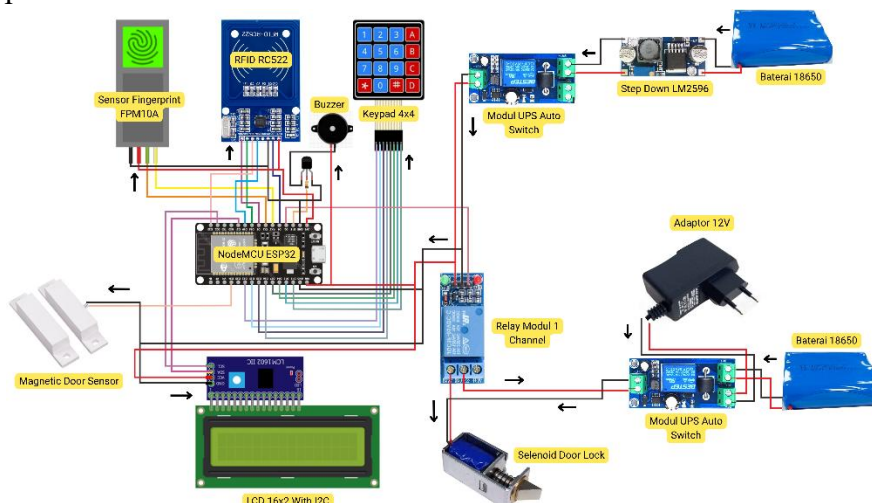
Perancangan sistem dimulai dengan pembuatan blok diagram, di mana setiap blok memiliki fungsi tersendiri sehingga membentuk suatu sistem yang saling terkoneksi satu dan lainnya. Diagram blok juga menggambarkan secara umum bagaimana cara kerja rangkaian secara keseluruhan. Diagram blok dari penelitian ini disajikan pada Gambar 2.



Gambar 2. Blok Diagram

B. Desain Perancangan Teknis

Desain perancangan teknis merupakan gambaran perancangan dengan pengkabelan atau wiring pada setiap komponen yang akan digunakan. Wiring diagram adalah skema pengkabelan yang dibuat berupa jalur-jalur aliran listrik dalam satu rangkaian sistem yang saling terhubung hingga membentuk suatu sistem yang telah ditetapkan. Wiring diagram sistem pada penelitian ini disajikan pada Gambar 3.

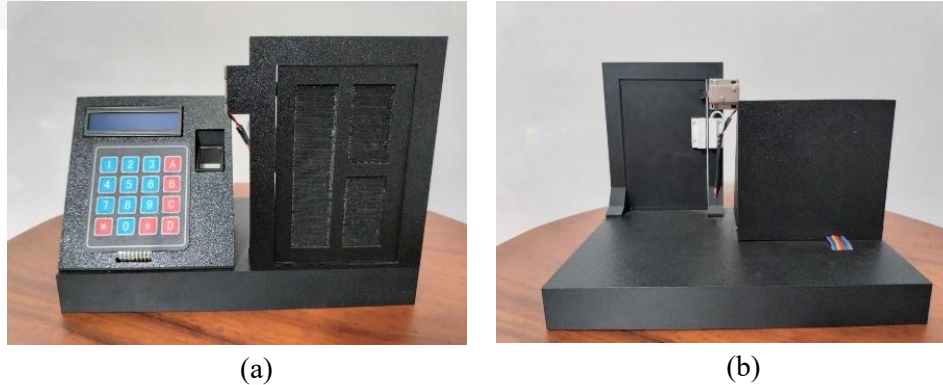


Gambar 3. Wiring Diagram Sistem

C. Desain Kemasan Alat

Perancangan desain kemasan alat merupakan tahap pembuatan wadah atau casing yang digunakan untuk menempatkan seluruh komponen yang telah dirangkai dan berfungsi sebagai

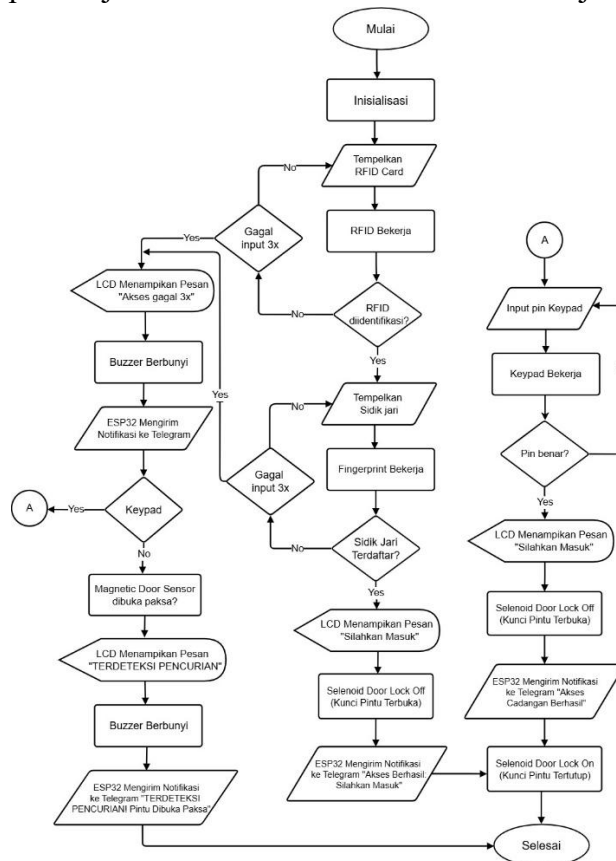
tempat pelindung komponen dari kerusakan yang disebabkan oleh gangguan eksternal. Pada penelitian ini, desain kemasan alat dibuat menggunakan teknologi 3D printing sebagai wadah komponen dan pintu. Desain kemasan alat tersebut disajikan pada Gambar 4.



