Jicom : Journal Information & Computer
Volume 4, Nomor 2, Juli 2026, hlm.110-117
DOI : 10.32493/jicomisc.v2i1.37666

P-ISSN : 3031-2779
E-ISSN : 3026-4197

Implementasi Sistem Kunci Pintar 2FA Berbasis IoT Menggunakan RFID dan Bot Telegram pada ESP32

Syahrul Rozikin*[1], Muhammad Gald Teary[2], Fery Antony[3]
1,2,3,) Sistem Komputer, Fakultas Ilmu Komputer dan Sains, Universitas Indo Global Mandiri
Email: *[1]syahrulrozikin2704@gmail.com, [2]m.gald@uigm.ac.id, [3]feryantony@uigm.ac.id

(Naskah masuk: 7 Juni 2026, diterima untuk diterbitkan: 31 Juli 2026)

Abstrak: *Penelitian ini merancang dan mengimplementasikan prototipe sistem kunci pintar tanpa kunci (smart keyless) dengan autentikasi dua faktor berbasis Internet of Things (IoT) menggunakan ESP32, RFID RC522, bot Telegram, relay, dan solenoid lock 12V. Sistem membatasi akses fisik melalui dua tahap autentikasi, yaitu validasi UID kartu RFID dan OTP yang dikirim melalui bot Telegram. Pengujian dilakukan pada tiga skenario, yaitu RFID terdaftar dengan OTP valid, RFID terdaftar dengan OTP tidak valid, dan RFID tidak terdaftar. Hasil pengujian menunjukkan bahwa sistem bekerja sesuai rancangan dengan tingkat keberhasilan 100% dari 10 percobaan pada setiap skenario dalam kondisi pengujian prototipe terbatas. Waktu respons rata-rata aktivasi solenoid lock setelah autentikasi valid adalah 0,26 detik. Prototipe mampu menjalankan fungsi autentikasi dua tahap sesuai skenario uji, tetapi pengujian keamanan lanjutan masih diperlukan sebelum diterapkan pada lingkungan nyata.*
Kata Kunci *- kunci pintar; autentikasi dua faktor; RFID; bot Telegram; ESP32*

Abstract: *This study designs and implements a smart keyless prototype with two-factor authentication based on the Internet of Things (IoT) using ESP32, RFID RC522, Telegram bot, relay, and a 12V solenoid lock. The system restricts physical access through two authentication stages: validating the RFID card UID and verifying a one-time password (OTP) sent through the Telegram bot. Testing was conducted in three scenarios: registered RFID with valid OTP, registered RFID with invalid OTP, and unregistered RFID. The results show that the system worked according to the design, achieving 100% success in 10 trials for each scenario under limited prototype testing conditions. The average solenoid activation response time after valid authentication was 0.26 seconds. The prototype can perform basic two-factor authentication according to the tested scenarios, although further security testing is required before deployment in real operational environments.*
Keywords *- smart keyless; two-factor authentication; RFID; Telegram bot; ESP32*

1. PENDAHULUAN

Perkembangan Internet of Things (IoT) mendorong pemanfaatan perangkat tertanam untuk membangun sistem akses fisik yang dapat dikendalikan dan dipantau secara digital. Pada sistem pengamanan pintu, konsep kunci pintar tanpa kunci atau smart keyless memungkinkan proses pembukaan kunci dilakukan tanpa kunci mekanis konvensional, melainkan melalui media autentikasi elektronik seperti kartu RFID, perangkat bergerak, atau kode verifikasi sekali pakai. Namun, penggunaan RFID pada sistem akses tetap perlu memperhatikan aspek keamanan karena teknologi RFID masih memiliki risiko seperti penyalahgunaan kartu, pelacakan, replay attack, dan autentikasi yang lemah apabila hanya menggunakan satu faktor pengenal [1], [2].

Autentikasi merupakan aspek penting dalam sistem IoT karena perangkat yang terhubung ke jaringan dapat berinteraksi dengan pengguna, layanan komunikasi, dan aktuator fisik. Pada sistem akses berbasis RFID, kartu digunakan sebagai faktor kepemilikan untuk mengenali pengguna yang memiliki hak akses. Meskipun demikian, penggunaan RFID sebagai satu-satunya faktor autentikasi masih memiliki keterbatasan, misalnya ketika kartu hilang, dipinjamkan, atau digunakan oleh pihak yang tidak berwenang. Oleh karena itu, two-factor authentication (2FA) dapat digunakan sebagai lapisan tambahan dengan menggabungkan faktor kepemilikan berupa kartu RFID dan faktor verifikasi tambahan berupa kode OTP yang dikirim secara dinamis [3], [4].

