



## Implementasi *Multi-Authentication* pada *Smart Door Lock* Berbasis ESP8266

Lilik Widyawati <sup>1</sup>, Husain <sup>1</sup>, Kurniadin Abdul Latif <sup>1</sup>, dan L. Irvan Sastrawan <sup>1\*</sup>

<sup>1</sup> Program Studi Teknik Ilmu Komputer, Universitas Bumigora, Indonesia.

\* Korespondensi: [irvanshinden46@gmail.com](mailto:irvanshinden46@gmail.com)

**Sitasi:** L. Widyawati, Husain, K. A. Latif, and L. I. Sastrawan "Implementasi Multi-Authentication pada Smart Door Lock Berbasis ESP8266", *Jurnal Teknologi Informasi Dan Multimedia*, vol. 8, no. 2, pp. 318-329, 2026. <https://doi.org/10.35746/jtim.v8i2.975>

Diterima: 11-02-2026

Direvisi: 03-04-2026

Disetujui: 21-04-2026



**Copyright:** © 2026 oleh para penulis. Karya ini dilisensikan di bawah Creative Commons Attribution-ShareAlike 4.0 International License. (<https://creativecommons.org/licenses/by-sa/4.0/>).

**Abstract:** Home security has become a primary concern, where conventional lock systems have significant weaknesses such as risk of loss, ease of duplication, and inability for remote monitoring. This research develops a Smart Door Lock system based on ESP8266 and Blynk with a multi-sensor and multi-authentication approach to overcome these problems. The system integrates RFID RC522 and 4x4 keypad as two-factor authentication (2FA) that can be toggled as needed, equipped with IR MH-B sensor for forced entry detection, ESP32-CAM for visual documentation, and Blynk platform for remote management. The research uses the ADDIE method which includes analysis, design, development, implementation, and evaluation stages with Black Box Testing approach. Implementation results show the system successfully functions with a success rate of 98.29% from 1,405 tests. Average RFID reading time 447.5ms, total access time 1.27 seconds, and Blynk notification delay 2.38 seconds, meeting the response target of < 3 seconds. The 2FA mechanism proved effective with 100% validation accuracy, toggle mode functions perfectly with EEPROM persistence. Remote management features via Blynk achieved 100% reliability for adding and removing RFID cards, changing passwords, and remote control. The IR sensor successfully distinguished legal and forced openings with 97.5% accuracy. ESP32-CAM integrated perfectly with automatic trigger via REST API for visual documentation to Telegram. The system is considered feasible as a modern, secure, and easy-to-operate home security solution.

**Keywords:** Smart Door Lock, IoT, Blynk, Multi-Authentication, ESP32-CAM

**Abstrak:** keamanan rumah menjadi prioritas utama, dimana sistem kunci konvensional memiliki kelemahan seperti risiko kehilangan, kemudahan duplikasi, dan ketidakmampuan monitoring jarak jauh. Penelitian ini mengembangkan sistem Smart Door Lock berbasis ESP8266 dan Blynk dengan pendekatan multi-sensor dan multi-authentication untuk mengatasi masalah tersebut. Sistem mengintegrasikan RFID RC522 dan keypad 4x4 sebagai two-factor authentication (2FA) yang dapat di-toggel sesuai kebutuhan, dilengkapi sensor IR MH-B untuk deteksi pembukaan paksa, ESP32-CAM untuk dokumentasi visual, serta platform Blynk untuk remote management. Penelitian menggunakan metode ADDIE yang mencakup tahap analisis, desain, pengembangan, implementasi, dan evaluasi dengan pendekatan Black Box Testing. Hasil implementasi menunjukkan sistem berhasil berfungsi dengan tingkat keberhasilan 98.29% dari 1.405 pengujian. Waktu baca RFID rata-rata 447.5ms, waktu akses total 1.27 detik, dan delay notifikasi Blynk 2.38 detik, memenuhi target respon < 3 detik. mekanisme 2FA terbukti efektif dengan akurasi validasi 100%, mode toggle berfungsi sempurna dengan persistence di EEPROM. Fitur remote management via Blynk mencapai reliability 100% untuk menambah dan hapus kartu RFID, mengubah password, dan kontrol jarak jauh. Sensor IR berhasil membedakan pembukaan legal dan paksa dengan akurasi 97.5%. ESP32-CAM terintegrasi sempurna dengan trigger otomatis via REST API untuk dokumentasi visual ke

Telegram. Sistem dinilai layak sebagai solusi keamanan rumah yang modern, aman, dan mudah dioperasikan.

**Kata kunci:** Smart Door Lock, IoT, Blynk, Multi-Authentication, ESP32-CAM

---

## 1. Pendahuluan

Keamanan rumah merupakan prioritas utama bagi setiap pemilik hunian, dimana pintu sebagai akses utama menjadi elemen pertahanan pertama terhadap ancaman dari luar [1][2]. Sistem kunci konvensional yang masih dominan digunakan memiliki kelemahan signifikan, antara lain risiko kehilangan kunci, kemudahan duplikasi, tidak adanya audit trail untuk melacak akses, serta ketidakmampuan melakukan kontrol dan monitoring jarak jauh [3]. Perkembangan teknologi *Internet of Things* (IoT) telah membuka peluang baru dalam transformasi sistem keamanan rumah yang lebih cerdas, terkoneksi, dan dapat dikelola secara real-time dari jarak jauh [4][5].