Gambar 4. Desain Kemasan Alat, (a) Tampak Depan dan (b) Tampak Belakang

D. Perancangan Perangkat Lunak (Software)

Proses pengembangan perangkat lunak diawali dengan penyusunan alur kerja sistem dalam bentuk flowchart. Tahap ini dilakukan untuk memastikan perangkat keras dapat beroperasi sesuai logika dan instruksi yang telah dirancang sebelumnya. Diagram alur tersebut menggambarkan tahapan kerja sistem secara keseluruhan dan disajikan pada Gambar 5.



Gambar 5. Flowchart

E. Tahap Pengujian dan Analisis

Pada tahap ini, alat yang telah dirancang akan dilakukan pengujian secara keseluruhan. Apabila sistem yang dirancang tidak memenuhi indikator pencapaian yang digunakan pada alat ini, maka akan dilakukan evaluasi dan pengujian kembali. Tahap pengujian pada penelitian ini dibagi menjadi tiga bagian antara lain sebagai berikut:

1. Pengujian Masing-masing Sensor

Pengujian akurasi masing-masing sensor menggunakan persamaan berikut.

$$\text{Akurasi} = \frac{\text{pengujian berhasil}}{\text{total pengujian}} \times 100\% \quad (1)$$

(Putri et al., 2025)

Nilai waktu respons rata-rata dari seluruh aktivitas pengujian performa menggunakan persamaan berikut.

$$\bar{x} = \frac{(d_1 + d_2 + \dots + d_n)}{n} \quad (2)$$

(Pangestu et al., 2023)

Keterangan:

$\bar{x}$ = waktu respons rata-rata

d_n = nilai rata-rata waktu respons aktivitas pengujian performa ke-n

n = jumlah aktivitas pengujian performa

2. Pengujian Notifikasi Telegram

Pengujian notifikasi Telegram menggunakan persamaan berikut.

$$\bar{x} = \frac{(d_1 + d_2 + \dots + d_n)}{n} \quad (2)$$

(Pangestu et al., 2023)

Keterangan:

$\bar{x}$ = waktu respons rata-rata

d_n = nilai rata-rata waktu respons aktivitas pengujian performa ke-n

n = jumlah aktivitas pengujian performa

3. Pengujian Sistem Secara Keseluruhan

Pengujian sistem secara keseluruhan menggunakan persamaan berikut.

$$\text{Akurasi sistem} = \frac{(\text{JSB} - \text{JTSH})}{\text{TSP}} \times 100\% \quad (3)$$

Keterangan:

JSB = jumlah skenario berhasil

JTSH = jumlah tidak sesuai harapan

TSP = total skenario pengujian

Nilai waktu respons rata-rata dari sistem secara keseluruhan menggunakan persamaan berikut.

$$\bar{x} = \frac{(d_1 + d_2 + \dots + d_n)}{n} \quad (2)$$

(Pangestu et al., 2023)

Keterangan:

$\bar{x}$ = waktu respons rata-rata

d_n = nilai rata-rata waktu respons aktivitas pengujian performa ke-n

n = jumlah aktivitas pengujian performa

HASIL DAN PEMBAHASAN

A. Pengujian RFID

1. Pengujian Tingkat Akurasi Pembacaan Kartu RFID

Berdasarkan hasil pengujian sebanyak 30 kali percobaan dengan variasi posisi dan jarak kartu RFID, diperoleh kemampuan pembacaan yang berbeda pada setiap kondisi pengujian. Hasil pengujian pada posisi horizontal yang disajikan pada Tabel 1 menunjukkan bahwa sensor RFID mampu membaca kartu dengan baik hingga jarak maksimum 3 cm. Pada posisi vertikal yang ditunjukkan pada Tabel 2, sensor juga mampu mendeteksi kartu secara optimal hingga jarak 3 cm. Namun, pada jarak 3,5 cm hingga 4,5 cm kartu tidak lagi terdeteksi oleh sistem pada kedua posisi tersebut. Sementara itu, hasil pengujian pada posisi miring 15° yang disajikan pada Tabel 3 menunjukkan penurunan kemampuan pembacaan, di mana kartu hanya dapat terbaca hingga jarak 1,5 cm dan gagal terdeteksi pada jarak 2 cm hingga 4,5 cm. Dokumentasi proses pengujian RFID dengan variasi posisi kartu ditunjukkan pada Gambar 6. Hasil ini menunjukkan bahwa orientasi kartu RFID berpengaruh terhadap kemampuan pembacaan sensor, dengan posisi horizontal dan vertikal memberikan performa yang lebih baik dibandingkan posisi miring 15°.