Beberapa penelitian sebelumnya telah membahas sistem keamanan pintu berbasis RFID dan IoT. [5] merancang sistem keamanan ruang server berbasis RFID dan IoT untuk membatasi akses pada ruang server. [6] mengembangkan RFID smart door lock system berbasis IoT untuk manajemen membership fitness center. [7] mengembangkan smart home IoT dengan integrasi kunci RFID dan otomasi elektronik. [8] merancang sistem keamanan pintu berbasis RFID dan IoT, sedangkan [9] mengembangkan sistem keamanan pintu otomatis berbasis IoT dengan RFID, aplikasi mobile, dan metode Fuzzy Mamdani.

Penelitian lain mulai mengarah pada sistem autentikasi berlapis. [10] mengembangkan sistem keamanan loker dua lapis menggunakan RFID e-KTP dan OTP melalui platform Blynk. [11] membahas simulasi sistem keamanan dan kendali

gerbang otomatis berbasis IoT dengan teknologi tanpa kunci. [12] mengembangkan smart lock system berbasis IoT menggunakan ESP32 untuk keamanan akses pusat data. Selain itu, [13] menunjukkan penerapan mikrokontroler NodeMCU ESP8266 dan platform IoT ThingSpeak untuk pemantauan ruang server berbasis WiFi. Berdasarkan penelitian-penelitian tersebut, sistem akses berbasis RFID dan IoT telah banyak dikembangkan, tetapi masih terdapat ruang kajian pada penerapan autentikasi dua tahap yang menggabungkan UID RFID dan OTP melalui bot Telegram pada prototipe berbasis ESP32.

Research gap dalam penelitian ini terletak pada perlunya rancangan dan pengujian fungsional sistem smart keyless yang tidak hanya menunjukkan kondisi ketika akses diberikan, tetapi juga menjelaskan kondisi ketika akses harus ditolak, seperti kartu RFID tidak terdaftar, OTP salah, atau OTP tidak sesuai dengan proses autentikasi. Dengan demikian, penelitian ini tidak hanya berfokus pada keberhasilan membuka kunci, tetapi juga pada validasi logika autentikasi dua faktor dalam lingkup prototipe.

Tujuan penelitian ini adalah merancang, mengimplementasikan, dan menguji fungsi dasar sistem smart keyless 2FA berbasis RFID dan bot Telegram pada ESP32. Pengujian difokuskan pada validasi skenario akses, meliputi kartu RFID terdaftar dengan OTP valid, kartu RFID terdaftar dengan OTP tidak valid, serta kartu RFID tidak terdaftar. Fokus pengujian tersebut digunakan untuk memastikan bahwa sistem memberikan respons sesuai dengan kondisi autentikasi yang dirancang.

Kontribusi penelitian ini meliputi penyusunan arsitektur sistem smart keyless berbasis ESP32, perumusan alur autentikasi dua tahap menggunakan UID RFID dan OTP Telegram, implementasi pengendalian relay dan solenoid lock berdasarkan hasil autentikasi, serta pengujian fungsional terhadap beberapa skenario akses. Kontribusi tersebut diarahkan sebagai pembanding bagi penelitian sistem akses fisik berbasis IoT yang menerapkan autentikasi berlapis pada perangkat berbiaya relatif rendah.

Manfaat penelitian ini adalah memberikan referensi rancangan prototipe sistem akses fisik berbasis IoT yang menerapkan autentikasi dua tahap menggunakan RFID dan OTP Telegram. Secara praktis, hasil penelitian ini dapat digunakan sebagai dasar pengembangan sistem smart keyless sederhana untuk lingkungan terbatas, seperti laboratorium, ruang kerja, ruang penyimpanan, atau area dengan kebutuhan akses terbatas. Secara akademik, penelitian ini dapat menjadi bahan pembanding bagi penelitian berikutnya yang membahas integrasi RFID, ESP32, bot Telegram, dan mekanisme OTP pada sistem keamanan akses. Namun, manfaat tersebut tetap berada dalam ruang lingkup prototipe dan pengujian fungsional, sehingga belum dapat digeneralisasi sebagai sistem keamanan final tanpa pengujian lebih lanjut terhadap aspek jaringan, ketahanan perangkat, keamanan token, risiko penyalahgunaan kartu, dan skenario serangan lainnya.