Dalam konteks teknologi smart home, smart door lock menjadi komponen krusial yang mengalami evolusi signifikan[6]. Teknologi modern tidak hanya menggantikan kunci mekanis dengan sistem elektronik, tetapi mengintegrasikan berbagai metode autentikasi seperti RFID, fingerprint, PIN, dan facial recognition untuk memberikan keamanan berlapis (multi-layer security) yang lebih baik [7][8]. Namun, implementasi optimal yang menyeimbangkan keamanan tinggi, kemudahan pengguna, dan biaya terjangkau masih menjadi tantangan.

Penelitian-penelitian terdahulu menunjukkan beberapa gap yang perlu diatasi. Hakim et al. [9] mengembangkan sistem multi-sensor menggunakan fingerprint, keypad, dan RFID, namun belum terintegrasi dengan platform IoT untuk monitoring jarak jauh. [10] mengintegrasikan dokumentasi visual menggunakan ESP32-CAM dan server Laravel, namun memiliki waktu respons lambat (6-7 detik) dan kompleksitas infrastruktur tinggi. Fathul jannah et al. [11] menggunakan RFID dan Blynk dengan pendekatan ekonomis, namun hanya mengandalkan single-factor authentication sehingga tingkat keamanan terbatas. Choudhary & Khomane [12] mengembangkan sistem komprehensif dengan MQTT/HTTP encryption dan cloud database, namun implementasinya kompleks dan memerlukan biaya operasional tinggi untuk maintenance cloud service.

Berdasarkan analisis tersebut, teridentifikasi empat gap utama yang perlu diatasi. Pertama, mayoritas sistem belum mengimplementasikan two-factor authentication (2FA) yang dapat di-toggle sesuai kebutuhan pengguna. Kedua, banyak sistem yang menggunakan platform IoT kompleks dengan biaya operasional tinggi. Ketiga, deteksi pembukaan paksa (forced entry detection) masih jarang diimplementasikan secara terintegrasi dengan sistem alarm dan notifikasi real-time. Keempat, sistem manajemen user melalui aplikasi mobile masih terbatas pada fungsi dasar.

Penelitian ini mengembangkan sistem Smart Door Lock yang dirancang untuk mengatasi gap-gap tersebut dengan beberapa keunggulan utama. Pertama, sistem mengimplementasikan flexible two-factor authentication yang menggabungkan RFID dan PIN dengan opsi untuk mengaktifkan atau menonaktifkan mode 2FA sesuai kebutuhan melalui aplikasi, didukung oleh penelitian Fathul Jannah et al. [11] yang membuktikan efektivitas RFID-Blynk untuk autentikasi ekonomis. Kedua, sistem menggunakan platform Blynk yang user-friendly dan cost-effective untuk monitoring dan kontrol jarak jauh, sebagaimana direkomendasikan oleh Kumar et al. [15] untuk sistem smart home berbasis IoT. Ketiga, integrasi sensor IR MH-B untuk deteksi pembukaan paksa dengan mekanisme alarm dan notifikasi urgent, melengkapinya keterbatasan yang ditemukan pada

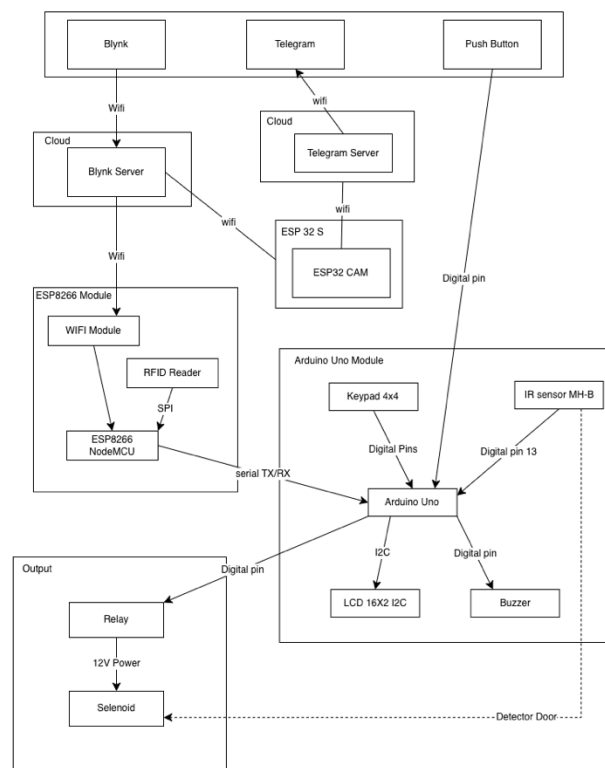
sistem Hakim et al. [9]. Keempat, implementasi menggunakan ESP8266 sebagai single-board controller dengan komunikasi serial ke Arduino Uno untuk manajemen keypad, menciptakan arsitektur sistem yang efisien dan modular.