Tabel 1. Pengujian Akurasi RFID Posisi Horizontal

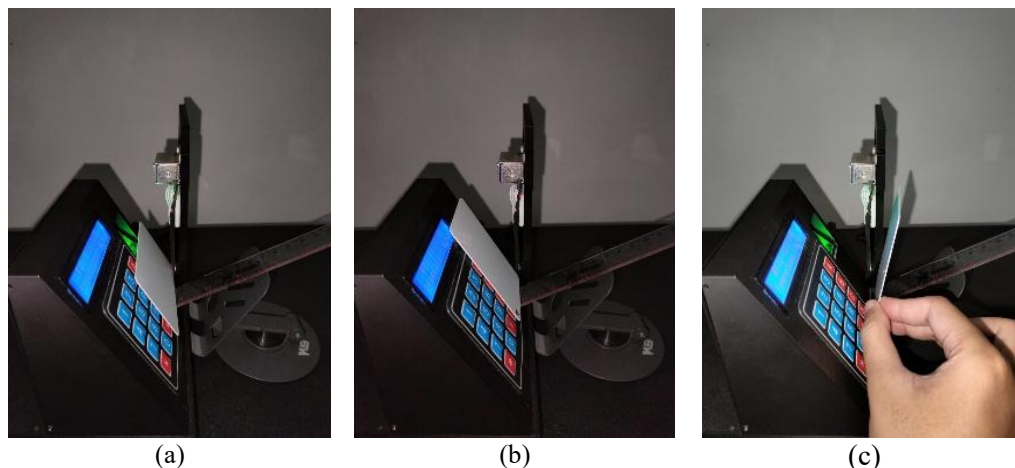
Percobaan Ke-	Kartu RFID	Posisi Kartu RFID	Jarak (cm)	Status
1	4	Horizontal	0 cm	Terbaca
2	2	Horizontal	0.5 cm	Terbaca
3	3	Horizontal	1 cm	Terbaca
4	1	Horizontal	1.5 cm	Terbaca
5	3	Horizontal	2 cm	Terbaca
6	4	Horizontal	2.5 cm	Terbaca
7	1	Horizontal	3 cm	Terbaca
8	2	Horizontal	3.5 cm	Tidak Terbaca
9	3	Horizontal	4 cm	Tidak Terbaca
10	1	Horizontal	4.5 cm	Tidak Terbaca

Tabel 2. Pengujian Akurasi RFID Posisi Vertikal

Percobaan Ke-	Kartu RFID	Posisi Kartu RFID	Jarak (cm)	Status
1	2	Vertikal	0 cm	Terbaca
2	4	Vertikal	0.5 cm	Terbaca
3	1	Vertikal	1 cm	Terbaca
4	3	Vertikal	1.5 cm	Terbaca
5	4	Vertikal	2 cm	Terbaca
6	3	Vertikal	2.5 cm	Terbaca
7	1	Vertikal	3 cm	Terbaca
8	2	Vertikal	3.5 cm	Tidak Terbaca
9	3	Vertikal	4 cm	Tidak Terbaca
10	1	Vertikal	4.5 cm	Tidak Terbaca

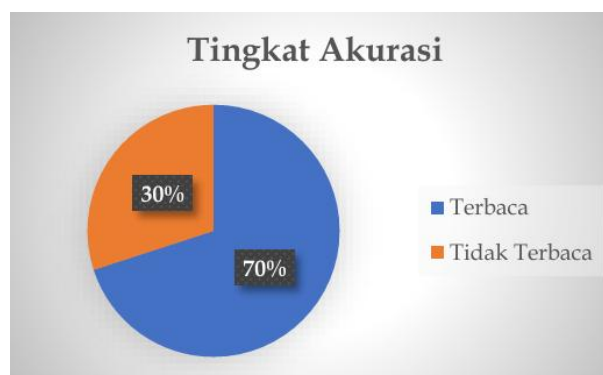
Tabel 3. Pengujian Akurasi RFID Posisi Miring 15°

Percobaan Ke-	Kartu RFID	Posisi Kartu RFID	Jarak (cm)	Status
1	1	Miring	0 cm	Terbaca
2	2	Miring	0.5 cm	Terbaca
3	3	Miring	1 cm	Terbaca
4	4	Miring	1.5 cm	Terbaca
5	2	Miring	2 cm	Tidak Terbaca
6	1	Miring	2.5 cm	Tidak Terbaca
7	4	Miring	3 cm	Tidak Terbaca
8	3	Miring	3.5 cm	Tidak Terbaca
9	2	Miring	4 cm	Tidak Terbaca
10	4	Miring	4.5 cm	Tidak Terbaca



Gambar 6. Pengujian kartu Gambar 7, 8, dan 9 Penyajian artu RFID dengan beberapa posisi sudut kemiringan, (a) Horizontal (b) Vertikal, (c) Miring 15°

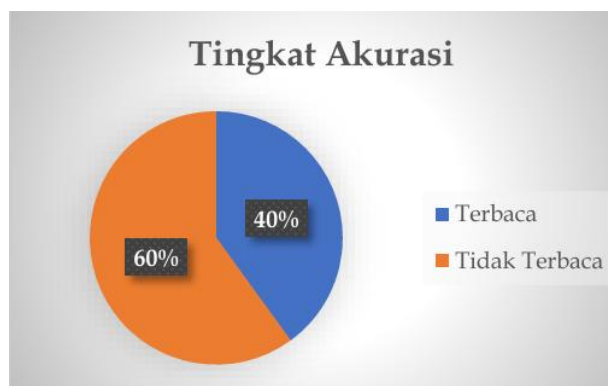
Untuk mempermudah analisis, data dari Tabel 1, 2, dan 3 disajikan dalam bentuk grafik pada Gambar 7, 8, dan 9 Penyajian data dalam bentuk grafik bertujuan untuk meningkatkan visibilitas tren dan pola, sehingga memudahkan proses analisis secara lebih tepat dan akurat.