2. METODE PENELITIAN

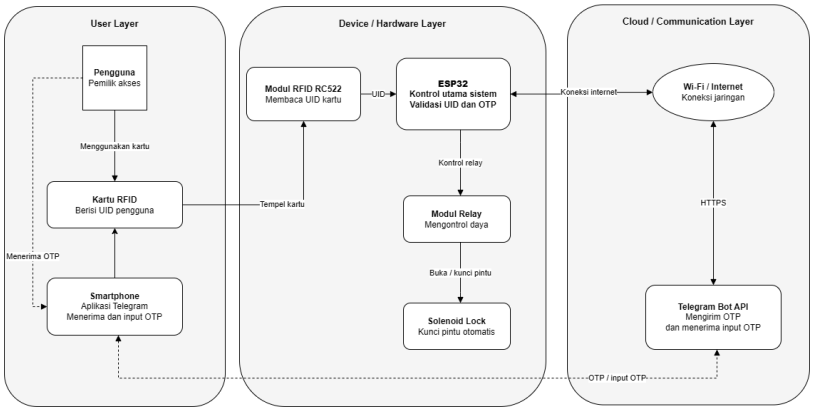
Penelitian ini menggunakan metode eksperimen berbasis prototipe untuk merancang dan menguji sistem smart keyless dengan autentikasi dua faktor berbasis Internet of Things (IoT). Sistem dikembangkan menggunakan ESP32 sebagai pengendali utama, RFID RC522 sebagai media autentikasi tahap pertama, Telegram Bot sebagai media pengiriman dan validasi One-Time Password (OTP), relay sebagai pengendali aktuator, serta solenoid lock 12V sebagai mekanisme penguncian.

Pengujian difokuskan pada fungsi autentikasi sistem berdasarkan kombinasi UID RFID dan OTP. Oleh karena itu, penelitian ini tidak bertujuan untuk menyatakan bahwa sistem telah sepenuhnya aman terhadap seluruh bentuk serangan, melainkan untuk menguji apakah sistem dapat memberikan respons sesuai dengan alur autentikasi yang dirancang.

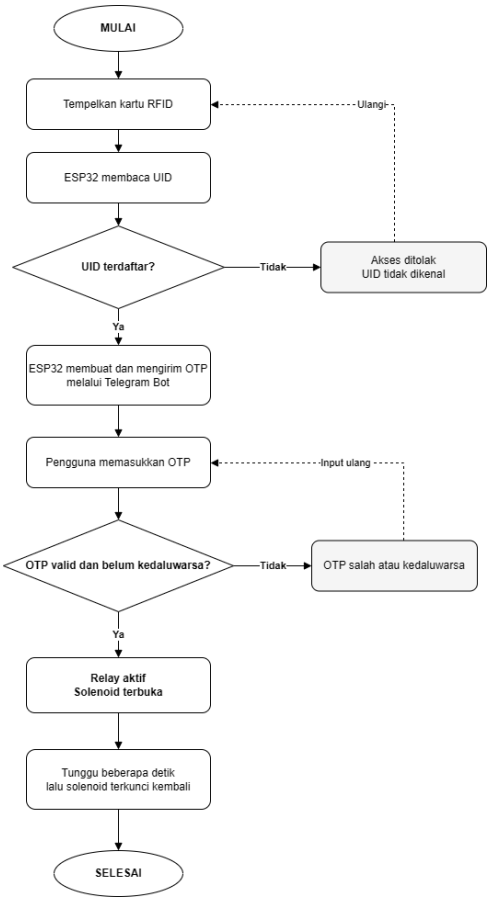
2.1. Desain Sistem

Sistem dirancang dengan alur autentikasi dua tahap. Tahap pertama dilakukan melalui pembacaan UID kartu RFID menggunakan modul RFID RC522. UID yang terbaca kemudian diproses oleh ESP32 dan dibandingkan dengan daftar UID yang telah didaftarkan. Apabila UID tidak terdaftar, proses autentikasi dihentikan dan solenoid lock tetap berada dalam kondisi terkunci.