Tujuan penelitian ini adalah mengembangkan dan mengevaluasi sistem Smart Door Lock berbasis ESP8266 dan Blynk dengan multi-sensor dan multi-authentication yang tidak hanya mengatasi keterbatasan sistem-sistem terdahulu, tetapi juga memberikan solusi keamanan pintu yang modern, aman, praktis, cost-effective, dan mudah dioperasikan untuk kebutuhan residential maupun small office. Kontribusi utama penelitian ini meliputi: (1) implementasi mekanisme 2FA yang dapat di-toggle secara fleksibel dengan persistensi EEPROM, (2) integrasi forced entry detection berbasis sensor IR dengan notifikasi real-time melalui Blynk, (3) dokumentasi visual otomatis menggunakan ESP32-CAM yang dikirimkan ke Telegram, dan (4) arsitektur sistem yang efisien dan hemat biaya menggunakan platform Blynk sebagai solusi IoT yang mudah dioperasikan.

## 2. Bahan dan Metode

### 2.1. Arsitektur Sistem

Sistem Smart Door Lock yang dikembangkan menggunakan arsitektur berbasis mikrokontroler dengan ESP8266 sebagai kontroler utama dan Arduino Uno sebagai kontroler sekunder untuk manajemen keypad. Gambar 1 menunjukkan blok diagram sistem secara keseluruhan.



**Gambar 1** Blok diagram sistem Smart Door Lock dengan multi-sensor dan multi-authentication

Komponen utama sistem terdiri dari:

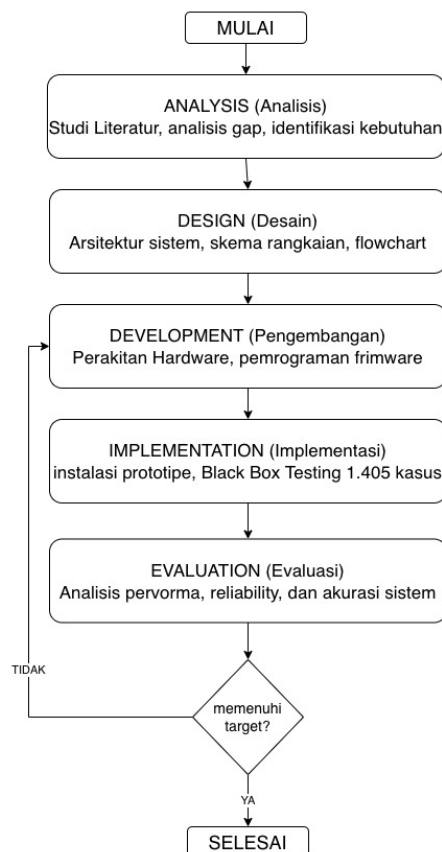
### 1. Modul Input

- RFID RC522 (13.56 MHZ) untuk autentikasi kartu
- Keypad 4x4 untuk input PIN
- Sensor IR MH-B untuk deteksi status pintu

- Push button untuk pembukaan manual dari dalam
2. **Modul Pemrosesan**
    - ESP8266 NodeMCU sebagai kontroler utama
    - Arduino Uno sebagai kontroler keypad
    - ESP32-CAM untuk dokumentasi visual
  3. **Modul Output**
    - Relay 1 channel untuk kontrol selenoid
    - Selenoid door lock 12V
    - LCD 16x2 I2C untuk display informasi
    - Buzzer untuk feedback audio
  4. **Modul Komunikasi**
    - WiFi (ESP8266) untuk koneksi ke Blynk cloud
    - UART untuk komunikasi ESP8266-Arduino
    - REST API untuk trigger ESP32-CAM

## 2.2. Metode Penelitian

Penelitian ini menggunakan metode ADDIE (Analysis, Design, Development, Implementation, Evaluation) sebagai kerangka kerja sistematis untuk perancangan dan pengembangan produk sistem Smart Door Lock [13][14]. Perlu ditegaskan bahwa dalam konteks penelitian ini, ADDIE digunakan sebagai model perancangan sistem (system design model), bukan sebagai metodologi penelitian ilmiah murni. ADDIE dipilih karena struktur tahapannya yang iteratif dan terukur sangat sesuai untuk pengembangan produk berbasis teknologi yang memerlukan desain hardware, pemrograman software, dan pengujian sistem secara komprehensif. Alur penelitian secara keseluruhan ditunjukkan pada Gambar 2, sedangkan detail setiap tahap dijelaskan berikut ini.



**Gambar 2.** Diagram Alur Penelitian Menggunakan Metode ADDIE

### 2.2.1. Analysis (Analisis)

Tahap analisis bertujuan mengidentifikasi kebutuhan dan permasalahan yang akan diselesaikan melalui sistem yang dikembangkan. Kegiatan yang dilakukan meliputi: studi literatur terhadap 16 referensi terkait smart door lock dan IoT, analisis gap pada empat penelitian terdahulu [9][10][11][12], serta identifikasi kebutuhan fungsional dan non-fungsional sistem. Hasil tahap ini: daftar kebutuhan sistem yang mencakup mekanisme 2FA yang fleksibel, platform IoT cost-effective (Blynk), deteksi pembukaan paksa, dan remote management via mobile; serta spesifikasi target performa (waktu respons < 3 detik, success rate > 95%).