Gambar 7. Grafik Pengujian Akurasi RFID Posisi Horizontal



Gambar 8. Grafik Pengujian Akurasi RFID Posisi Vertikal



Gambar 9. Grafik Pengujian Akurasi RFID Posisi Miring 15°

B. Pengujian Fingerprint

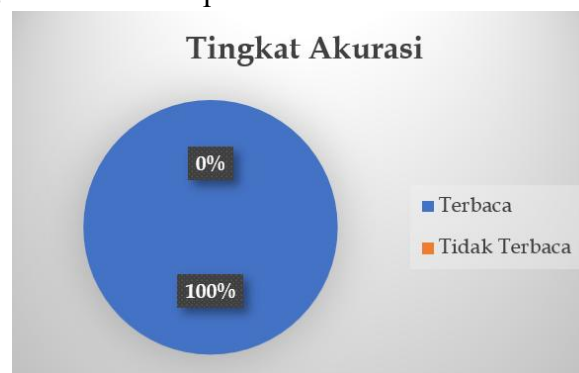
1. Pengujian Tingkat Akurasi Sensor Fingerprint

Berdasarkan hasil pengujian sensor fingerprint yang dilakukan sebanyak 30 kali percobaan, seluruh sidik jari yang terdaftar berhasil dikenali oleh sistem. Pengujian dilakukan menggunakan beberapa jenis jari, yaitu jari telunjuk, jari tengah, jari manis, dan ibu jari. Hasil pengujian yang disajikan pada Tabel 4 menunjukkan bahwa seluruh percobaan berhasil dilakukan tanpa adanya kegagalan identifikasi. Hasil ini menunjukkan bahwa sensor fingerprint memiliki tingkat akurasi sebesar 100% dalam mengenali sidik jari pengguna yang telah terdaftar pada sistem.

Tabel 4. Pengujian Akurasi Fingerprint

Percobaan Ke-	Jari	Status
1	Telunjuk	Terbaca
2	Tengah	Terbaca
3	Manis	Terbaca
4	Ibu jari	Terbaca
5	Tengah	Terbaca
6	Telunjuk	Terbaca
7	Manis	Terbaca
8	Tengah	Terbaca
9	Ibu jari	Terbaca
10	Manis	Terbaca
11	Telunjuk	Terbaca
12	Ibu jari	Terbaca
13	Tengah	Terbaca
14	Manis	Terbaca
15	Telunjuk	Terbaca
16	Tengah	Terbaca
17	Ibu jari	Terbaca
18	Manis	Terbaca
19	Ibu jari	Terbaca
20	Telunjuk	Terbaca
21	Manis	Terbaca
22	Tengah	Terbaca
23	Manis	Terbaca
24	Ibu jari	Terbaca
25	Tengah	Terbaca
26	Telunjuk	Terbaca
27	Tengah	Terbaca
28	Manis	Terbaca
29	Ibu jari	Terbaca
30	Telunjuk	Terbaca

Untuk mempermudah analisis, data dari Tabel 4 disajikan dalam bentuk grafik pada Gambar 10. Penyajian data dalam bentuk grafik bertujuan untuk meningkatkan visibilitas tren dan pola, sehingga memudahkan proses analisis secara lebih tepat dan akurat.



Gambar 10. Grafik Pengujian Akurasi Fingerprint

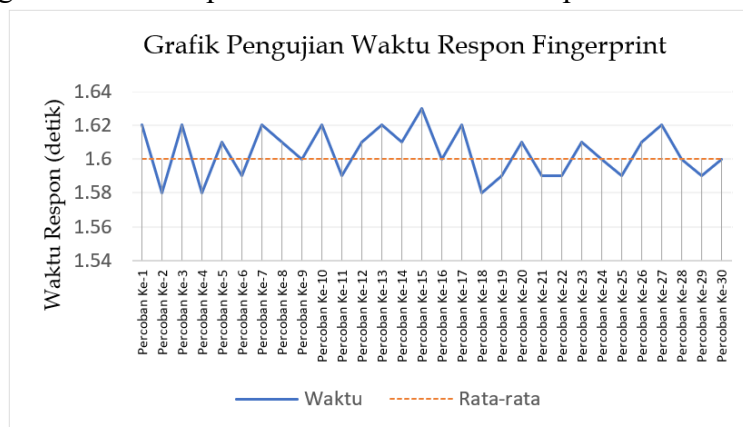
2. Pengujian Waktu Respons Sensor Fingerprint

Berdasarkan hasil pengujian sensor fingerprint pada 30 kali percobaan, diperoleh rata-rata waktu respons sebesar 1,60 detik. Hasil pengujian yang disajikan pada Tabel 5 menunjukkan bahwa waktu respons tercepat terjadi pada percobaan ke-2, ke-4, dan ke-18 dengan nilai 1,58 detik, sedangkan waktu respons terlama terjadi pada percobaan ke-15 dengan nilai 1,63 detik. Hasil ini menunjukkan bahwa sensor fingerprint memiliki waktu respons yang relatif stabil dengan selisih waktu yang kecil antar percobaan.