Apabila UID terdaftar, sistem melanjutkan proses ke tahap kedua, yaitu pengiriman dan validasi OTP melalui Telegram Bot. Sistem menghasilkan OTP dengan masa berlaku tertentu, kemudian mengirimkan kode tersebut kepada pengguna melalui Telegram. Pengguna memasukkan OTP melalui bot, lalu sistem membandingkan OTP yang diterima dengan OTP yang telah dihasilkan. Jika OTP sesuai dan masih berada dalam batas waktu berlaku, ESP32 mengaktifkan relay untuk membuka solenoid lock selama durasi yang telah ditentukan. Jika OTP tidak sesuai atau melewati batas waktu berlaku, relay tidak diaktifkan dan solenoid lock tetap terkunci.



Gambar 1. Arsitektur Sistem Smart Keyless 2FA Berbasis ESP32, RFID, dan Telegram Bot



Gambar 2. Diagram Alur Autentikasi RFID dan OTP Telegram

2.2. Perangkat dan Bahan Penelitian

Perangkat keras yang digunakan dalam penelitian ini meliputi ESP32, modul RFID RC522, kartu RFID, relay module, solenoid lock 12V, catu daya eksternal, dan kabel penghubung. ESP32 digunakan sebagai pusat kendali sistem karena memiliki konektivitas WiFi yang diperlukan untuk komunikasi dengan Telegram Bot. Modul RFID RC522 digunakan untuk membaca UID kartu RFID, sedangkan relay digunakan sebagai sakelar elektronik untuk mengendalikan solenoid lock.

Solenoid lock tidak dihubungkan langsung ke ESP32 karena membutuhkan tegangan dan arus yang lebih besar dibandingkan keluaran pin mikrokontroler. Oleh karena itu, solenoid lock dikendalikan melalui relay dan catu daya eksternal 12V. Rancangan ini bertujuan agar ESP32 hanya berfungsi sebagai pengendali sinyal, sedangkan beban aktuator ditangani oleh rangkaian daya terpisah.

Perangkat lunak yang digunakan meliputi program pada ESP32 dan bot Telegram. Program ESP32 digunakan untuk membaca UID kartu, memvalidasi UID, menghasilkan OTP, mengatur komunikasi dengan bot Telegram, memvalidasi OTP yang dimasukkan pengguna, serta mengendalikan relay. Bot Telegram dibuat melalui BotFather dan digunakan sebagai media komunikasi antara sistem dan pengguna dengan memanfaatkan Telegram Bot API [14].

2.3. Implementasi Sistem

Implementasi perangkat keras dilakukan dengan menghubungkan RFID RC522 ke ESP32 menggunakan komunikasi SPI. Relay dihubungkan ke salah satu pin digital ESP32 untuk mengatur kondisi aktif dan tidak aktif pada solenoid lock. Solenoid lock dikendalikan melalui relay dengan sumber daya eksternal 12V.

Pada sisi perangkat lunak, sistem diprogram untuk menjalankan autentikasi secara berurutan. Proses dimulai dari pembacaan UID kartu RFID. Jika UID sesuai dengan daftar kartu yang terdaftar, sistem membuat OTP dan mengirimkannya melalui Telegram Bot. Setelah pengguna mengirimkan OTP kembali melalui Telegram, sistem melakukan validasi terhadap kode tersebut. Relay hanya diaktifkan apabila UID RFID dan OTP memenuhi kondisi yang telah ditentukan.

Penggunaan OTP dibatasi oleh waktu berlaku tertentu agar kode tidak digunakan di luar sesi autentikasi. Namun, pengujian terhadap penyalahgunaan OTP, seperti penggunaan ulang OTP atau percobaan brute force, hanya dapat disimpulkan apabila skenario tersebut benar-benar diuji dalam penelitian.

2.4. Skenario Pengujian

Pengujian dilakukan untuk mengetahui kesesuaian respons sistem terhadap beberapa kondisi autentikasi. Skenario utama yang digunakan dalam penelitian ini adalah sebagai berikut.

1. Kartu RFID terdaftar dan OTP valid.
2. Kartu RFID terdaftar dan OTP tidak valid.
3. Kartu RFID tidak terdaftar.

Pada skenario pertama, sistem diharapkan membuka solenoid lock karena kedua tahap autentikasi terpenuhi. Pada skenario kedua, sistem diharapkan menolak akses karena OTP tidak sesuai meskipun UID RFID terdaftar. Pada skenario ketiga, sistem diharapkan menolak akses sejak tahap pertama karena UID RFID tidak terdaftar.