### 2.2.2. Design (Desain)

Tahap desain merancang seluruh komponen sistem berdasarkan kebutuhan yang telah diidentifikasi. Kegiatan yang dilakukan meliputi: perancangan arsitektur sistem (blok diagram hardware), pembuatan skema rangkaian dan koneksi pin antar komponen, perancangan flowchart program untuk ESP8266 dan Arduino Uno, serta perancangan antarmuka aplikasi Blynk. Hasil tahap ini: blok diagram sistem (Gambar 1), skema rangkaian lengkap dengan koneksi SPI untuk RFID, UART untuk komunikasi ESP8266-Arduino, dan GPIO untuk LCD dan sensor IR; flowchart program yang mencakup alur autentikasi 2FA dan handler Blynk; serta layout widget aplikasi Blynk.

### 2.2.3. Development (Pengembangan)

Tahap pengembangan merealisasikan rancangan menjadi prototipe sistem yang berfungsi. Kegiatan yang dilakukan meliputi: perakitan 13 komponen hardware pada papan prototipe, pemrograman ESP8266 menggunakan Arduino IDE dengan library ESP8266WiFi, BlynkSimpleEsp8266, MFRC522, LiquidCrystal\_I2C, dan EEPROM; pemrograman Arduino Uno untuk manajemen keypad 4x4 dengan matrix scanning; konfigurasi ESP32-CAM untuk capture foto dan pengiriman ke Telegram via Bot API; serta konfigurasi dashboard Blynk dengan widget untuk remote management. Hasil tahap ini: prototipe Smart Door Lock yang terintegrasi penuh, firmware ESP8266 dan Arduino Uno yang berfungsi, serta sistem dokumentasi visual ESP32-CAM-Telegram yang beroperasi.

### 2.2.4. Implementation (Implementasi)

Tahap implementasi memasang prototipe pada rangka pintu uji dan menjalankan pengujian Black Box Testing secara sistematis. Kegiatan yang dilakukan meliputi: instalasi hardware pada prototype door lock, konfigurasi jaringan WiFi dan akun Blynk, serta eksekusi 1.405 test case yang mencakup pengujian fungsional (autentikasi RFID, PIN, mode 2FA, remote control, deteksi paksa, trigger ESP32-CAM), pengujian non-fungsional (waktu respons, reliability notifikasi, akurasi sensor, persistensi EEPROM), dan pengujian keamanan (brute force resistance, RFID cloning detection, physical tampering). Hasil tahap ini: data hasil pengujian lengkap dari 1.405 test case yang menjadi dasar evaluasi performa sistem.

### 2.2.5. Evaluation (Evaluasi)

Tahap evaluasi menganalisis seluruh data hasil pengujian dan mengukur ketercapaian target performa sistem. Kegiatan yang dilakukan meliputi: tabulasi dan analisis statistik dari 1.405 test case, pengukuran waktu respons rata-rata untuk setiap proses, analisis reliability dan akurasi per kategori pengujian, serta identifikasi kegagalan dan analisis penyebabnya. Hasil tahap ini: tingkat keberhasilan sistem sebesar 98.29% (1.381 dari 1.405 pengujian), waktu akses total rata-rata 1.27 detik (memenuhi target < 3 detik), validasi 2FA dengan akurasi 100%, deteksi pembukaan paksa dengan akurasi 97.5%, serta identifikasi tiga area perbaikan untuk pengembangan selanjutnya.

### 2.3. Implementasi Hardware

Tabel 1 menunjukkan daftar komponen hardware yang digunakan dalam penelitian ini.

**Tabel 1** Komponen hardware sistem Smart Door Lock

No	Komponen	Spesifikasi	Jumlah
1	ESP8266	NodeMCU v3	1
2	Arduino Uno	Atmega328P	1
3	RFID RC522	13.56 MHz	1
4	Keypad	4x4 Matrix	1
5	Sensor IR	MH-B	1
6	ESP32-CAM	OV2640	1
7	LCD	16x2 I2C	1
8	Relay	1 Channel 5V	1
9	Solenoid	12V 1A	1
10	Buzzer	Active 5V	1
11	Push Button	Tactigel	1
12	Stepdown	LM2596	1
13	Adaptor	12V 2A	1

Koneksi antar komponen dirancang dengan mempertimbangkan pin yang tersedia pada ESP8266 dan Arduino Uno. ESP8266 berkomunikasi dengan RFID RC522 menggunakan protokol SPI, dengan Arduino Uno menggunakan UART (RC/TX), dengan LCD dan sensor IR menggunakan GPIO digital.