Tabel 5. Pengujian Waktu Respons Fingerprint

Percobaan Ke-	Jari	Waktu Respon (detik)
1	Telunjuk	1.62
2	Tengah	1.58
3	Manis	1.62
4	Ibu jari	1.58
5	Tengah	1.61
6	Telunjuk	1.59
7	Manis	1.62
8	Tengah	1.61
9	Ibu jari	1.60
10	Manis	1.62
11	Telunjuk	1.59
12	Ibu jari	1.61
13	Tengah	1.62
14	Manis	1.61
15	Telunjuk	1.63
16	Tengah	1.60
17	Ibu jari	1.62
18	Manis	1.58
19	Ibu jari	1.59
20	Telunjuk	1.61
21	Manis	1.59
22	Tengah	1.59
23	Manis	1.61
24	Ibu jari	1.60
25	Tengah	1.59
26	Telunjuk	1.61
27	Tengah	1.62
28	Manis	1.60
29	Ibu jari	1.59
30	Telunjuk	1.60
Rata-rata		1.60

Untuk mempermudah analisis, data dari Tabel 5 disajikan dalam bentuk grafik pada Gambar 11. Penyajian data dalam bentuk grafik bertujuan untuk meningkatkan visibilitas tren dan pola, sehingga memudahkan proses analisis secara lebih tepat dan akurat.



Gambar 11. Grafik Pengujian Waktu Respon Fingerprint

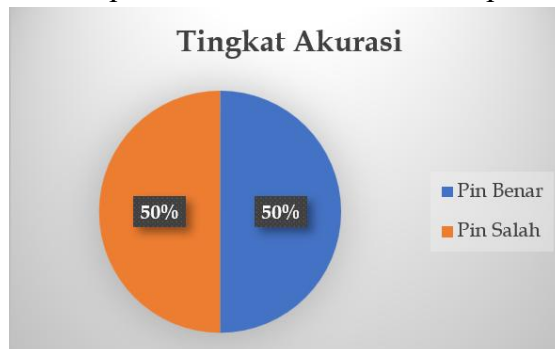
C. Pengujian Keypad

Berdasarkan hasil pengujian keypad yang dilakukan sebanyak 30 kali percobaan, sistem mampu membaca dan memproses input PIN dengan baik. Pengujian menggunakan PIN 4578 sebagai kata sandi yang telah terdaftar pada sistem. Hasil pengujian yang disajikan pada Tabel 6 menunjukkan bahwa dari 30 kali percobaan, sebanyak 15 percobaan dengan PIN yang sesuai berhasil dikenali dan menghasilkan respons “PIN Benar!”, sedangkan 15 percobaan dengan PIN yang tidak sesuai menghasilkan respons “PIN Salah!”.

Tabel 6. Pengujian Akurasi Keypad

Percobaan Ke-	Keyword	Input	Keterangan
1	4578	4578	Pin Benar!
2		0874	Pin Salah!
3		4578	Pin Benar!
4		1234	Pin Salah!
5		4578	Pin Benar!
6		6987	Pin Salah!
7		4578	Pin Benar!
8		3258	Pin Salah!
9		4578	Pin Benar!
10		7124	Pin Salah!
11		4578	Pin Benar!
12		9842	Pin Salah!
13		4578	Pin Benar!
14		5614	Pin Salah!
15		4578	Pin Benar!
16		1698	Pin Salah!
17		4578	Pin Benar!
18		7456	Pin Salah!
19		4578	Pin Benar!
20		3654	Pin Salah!
21		4578	Pin Benar!
22		8521	Pin Salah!
23		4578	Pin Benar!
24		4862	Pin Salah!
25		4578	Pin Benar!
26		7843	Pin Salah!
27		4578	Pin Benar!
28		8137	Pin Salah!
29		4578	Pin Benar!
30		9713	Pin Salah!

Untuk mempermudah analisis, data dari Tabel 6 disajikan dalam bentuk grafik pada Gambar 12. Penyajian data dalam bentuk grafik bertujuan untuk meningkatkan visibilitas tren dan pola, sehingga memudahkan proses analisis secara lebih tepat dan akurat.



Gambar 12. Grafik Pengujian Akurasi Keypad

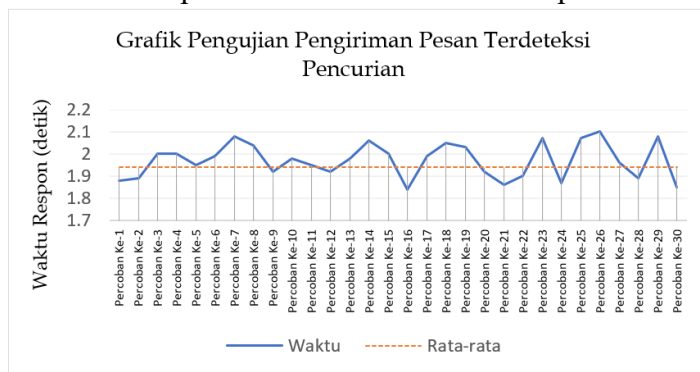
D: Pengujian Notifikasi Telegram

Berdasarkan hasil pengujian pada Tabel 7, notifikasi Telegram pada kondisi terdeteksi pencurian memiliki waktu respons tercepat 1,84 detik dan terlama 2,10 detik, dengan rata-rata waktu penerimaan sebesar 1,94 detik. Hasil ini menunjukkan bahwa sistem mampu mengirimkan notifikasi secara cepat dan responsif. Kecepatan penerimaan notifikasi dipengaruhi oleh kualitas koneksi internet yang digunakan.