Skenario tambahan dapat dilakukan untuk menguji OTP yang melewati batas waktu berlaku dan OTP yang digunakan kembali. Namun, apabila skenario tambahan tersebut tidak dilakukan, maka pembahasan hasil tidak boleh menyatakan bahwa sistem telah mampu mengatasi seluruh bentuk penyalahgunaan OTP.

2.5. Parameter Pengujian

Parameter yang diamati dalam penelitian ini meliputi status pembacaan UID RFID, status validasi UID, status pengiriman OTP, kesesuaian OTP, respons relay, kondisi solenoid lock, dan waktu respons sistem. Status pembacaan UID digunakan untuk mengetahui apakah kartu RFID dapat terbaca oleh modul RC522. Status validasi UID digunakan untuk mengetahui apakah kartu termasuk dalam daftar yang terdaftar pada sistem.

Status pengiriman OTP digunakan untuk memastikan bahwa OTP hanya dikirim ketika UID RFID terdaftar. Kesesuaian OTP digunakan untuk menentukan apakah kode yang dimasukkan pengguna sesuai dengan kode yang dihasilkan sistem. Respons relay dan kondisi solenoid lock digunakan untuk mengetahui apakah sistem membuka atau menolak akses sesuai dengan hasil autentikasi. Waktu respons digunakan untuk mengetahui durasi proses dari pembacaan RFID sampai solenoid lock terbuka pada skenario akses valid.

2.6. Teknik Analisis Data

Data hasil pengujian dianalisis secara deskriptif kuantitatif. Analisis dilakukan dengan membandingkan respons aktual sistem terhadap respons yang diharapkan pada setiap skenario pengujian. Jika respons aktual sesuai dengan respons yang diharapkan, maka percobaan tersebut dinyatakan berhasil. Jika respons aktual tidak sesuai dengan respons yang diharapkan, maka percobaan tersebut dinyatakan gagal.

$$TK = (PB / TP) \times 100\% \quad (1)$$

$$TG = (PG / TP) \times 100\% \quad (2)$$

$$\bar{T} = (\Sigma_{i=1}^{n} T_i) / n \quad (3)$$

Keterangan variabel:
TK = Tingkat Keberhasilan
TG = Tingkat Kegagalan
PB = Jumlah Percobaan Berhasil

PG = Jumlah Percobaan Gagal
TP = Jumlah Seluruh Percobaan
$\bar{T}$ = Rata-rata Waktu Respons
T_i = Waktu respons pada percobaan ke-i
n = Jumlah percobaan

Untuk skenario akses valid, keberhasilan dihitung berdasarkan kemampuan sistem membuka solenoid lock ketika UID RFID terdaftar dan OTP yang dimasukkan sesuai. Untuk skenario akses tidak valid, keberhasilan dihitung berdasarkan kemampuan sistem menolak akses ketika OTP salah atau UID RFID tidak terdaftar. Dengan demikian, analisis tidak hanya menilai keberhasilan sistem dalam membuka kunci, tetapi juga menilai kesesuaian sistem dalam menolak akses yang tidak memenuhi syarat autentikasi.

Hasil pengujian dan perhitungan dari setiap skenario disajikan pada bagian Hasil dan Pembahasan. Kesimpulan penelitian dibatasi pada skenario yang diuji agar tidak menghasilkan klaim yang melebihi data pengujian.

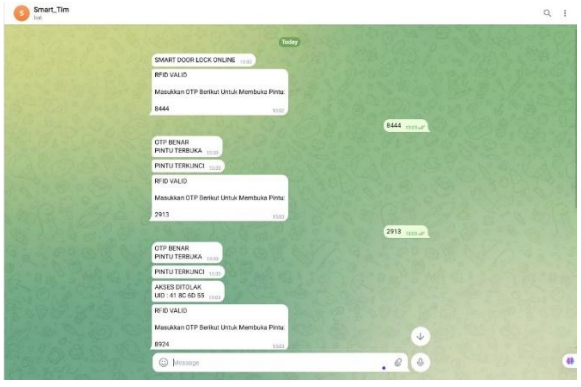
3. HASIL DAN PEMBAHASAN

3.1. Hasil Implementasi Sistem

Sistem smart keyless 2FA berbasis IoT telah diimplementasikan menggunakan ESP32, RFID RC522, Telegram Bot, relay, dan solenoid lock 12V. ESP32 berperan sebagai pusat kendali untuk membaca UID kartu RFID, memvalidasi data pengguna, mengirim dan memeriksa OTP melalui Telegram Bot, serta mengendalikan relay untuk membuka atau menutup solenoid lock.