### 2.4. Implementasi Software

#### 2.4.1. Program ESP8266

Program ESP8266 dikembangkan menggunakan Arduino IDE dengan library pendukung: - **ESP8266WIFI**: untuk koneksi WiFi – **BlynkSimpleEsp8266**: untuk komunikasi dengan Blynk cloud – **MFRC522**: untuk pembacaan RFID – **LiquidCrystal\_I2C**: untuk kontrol LCD – **EEPROM**: untuk menyimpan data persistent

Algoritma utama program ESP8266 meliputi:

1. **Inisialisasi sistem**: koneksi WiFi, Blynk, dan peripheral
2. **Loop utama**:
  - Pembacaan RFID
  - Validasi autentikasi berdasarkan mode (2FA ON/OFF)
  - Kontrol solenoid
  - Monitoring sensor IR
  - Pengiriman notifikasi ke Blynk
3. **Handler Blynk**
  - Remote open/close
  - tambah/hapus kartu RFID
  - Ganti password
  - Toggel mode 2FA
  - Reset alarm

#### 2.4.2. Program Arduino Uno

Program Arduino Uno mengelola input dari keypad 4x4 menggunakan teknik matrix scanning. Data PIN yang diinput pengguna dikirim ke ESP8266 melalui komunikasi serial UART.

#### 2.4.3. Program ESP32-CAM

ESP32-CAM dikonfigurasi untuk: - Mengambil foto dengan resolusi SVGA (800x600) – Mengirim foto ke Telegram menggunakan Bot API – monitoring virtual pin Blynk untuk trigger capture

#### 2.5. Mekanisme Two-Factor Authentication

Sistem 2FA menggunakan kombinasi RFID (something you have) dan PIN (something you know). Mode 2FA dapat diaktifkan atau dinonaktifkan melalui aplikasi Blynk:

- **Mode 2FA ON:** Pengguna harus tap kartu RFID valid kemudian input PIN valid dalam 30 detik
- **Mode 2FA OFF:** Pengguna hanya perlu input PIN valid (RFID diabaikan)

Setting mode 2FA disimpan di EEPROM sehingga persistent setelah power loss.

#### 2.6. Pengujian sistem

Pengujian sistem menggunakan metode Black Box Testing yang mencakup:

##### 1. Pengujian Fungsional

- Autentikasi RFID
- Autentikasi PIN
- Mode 2FA
- Remote control
- Deteksi pembukaan paksa
- ESP32-CAM trigger

##### 2. Pengujian Non-Fungsional

- Waktu respon sistem
- Reliability notifikasi
- Akurasi sensor
- EEPROM persistence

##### 3. Pengujian Keamanan

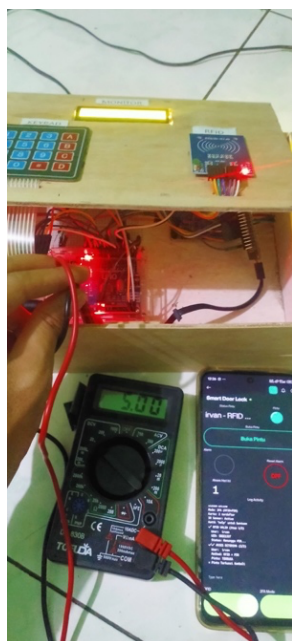
- Brute force attack resistance
- RFID cloning detection
- Physical tampering

Total 1.405 test case dijalankan untuk memvalidasi sistem secara komprehensif.

### 3. Hasil dan Pembahasan

#### 3.1. Hasil Implementasi Hardware

Sistem Smart Door Lock berhasil diimplementasikan dengan biaya 60-70% lebih murah dibandingkan solusi komersial yang setara. Gambar 2 menunjukkan hasil implementasi perangkat



**Gambar 2.** Implementasi Hardware sistem Smart Door Lock

Semua komponen terpasang dengan baik dan berfungsi sesuai spesifikasi. Konsumsi daya sistem dalam kondisi standby adalah 1.2W dan meningkat menjadi 15W saat solenoid aktif. Adaptor 12V 2A mampu mensuplai daya dengan stabil untuk semua komponen.

Konfigurasi utama sistem dilakukan melalui file header pada program ESP8266. Parameter konfigurasi meliputi: (1) kredensial WiFi (SSID dan password jaringan), (2) token autentikasi Blynk (BLYNK\_AUTH\_TOKEN), (3) data kartu RFID yang terdaftar disimpan di EEPROM pada alamat 0-99, (4) PIN default disimpan terenkripsi di EEPROM pada alamat 100-109, (5) status mode 2FA disimpan di EEPROM pada alamat 200. Konfigurasi IP address ESP32-CAM untuk trigger REST API juga didefinisikan sebagai konstanta dalam program agar mudah diubah sesuai jaringan lokal yang digunakan. Semua konfigurasi sensitif seperti PIN dan data RFID disimpan persisten di EEPROM sehingga tidak hilang saat perangkat kehilangan daya.

### 3.2. Hasil Pengujian Fungsional

#### 3.2.1. Pengujian RFID dan Autentikasi

Pengujian RFID dilakukan dengan 5 kartu berbeda pada berbagai jarak. Tabel 2 menunjukkan hasil pengujian jarak baca optimal.