Tabel 7. Pengujian Pengiriman Pesan Terdeteksi Pencurian

Percobaan Ke-	Status	Pesan Masuk	Waktu Terima Pesan (detik)
1	Sensor magnet berjauhan	TERDETEKSI PENCURIAN!	1.88
2	Sensor magnet berjauhan	TERDETEKSI PENCURIAN!	1.89
3	Sensor magnet berjauhan	TERDETEKSI PENCURIAN!	2.00
4	Sensor magnet berjauhan	TERDETEKSI PENCURIAN!	2.00
5	Sensor magnet berjauhan	TERDETEKSI PENCURIAN!	1.95
6	Sensor magnet berjauhan	TERDETEKSI PENCURIAN!	1.99
7	Sensor magnet berjauhan	TERDETEKSI PENCURIAN!	2.08
8	Sensor magnet berjauhan	TERDETEKSI PENCURIAN!	2.04
9	Sensor magnet berjauhan	TERDETEKSI PENCURIAN!	1.92
10	Sensor magnet berjauhan	TERDETEKSI PENCURIAN!	1.98
11	Sensor magnet berjauhan	TERDETEKSI PENCURIAN!	1.95
12	Sensor magnet berjauhan	TERDETEKSI PENCURIAN!	1.92
13	Sensor magnet berjauhan	TERDETEKSI PENCURIAN!	1.98
14	Sensor magnet berjauhan	TERDETEKSI PENCURIAN!	2.06
15	Sensor magnet berjauhan	TERDETEKSI PENCURIAN!	2.00
16	Sensor magnet berjauhan	TERDETEKSI PENCURIAN!	1.84
17	Sensor magnet berjauhan	TERDETEKSI PENCURIAN!	1.99
18	Sensor magnet berjauhan	TERDETEKSI PENCURIAN!	2.05
19	Sensor magnet berjauhan	TERDETEKSI PENCURIAN!	2.03
20	Sensor magnet berjauhan	TERDETEKSI PENCURIAN!	1.92
21	Sensor magnet berjauhan	TERDETEKSI PENCURIAN!	1.86
22	Sensor magnet berjauhan	TERDETEKSI PENCURIAN!	1.90
23	Sensor magnet berjauhan	TERDETEKSI PENCURIAN!	2.07
24	Sensor magnet berjauhan	TERDETEKSI PENCURIAN!	1.87
25	Sensor magnet berjauhan	TERDETEKSI PENCURIAN!	2.07
26	Sensor magnet berjauhan	TERDETEKSI PENCURIAN!	2.10
27	Sensor magnet berjauhan	TERDETEKSI PENCURIAN!	1.96
28	Sensor magnet berjauhan	TERDETEKSI PENCURIAN!	1.89
29	Sensor magnet berjauhan	TERDETEKSI PENCURIAN!	2.08
30	Sensor magnet berjauhan	TERDETEKSI PENCURIAN!	1.85
Rata-rata			1.94

Untuk mempermudah analisis, data dari Tabel 7 disajikan dalam bentuk grafik pada Gambar 13. Penyajian data dalam bentuk grafik bertujuan untuk meningkatkan visibilitas tren dan pola, sehingga memudahkan proses analisis secara lebih tepat dan akurat.



Gambar 13. Grafik Pengujian Pengiriman Pesan Terdeteksi Pencurian

E. Pengujian Sistem Secara Keseluruhan

1. Pengujian Tingkat Akurasi Sistem Secara Keseluruhan

Hasil pengujian yang disajikan pada Tabel 8 menunjukkan bahwa seluruh 30 percobaan berhasil dijalankan sesuai dengan yang diharapkan tanpa adanya kegagalan. Berdasarkan perhitungan akurasi sistem, diperoleh nilai akurasi sebesar 100%. Hasil ini menunjukkan bahwa sistem mampu beroperasi sesuai dengan perancangan dan memenuhi indikator keberhasilan yang telah ditetapkan.