Pada implementasi perangkat keras, RFID RC522 dihubungkan ke ESP32 melalui komunikasi SPI. Relay digunakan untuk mengendalikan solenoid lock 12V dengan sumber daya eksternal, sehingga solenoid tidak terhubung langsung ke pin ESP32. Pada implementasi perangkat lunak, sistem menjalankan autentikasi secara berurutan, yaitu membaca UID RFID, memeriksa status UID, mengirim OTP jika UID terdaftar, memvalidasi OTP yang dikirim pengguna, dan mengaktifkan relay apabila autentikasi sesuai dengan kondisi yang ditentukan.

Gambar 3. Prototipe Sistem Smart Keyless 2FA Berbasis ESP32, RFID RC522, Telegram Bot, Relay, dan Solenoid Lock



Gambar 4. Tampilan Pengiriman OTP melalui Telegram Bot

3.2. Hasil Pengujian Fungsional

Pengujian fungsional dilakukan untuk mengetahui kesesuaian respons sistem terhadap kombinasi UID RFID dan OTP. Sistem dinyatakan berhasil apabila respons aktual sesuai dengan respons yang diharapkan pada setiap skenario pengujian. Pengujian ini tidak digunakan untuk menyatakan bahwa sistem aman terhadap seluruh bentuk serangan, tetapi untuk menilai apakah alur autentikasi dua tahap berjalan sesuai rancangan.

Tabel 1. Hasil Pengujian Fungsional Autentikasi RFID dan OTP

No	Skenario Pengujian	UID	OTP	Respons Sistem	Jumlah Percobaan	Berhasil	Gagal	Keberhasilan
1	RFID terdaftar dan OTP valid	Terdaftar	Valid	Solenoid lock terbuka	10	10	0	100%
2	RFID terdaftar dan OTP tidak valid	Terdaftar	Tidak valid	Solenoid lock tetap terkunci	10	10	0	100%
3	RFID tidak terdaftar	Tidak terdaftar	OTP tidak dikirim	Solenoid lock tetap terkunci	10	10	0	100%

Berdasarkan Tabel 1, pengujian fungsional dilakukan pada tiga skenario autentikasi dengan masing-masing 10 kali percobaan. Pada skenario RFID terdaftar dan OTP valid, sistem berhasil membuka solenoid lock sebanyak 10 kali dari 10 percobaan, sehingga tingkat keberhasilan mencapai 100%. Pada skenario RFID terdaftar tetapi OTP tidak valid, sistem berhasil menolak akses dengan mempertahankan solenoid lock tetap terkunci sebanyak 10 kali dari 10 percobaan. Hasil serupa juga diperoleh pada skenario RFID tidak terdaftar, yaitu sistem tidak mengirimkan OTP dan solenoid lock tetap terkunci pada seluruh percobaan.

Secara keseluruhan, hasil pengujian menunjukkan bahwa sistem memberikan respons sesuai dengan rancangan pada seluruh skenario yang diuji. Akses hanya diberikan ketika UID RFID terdaftar dan OTP yang dimasukkan valid, sedangkan akses ditolak ketika OTP tidak valid atau UID RFID tidak terdaftar. Dengan demikian, logika autentikasi dua tahap pada prototipe ini berjalan sesuai skenario pengujian. Namun, hasil tersebut masih terbatas pada pengujian fungsional dan belum mencakup pengujian terhadap risiko keamanan lain, seperti duplikasi kartu RFID, percobaan OTP berulang, atau gangguan koneksi internet.

3.3. Hasil Pengujian Waktu Respons

Pengujian waktu respons dilakukan pada skenario kartu RFID terdaftar dan OTP valid. Pengujian ini bertujuan untuk mengetahui durasi proses autentikasi dari pembacaan RFID sampai solenoid lock terbuka. Waktu respons dapat dipengaruhi oleh koneksi WiFi, respons Telegram Bot, dan waktu pemrosesan pada ESP32.