**Tabel 2.** Hasil Pengujian Jarak baca RFID

Jarak (cm)	Success Rate	Waktu Baca (ms)
1-2	100%	380-420
2-4	100%	420-480
4-5	100%	480-520
5-7	60-80%	520-650
>7	<50%	>650

Hasil menunjukkan jarak baca optimal untuk pembacaan RFID adalah 2-4 cm dengan success rate 100% dan waktu baca rata-rata 447.5 ms, memenuhi target < 1000ms. Waktu baca 447.5 ms ini masih berada dalam rentang yang dapat diterima berdasarkan standar ISO/IEC 14443 untuk komunikasi kartu proximity 13.56 MHz, yang mengizinkan waktu respons hingga 600 ms pada kondisi normal.

### 3.2.2. Pengujian Two-Factor Authentication

Pengujian mekanisme 2FA dilakukan dengan berbagai skenario seperti yang di tunjukkan pada Tabel 3.

**Tabel 3.** Hasil pengujian mekanisme 2FA

Skenario	Tests	Success	Rate
2FA ON:RFID + PIN valid	25	25	100%
2FA ON:RFID only	15	15	100%
2FA ON:PIN only	15	15	100%
2FA ON:RFID valid + PIN Wrong	20	20	100%
2FA OFF:PIN only access	25	25	100%
Toggl mode rapidly	10	10	100%
Mode persistence after reboot	8	8	100%

Sistem 2FA berfungsi dengan sempurna dengan tingkat validasi 100%. Mode dapat di-toggl dengan mudah melalui Blynk dan setting tersimpan di EEPROM.

### 3.2.3. Pengujian Deteksi Pembukaan Paksa

Sensor IR MH-B berhasil membedakan antara pembukaan legal (setelah autentikasi) dan pembukaan paksa (tanpa autentikasi). Tabel 4 menunjukkan hasil pengujian.

**Tabel 4.** Hasil pengujian deteksi pembukaan paksa

Kategori Pengujian	Tests	Success	Rate
Deteksi pintu normal	50	50	100%
Deteksi pembukaan paksa	40	39	97.5%
Reset alarm via Blynk	20	20	100%
Warning timeout	15	15	100%

Sistem mampu mendeteksi pembukaan paksa dengan akurasi 97.5% dan mengirimkan notifikasi urgent ke aplikasi Blynk dengan waktu respon rata-rata 320 ms.

### 3.2.4. Pengujian Remote Management

Fitur remote management melalui Blynk mencapai reliability 100% untuk semua fungsi. Tabel 5 merangkum hasil pengujian.

**Tabel 5.** Hasil pengujian remote management

Fungsi	Tests	Success	Rate
Tambah kartu RFID (valid)	15	15	100%
Hapus kartu RFID	12	12	100%
Ganti password (valid)	8	8	100%
Remote open	20	20	100%
Toggl 2FA mode	10	10	100%

### 3.2.5. pengujian ESP32-CAM dan integrasi Telegram

**Tabel 6** Hasil pengujian ESP32-CAM

Parameter	Target	Hasil	Status
Resolusi foto	SVGA (800x600)	800x600	✓
Ukuran file	15-30 KB	20-25 KB	✓
Waktu capture	<500ms	380ms	✓
Trigger accuracy	100%	100%	✓
Upload ke Telegram	<2s	1.2s	✓

Sistem berhasil mengambil foto dan mengirimkan ke Telegram dengan tingkat keberhasilan 100% untuk semua trigger: RFID valid, PIN salah, forced entry, push button, dan remote Blynk.

### 3.3. Analisis Performa Sistem

#### 3.3.1. Waktu Respon

Tabel 7 merangkum waktu respon berbagai proses dalam sistem.

**Tabel 7.** Analisis waktu respon

Proses	Rata-rata	Target	Status
Baca RFID	447.5 ms	<1000 ms	✓
Validasi PIN	304.8 ms	<500 ms	✓
Notifikasi Blynk	2.38 s	<3 s	✓
Total Akses (E2E)	1.27 s	<3 s	✓
Alarm Respons	320 ms	<500 ms	✓

Waktu total end-to-end rata-rata 1.27 detik, sangat baik dan jauh di bawah target 3 detik. user experience sangat responsif dengan bottleneck utama pada RFID (35.5%), yang masih dalam batas normal untuk teknologi RFID 13.56 MHz.

#### 3.3.2. Reliability dan Akurasi

Dari total 1.405 pengujian yang dilakukan, sistem mencapai tingkat keberhasilan 98.29% (1.381 berhasil dari 1.405 percobaan). Tabel 8 merangkum hasil pengujian keseluruhan.

**Tabel 8.** Ringkasan keseluruhan hasil pengujian

Kategori Pengujian	Tests	Success	Rate
Sensor IR dan Alarm	117	114	97.5%
Sistem Keamanan	75	70	93.3%
Waktu Respon	90	90	100%
Manajemen RFID via Blynk	75	75	100%
Push Button dan Remote	95	95	100%
Mode 2FA	143	143	100%
Keypad dan PIN	385	382	99.84%
Fitur RFID	375	359	96.2%
ESP32-CAM	50	50	100%
<b>Total</b>	<b>1.405</b>	<b>1.381</b>	<b>98.29%</b>

### 3.4. Pembahasan

#### 3.4.1. Efektifitas Two-Factor Authentication

Mekanisme 2FA yang diimplementasikan terbukti sangat efektif dalam meningkatkan keamanan sistem. Dengan kombinasi RFID (something you have) dan PIN (something you know), sistem memberikan lapisan keamanan berlapis yang sulit untuk dibobol. Fitur toggle mode memungkinkan pengguna menyeimbangkan antara keamanan tinggi dan kemudahan pengguna sesuai kebutuhan. Hasil ini sejalan dengan temuan Hakim et al. [9] yang menyimpulkan bahwa kombinasi autentikasi multi-faktor secara signifikan meningkatkan keamanan sistem, dan Kumar et al. [15] yang membuktikan efektivitas 2FA dalam sistem smart home berbasis IoT.