Tabel 8. Pengujian Akurasi Sistem Secara Keseluruhan

Percobaan Ke-	RFID	Fingerprint	Solenoid Door	Notifikasi Telegram
1	Terbaca	Terbaca	Pintu Terbuka	Terkirim
2	Terbaca	Terbaca	Pintu Terbuka	Terkirim
3	Terbaca	Terbaca	Pintu Terbuka	Terkirim
4	Terbaca	Terbaca	Pintu Terbuka	Terkirim
5	Terbaca	Terbaca	Pintu Terbuka	Terkirim
6	Terbaca	Terbaca	Pintu Terbuka	Terkirim
7	Terbaca	Terbaca	Pintu Terbuka	Terkirim
8	Terbaca	Terbaca	Pintu Terbuka	Terkirim
9	Terbaca	Terbaca	Pintu Terbuka	Terkirim
10	Terbaca	Terbaca	Pintu Terbuka	Terkirim
11	Terbaca	Terbaca	Pintu Terbuka	Terkirim
12	Terbaca	Terbaca	Pintu Terbuka	Terkirim
13	Terbaca	Terbaca	Pintu Terbuka	Terkirim
14	Terbaca	Terbaca	Pintu Terbuka	Terkirim
15	Terbaca	Terbaca	Pintu Terbuka	Terkirim
16	Terbaca	Terbaca	Pintu Terbuka	Terkirim
17	Terbaca	Terbaca	Pintu Terbuka	Terkirim
18	Terbaca	Terbaca	Pintu Terbuka	Terkirim
19	Terbaca	Terbaca	Pintu Terbuka	Terkirim
20	Terbaca	Terbaca	Pintu Terbuka	Terkirim
21	Terbaca	Terbaca	Pintu Terbuka	Terkirim
22	Terbaca	Terbaca	Pintu Terbuka	Terkirim
23	Terbaca	Terbaca	Pintu Terbuka	Terkirim
24	Terbaca	Terbaca	Pintu Terbuka	Terkirim
25	Terbaca	Terbaca	Pintu Terbuka	Terkirim
26	Terbaca	Terbaca	Pintu Terbuka	Terkirim
27	Terbaca	Terbaca	Pintu Terbuka	Terkirim
28	Terbaca	Terbaca	Pintu Terbuka	Terkirim
29	Terbaca	Terbaca	Pintu Terbuka	Terkirim
30	Terbaca	Terbaca	Pintu Terbuka	Terkirim

Untuk mempermudah analisis, data dari Tabel 8 disajikan dalam bentuk grafik pada Gambar 14. Penyajian data dalam bentuk grafik bertujuan untuk meningkatkan visibilitas tren dan pola, sehingga memudahkan proses analisis secara lebih tepat dan akurat.



Gambar 14. Grafik Pengujian Akurasi Sistem Secara Keseluruhan

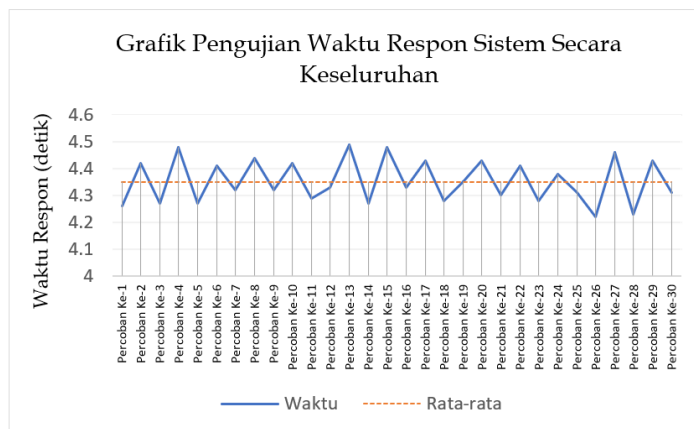
2. Pengujian Waktu Respons Sistem Secara Keseluruhan

Berdasarkan 30 kali percobaan, sistem smart door lock menunjukkan performa yang stabil dalam proses autentikasi dan pengiriman notifikasi. Hasil pengujian yang disajikan pada Tabel 9 menunjukkan bahwa waktu respons pembacaan RFID berada pada rentang 0,80–0,85 detik dengan rata-rata 0,82 detik, sedangkan waktu pembacaan fingerprint berada pada rentang 1,58–1,63 detik dengan rata-rata 1,60 detik. Waktu pengiriman notifikasi Telegram berkisar antara 1,79–2,10 detik dengan rata-rata 1,93 detik. Secara keseluruhan, total waktu respons sistem berada pada rentang 4,22–4,49 detik dengan rata-rata 4,35 detik. Hasil ini menunjukkan bahwa sistem mampu melakukan autentikasi multifaktor dan mengirimkan notifikasi secara real-time dalam waktu kurang dari 5 detik.

Tabel 9. Pengujian Waktu Respons Sistem Secara Keseluruhan

Percobaan Ke-	Pembacaan RFID (milidetik)	Pembacaan Fingerprint (detik)	Notifikasi Telegram (detik)	Total Waktu (detik)
1	0.83	1.62	1.81	4.26
2	0.85	1.61	1.96	4.42
3	0.80	1.63	1.84	4.27
4	0.84	1.59	2.05	4.48
5	0.83	1.60	1.84	4.27
6	0.84	1.61	1.96	4.41
7	0.81	1.59	1.92	4.32
8	0.82	1.62	2.00	4.44
9	0.83	1.58	1.91	4.32
10	0.84	1.63	1.95	4.42
11	0.81	1.59	1.89	4.29
12	0.82	1.60	1.91	4.33
13	0.81	1.58	2.10	4.49
14	0.82	1.58	1.87	4.27
15	0.81	1.63	2.04	4.48
16	0.80	1.58	1.95	4.33
17	0.83	1.62	1.98	4.43
18	0.80	1.60	1.88	4.28
19	0.85	1.61	1.89	4.35
20	0.81	1.59	2.03	4.43
21	0.81	1.58	1.91	4.3
22	0.84	1.62	1.95	4.41
23	0.84	1.61	1.83	4.28
24	0.85	1.58	1.95	4.38
25	0.81	1.60	1.90	4.31
26	0.83	1.60	1.79	4.22
27	0.85	1.63	1.98	4.46
28	0.82	1.59	1.82	4.23
29	0.80	1.61	2.02	4.43
30	0.82	1.59	1.90	4.31
Rata-rata				4.35

Untuk mempermudah analisis, data dari Tabel 9 disajikan dalam bentuk grafik pada Gambar 15. Penyajian data dalam bentuk grafik bertujuan untuk meningkatkan visibilitas tren dan pola, sehingga memudahkan proses analisis secara lebih tepat dan akurat.