Tabel 2. Hasil Pengujian Waktu Respons Sistem

No	Percobaan	Waktu Respons	Respons Sistem	Keterangan
1	Percobaan 1	0,3 detik	Solenoid lock terbuka	Berhasil
2	Percobaan 2	0,4 detik	Solenoid lock terbuka	Berhasil
3	Percobaan 3	0,1 detik	Solenoid lock terbuka	Berhasil
4	Percobaan 4	0,2 detik	Solenoid lock terbuka	Berhasil
5	Percobaan 5	0,3 detik	Solenoid lock terbuka	Berhasil
Rata-rata	-	0,26 detik	-	-

Berdasarkan Tabel 2, pengujian waktu respons dilakukan sebanyak lima kali pada skenario RFID terdaftar dan OTP valid. Hasil pengujian menunjukkan bahwa seluruh percobaan berhasil membuka solenoid lock, dengan waktu respons masing-masing sebesar 0,3 detik, 0,4 detik, 0,1 detik, 0,2 detik, dan 0,3 detik. Dari hasil tersebut, diperoleh rata-rata waktu respons sebesar 0,26 detik.

Nilai rata-rata tersebut menunjukkan waktu yang dibutuhkan sistem untuk memberikan respons setelah proses autentikasi dinyatakan valid hingga solenoid lock terbuka. Hasil ini menunjukkan bahwa sistem dapat mengaktifkan solenoid lock sesuai rancangan pada kondisi pengujian. Namun, nilai waktu respons tersebut tidak dapat digeneralisasi untuk seluruh kondisi penggunaan karena proses komunikasi dengan Telegram Bot tetap dipengaruhi oleh koneksi internet, respons layanan Telegram, dan kondisi jaringan saat pengujian dilakukan.

3.4.Pembahasan

Hasil pengujian menunjukkan bahwa sistem menerapkan autentikasi secara berlapis. Kartu RFID berfungsi sebagai tahap autentikasi pertama, sedangkan OTP Telegram berfungsi sebagai tahap autentikasi kedua. Akses hanya diberikan apabila kedua tahap tersebut memenuhi kondisi yang ditentukan. Dengan demikian, kepemilikan kartu RFID saja belum cukup untuk membuka solenoid lock apabila OTP yang dimasukkan tidak valid.

Pada skenario kartu RFID tidak terdaftar, sistem tidak mengirimkan OTP. Hal ini menunjukkan bahwa validasi UID dilakukan sebelum proses autentikasi kedua dijalankan. Mekanisme tersebut membuat sistem hanya memproses OTP untuk kartu yang telah didaftarkan. Namun, hasil ini masih terbatas pada pengujian fungsional dan belum mencakup pengujian terhadap risiko seperti duplikasi kartu RFID, percobaan OTP berulang, gangguan jaringan, atau kebocoran token Telegram Bot.

Jika dibandingkan dengan penelitian sebelumnya, sebagian sistem keamanan pintu berbasis IoT masih menempatkan RFID sebagai faktor utama autentikasi [5]–[9]. Pendekatan tersebut dapat membantu proses identifikasi pengguna, tetapi belum sepenuhnya mengurangi risiko apabila kartu RFID digunakan oleh pihak yang tidak berwenang. Penelitian yang menerapkan autentikasi berlapis, seperti kombinasi RFID e-KTP dan OTP melalui platform mobile, menunjukkan bahwa penambahan faktor autentikasi dapat memperkuat validasi akses [10]. Penelitian ini memiliki perbedaan pada penggunaan UID RFID sebagai tahap pertama dan OTP melalui bot Telegram sebagai tahap kedua pada prototipe berbasis ESP32. Oleh karena itu, kontribusi penelitian ini berada pada validasi alur autentikasi dua tahap serta pengujian kondisi akses diterima dan ditolak dalam sistem smart keyless berbasis IoT.

3.5. Keterbatasan Sistem

Penelitian ini masih memiliki beberapa keterbatasan. Pertama, proses OTP bergantung pada koneksi internet dan layanan Telegram Bot. Kedua, pengujian belum mencakup risiko duplikasi kartu RFID, brute force OTP, dan kebocoran token bot. Ketiga, sistem masih diuji dalam bentuk prototipe, sehingga hasilnya belum dapat langsung digeneralisasi untuk penggunaan operasional skala luas. Oleh karena itu, penelitian lanjutan dapat menambahkan pembatasan percobaan OTP, pencatatan log akses, pengujian kestabilan jaringan, serta pengujian keamanan yang lebih mendalam.