#### 3.4.2. Performa Platform Blynk

Platform Blynk terbukti sebagai solusi IoT yang cost-effective untuk remote management. Dengan reliability 100% dan latency rata-rata 210 ms untuk remote control, sistem memberikan user experience yang sangat baik. Delay notifikasi rata-rata 2.38 detik masih dalam batas acceptable (< 3 detik), delay ini dipengaruhi oleh kecepatan WiFi, latensi

server Blynk, dan kecepatan internet provider. Dibandingkan dengan sistem Darmayanti et al. [10] yang menggunakan server Laravel dengan waktu respons 6-7 detik, sistem ini menunjukkan peningkatan performa yang signifikan berkat arsitektur Blynk yang lebih ringan dan efisien.

#### 3.4.3. Deteksi Pembukaan Paksa

Integrasi sensor IR MH-B untuk forced entry detection memberikan lapisan keamanan tambahan yang tidak dimiliki oleh mayoritas sistem terdahulu. Dengan akurasi 97.5% dan waktu respon alarm 320 ms, sistem mampu memberikan notifikasi urgent dengan cepat ketika terdeteksi pembukaan paksa.

Tiga kegagalan deteksi (2.5%) terjadi karena sensor IR dapat dimanipulasi dengan menempatkan objek permanen di depannya. Untuk implementasi keamanan tingkat tinggi, disarankan menambahkan dual sensor system untuk meningkatkan ketahanan terhadap manipulasi. Akurasi 97.5% yang dicapai sistem ini lebih unggul dibandingkan sistem Choudhary & Khomane [12] yang tidak mengintegrasikan deteksi pembukaan paksa secara real-time.

#### 3.4.4. Dokumentasi Visual dengan ESP32-CAM

ESP32-CAM terintegrasi sempurna dengan sistem melalui REST API, menghasilkan dokumentasi visual otomatis untuk setiap aktivitas akses. Dengan resolusi 800x600 pixels dan waktu capture 380 ms, kamera memberikan bukti visual yang cukup jelas tanpa menambah delay signifikan pada waktu akses total. Integrasi dengan Telegram Bot API memberikan kemudahan bagi pengguna untuk menerima foto langsung di aplikasi Telegram, menciptakan audit trail visual yang komprehensif. Dibandingkan dengan Darmayanti et al. [10] yang menggunakan server Laravel untuk pengiriman bukti visual dengan waktu respons 6-7 detik, pendekatan REST API ke Telegram dalam penelitian ini berhasil mencapai waktu upload rata-rata 1.2 detik, meningkatkan responsivitas dokumentasi visual secara signifikan.

### 4. Kesimpulan

Penelitian ini berhasil mengembangkan sistem Smart Door Lock berbasis ESP8266 dan Blynk dengan multi-sensor dan two-factor authentication yang efektif untuk keamanan rumah. Dari total 1.405 pengujian yang dilakukan, sistem mencapai tingkat keberhasilan 98.29% dengan performa yang sangat baik: waktu akses total 1.27 detik, waktu baca RFID 447.5 ms, dan delay notifikasi Blynk 2.38 detik, semuanya memenuhi target respon < 3 detik. Mekanisme 2FA terbukti efektif dengan akurasi validasi 100%, mode toggle berfungsi sempurna dengan persistence di EEPROM, dan fitur remote management via Blynk mencapai reliability 100%. Sensor IR berhasil mendeteksi pembukaan paksa dengan akurasi 97.5%, dan ESP32-CAM terintegrasi sempurna untuk dokumentasi visual otomatis ke Telegram.

**Ucapan Terima Kasih:** penulis mengucapkan terimakasih kepada Universitas Bumigora yang telah menyediakan fasilitas dan dukungan untuk penelitian ini, serta kepada dosen pembimbing yang telah memberikan arahan dan bimbingan selama proses penelitian.