Gambar 15. Grafik Pengujian Waktu Respons Sistem Secara Keseluruhan

PENUTUP

Simpulan

Berdasarkan hasil penelitian yang telah dilakukan, sistem smart door lock menggunakan metode autentikasi integrasi multifaktor berbasis ESP32 berhasil dirancang dan diimplementasikan dengan mengintegrasikan sensor fingerprint, RFID RC522, keypad 4×4, magnetic door sensor, serta notifikasi Telegram berbasis Internet of Things (IoT). Sistem menerapkan autentikasi multifaktor melalui kombinasi sidik jari dan kartu RFID sebagai metode utama akses pintu, sementara keypad digunakan sebagai metode cadangan saat terjadi gangguan jaringan internet atau kondisi darurat tertentu. Selain itu, sistem mampu memberikan notifikasi secara real-time melalui Telegram.

Hasil pengujian menunjukkan bahwa sensor RFID memiliki tingkat akurasi 70% pada posisi horizontal dan vertikal dengan jarak baca maksimal 3 cm, serta 40% pada posisi miring dengan jarak baca 1,5 cm. Sensor fingerprint menunjukkan performa yang sangat baik dengan tingkat akurasi 100% dan waktu respons rata-rata 1,60 detik. Pengujian keypad sebagai metode autentikasi cadangan juga berjalan dengan baik dalam membedakan PIN yang benar dan salah. Selain itu, notifikasi Telegram berhasil dikirim dengan rata-rata waktu respons 1,94 detik ketika sistem mendeteksi percobaan pembobolan. Secara keseluruhan, sistem terintegrasi mampu bekerja sesuai perancangan dengan tingkat akurasi 100% dan waktu respons rata-rata 4,35 detik, sehingga dapat meningkatkan keamanan akses pintu melalui penerapan mekanisme keamanan berlapis.

Saran

Berdasarkan hasil penelitian yang telah dilakukan, masih terdapat beberapa keterbatasan pada sistem yang dapat menjadi bahan pengembangan pada penelitian selanjutnya. Sistem smart door lock dapat ditingkatkan dengan menambahkan metode autentikasi lain, seperti face recognition, One Time Password (OTP), atau mobile authentication untuk memperkuat keamanan akses. Selain itu, integrasi modul ESP32-CAM atau kamera pengawas dapat diterapkan agar sistem mampu mendokumentasikan dan mengirimkan gambar atau video saat terjadi percobaan akses ilegal maupun pembobolan.

Penggunaan sensor fingerprint yang digunakan pada penelitian ini masih memiliki keterbatasan dalam membaca sidik jari pada kondisi tertentu, seperti jari basah, kotor, atau berminyak. Penelitian selanjutnya diharapkan menggunakan sensor fingerprint dengan kualitas dan sensitivitas yang lebih tinggi. Pengembangan lainnya dapat dilakukan dengan menambahkan indikator kapasitas baterai sehingga kondisi daya cadangan dapat dipantau secara real-time. Selain itu, penelitian selanjutnya diharapkan dapat mengimplementasikan sistem pada lingkungan nyata seperti rumah, kantor, atau ruang penyimpanan barang berharga.

DAFTAR PUSTAKA

- Febriyanto, E., -, P., & Suprayogi, D. (2019). Prototype Sistem Smart Lock Door Dengan Timer Dan Fingerprint Sebagai Alat Autentikasi Berbasis Arduino Uno Pada Ruangan. *Jurnal Informatika*, 19(1), 10–19.
- Pangestu, N. P., Telkom, U., Tulloh, R., Telkom, U., Priyanto, W. B., Grapari, N. S., & Pendahuluan, I. (2023). Perancangan Bot Telegram Sebagai Platform Laporan Gangguan Jaringan Telkomsel Di Wilayah Purwokerto Design of Telegram Bot as a Platform For Reporting Telkomsel Network Trouble at Purwokerto Region. 9(3), 1110–1118.
- Putri, A. T., Salamah, I., & Rose, M. M. (2025). Implementasi Sistem Keamanan Brankas Berbasis Face Recognition Menggunakan Algoritma YOLO dengan Verifikasi Fingerprint. 7(2), 161–174.
- 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.
- Saputra, R. P. (2019). Perkembangan Tindak Pidana Pencurian Di Indonesia. *Jurnal Pahlawan*, 2(2), 1–8.
- Simanjuntak, I. U. V., Basuki, A. Y., & Ridlon, M. (2020). Rancang Bangun Sistem Pengamanan Pintu Rumah Tinggal Menggunakan E-KTP Dan Magnetic Door Lock Berbasis ATMEGA328. *Jurnal Ilmiah Teknologi Dan Rekayasa*, 25(2), 149–160.
- Suharsoyo, A. (2015). Karakter pelaku tindak pidana pencurian dalam tipologi kejahatan pencurian di wilayah sukoharjo. *Jurisprudence*, 5(1), 64–74.