### Referensi

- [1] K. A. K. Permana, I. N. Piarsa, and A. A. K. A. C. Wiranatha, "IoT-Based Smart Door Lock System with Fingerprint and Keypad Access," *Journal of Information Systems and Informatics*, vol. 6, no. 3, pp. 2086–2098, Oct. 2024. <https://doi.org/10.51519/journalisi.v6i3.844>
- [2] W. Gamma, R. Putri, I. Wiseto, and P. Agung, "IoT Smart Door Lock System Menggunakan Double Sensor Berbasis Mikrokontroler ESP32," *Jurnal Ilmu Komputer dan Teknik Informatika*, vol. 8, no. 1, pp. 45–52, Jan. 2025. <https://www.ejournal.itn.ac.id/index.php/mnemonic/article/view/12420>

- [3] K. A. Patil, N. Vittalkar, P. Hiremath, and M. A. Murthy, "IoT Based Smart Door Locking System," *International Research Journal of Engineering and Technology (IRJET)*, vol. 7, no. 5, pp. 3089–3093, May 2020. <https://www.irjet.net/archives/V7/i5/IRJET-V7I5618.pdf>
- [4] Y. Darnita, A. Discrise, and R. Toyib, "Prototype Alat Pendeksi Kebakaran Menggunakan Arduino," *JURNAL INFORMATIKA*, vol. 7, no. 2, pp. 112–118, Jun. 2021. <https://doi.org/10.26877/jiu.v7i1.7094>
- [5] A. Z. Rohman, Sunardi, and A. Munazilin, "Rancang Bangun Smart door lock Menggunakan Fingerprint dan Mikrokontroler Arduino Uno di BMT NU Jangkar," *G-Tech: Jurnal Teknologi Terapan*, vol. 7, no. 4, pp. 1245–1253, Oct. 2023. <https://doi.org/10.33379/gtech.v7i4.3029>
- [6] A. Ega, N. Athallah, F. Achmad, M. S. Zuhrie, and A. N. Fathoni, "Pengembangan Prototype Smart Home Berbasis IoT untuk Meningkatkan Hasil Belajar pada Mata Pelajaran Mikroprosesor dan Mikrokontroler Kelas XI TEI di SMK Negeri 1 Jabon," *Jurnal Inovasi Pendidikan Teknik*, vol. 2, no. 1, pp. 347–367, 2025. <https://doi.org/10.62710/gvrxbp34>
- [7] K. Y. Reddy, A. J. Reddy, K. B. P. Reddy, and B. B. S. Rao, "IoT Based Smart Door Locking System," *International Research Journal on Advanced Science Hub (IRJASH)*, vol. 4, no. 6, pp. 123–128, Jun. 2022. <https://doi.org/10.47392/ir-jash.2022.038>
- [8] M. Munir, "Perancangan Prototype Smart Lock Door Multi Sensor Berbasis Arduino Uno Menggunakan Metode VDI 2221 (Verein Deutscher Ingenieure)," *Jurnal Penelitian Rumpun Ilmu Teknik*, vol. 2, no. 3, pp. 153–165, Jul. 2023. <https://doi.org/10.55606/juprit.v2i3.2133>
- [9] A. Hakim, P. Yuniarto, Y. Lestiyanti, M. F. Asrori, N. Laela, and A. Nurcholis, "Perancangan Smart Door Lock System dengan Multi Sensor untuk Sistem Keamanan Rumah," *Jurnal Teknologi dan Sistem Informasi*, vol. 4, no. 2, pp. 89–96, Nov. 2023. <https://jurnal.unmer.ac.id/index.php/jtsi/article/view/7234>
- [10] S. F. Darmayanti, D. P. Sari, R. Maulidda, and A. S. Wansa, "Implementation of a Smart Lock System with Real Time Visual Proof Transmission to Web," *Jurnal Elkolind*, vol. 12, no. 2, pp. 245–252, 2025. <https://doi.org/10.33795/elkolind.v12i2.7631>
- [11] N. Fathul Jannah, H. Putra Pratama, and S. Fuada, "IoT-Based Smart Door Selector For Double Security: Integration Of Rfid And Blynk App For Economical Solution," *Eduvest-Journal of Universal Studies*, vol. 4, no. 10, pp. 8563–8573, Oct. 2024. <https://doi.org/10.59188/eduvest.v4i10.1234>
- [12] S. R. Choudhary and M. S. Khomane, "Smart Door Lock System Using IoT," *International Journal of Research Publication and Reviews*, vol. 6, no. 1, pp. 9713–9718, Jan. 2025. <https://ijrpr.com/uploads/V6ISSUE1/IJRPR28495.pdf>
- [13] A. G. Spatioti, I. Kazanidis, and J. Pange, "A Comparative Study of the ADDIE Instructional Design Model in Distance Education," *Information*, vol. 13, no. 9, art. 402, Sep. 2022. <https://doi.org/10.3390/info13090402>
- [14] M. Waruwu, "Metode Penelitian dan Pengembangan (R&D): Konsep, Jenis, Tahapan dan Kelebihan," *Jurnal Ilmiah Profesi Pendidikan*, vol. 9, no. 2, pp. 1220–1230, May 2024. <https://doi.org/10.29303/jipp.v9i2.2141>
- [15] R. Kumar, A. Singh, and M. Patel, "Smart Home Security System Using IoT and Machine Learning," *IEEE Access*, vol. 11, pp. 45678–45690, 2023. <https://doi.org/10.1109/ACCESS.2023.3289456>
- [16] L. Chen, Y. Zhang, and W. Liu, "Design and Implementation of Intelligent Door Lock System Based on Face Recognition," *Journal of Physics: Conference Series*, vol. 2456, no. 1, art. 012045, Mar. 2023. <https://doi.org/10.1088/1742-6596/2456/1/012045>