4. KESIMPULAN

Penelitian ini berhasil merancang dan mengimplementasikan prototipe sistem smart keyless 2FA berbasis IoT menggunakan ESP32, RFID RC522, Telegram Bot, relay, dan solenoid lock 12V. Sistem menerapkan autentikasi dua tahap, yaitu validasi UID RFID sebagai tahap pertama dan validasi OTP melalui Telegram Bot sebagai tahap kedua. Berdasarkan hasil pengujian fungsional pada tiga skenario utama, sistem memberikan respons sesuai dengan rancangan. Pada skenario RFID terdaftar dan OTP valid, sistem berhasil membuka solenoid lock sebanyak 10 kali dari 10 percobaan. Pada skenario RFID terdaftar tetapi OTP tidak valid, sistem berhasil menolak akses sebanyak 10 kali dari 10 percobaan. Pada skenario RFID tidak terdaftar, sistem juga berhasil menolak akses dengan tidak mengirimkan OTP dan mempertahankan solenoid lock tetap terkunci sebanyak 10 kali dari 10 percobaan.

Hasil pengujian waktu respons menunjukkan bahwa sistem memiliki rata-rata waktu respons sebesar 0,26 detik pada proses aktivasi solenoid lock setelah autentikasi dinyatakan valid. Hasil tersebut menunjukkan bahwa prototipe dapat menjalankan fungsi dasar autentikasi dua tahap sesuai skenario pengujian. Namun, penelitian ini masih terbatas pada pengujian fungsional dan belum mencakup pengujian keamanan lanjutan, seperti duplikasi kartu RFID, percobaan OTP berulang, kebocoran token Telegram Bot, maupun gangguan koneksi internet. Oleh karena itu, pengembangan selanjutnya dapat difokuskan pada penambahan pembatasan percobaan OTP, pencatatan log akses, pengujian kestabilan jaringan, serta penguatan mekanisme keamanan sistem sebelum diterapkan pada lingkungan operasional yang lebih luas.

UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih kepada dosen pembimbing dan rekan sejawat yang telah memberikan bimbingan, masukan, dan saran selama proses penelitian. Terima kasih juga disampaikan kepada pihak yang telah membantu penyediaan sarana dan dukungan selama proses perancangan, implementasi, dan pengujian prototipe smart keyless 2FA.

DAFTAR PUSTAKA

[1] A. Kumar, A. K. Jain, and M. Dua, "A comprehensive taxonomy of security and privacy issues in RFID," *Complex Intell. Syst.*, vol. 7, no. 3, pp. 1327–1347, Jun. 2021, doi: 10.1007/s40747-021-00280-6.

[2] V. Kumar, R. Kumar, A. A. Khan, V. Kumar, Y.-C. Chen, and C.-C. Chang, "RAFI: Robust Authentication Framework for IoT-Based RFID Infrastructure," *Sensors*, vol. 22, no. 9, p. 3110, Apr. 2022, doi: 10.3390/s22093110.

[3] T.-M. Hoang, V.-H. Bui, and N.-H. Nguyen, "An Integrated Two-Factor Authentication Scheme for Smart Communications and Control Systems," *MENDEL*, vol. 29, no. 2, pp. 181–190, Dec. 2023, doi: 10.13164/mendel.2023.2.181.

[4] M. S. Ahmed, P. Kumar, and R. Singh, "Secure and Smart Door Lock with Dual-Factor Authentication for Critical Zones," *Math. Stat. Eng. Appl.*, vol. 72, no. 1, pp. 1491–1501, 2023, doi: 10.17762/msea.v72i1.2373.

[5] A. S. Permana, J. Arthady Sormin, and N. Ketut H.D, "Perancangan Sistem Keamanan Ruang Server Akses Doorlock Dengan Teknologi RFID Berbasis IoT Pada Ruang Server FISIP UNJANI," *Epsil. J. Electr. Eng. Inf. Technol.*, vol. 20, no. 2, pp. 100–110, Dec. 2022, doi: 10.55893/epsilon.v20i2.91.

[6] Azhar Jauharul Umam, D. Setiana, and A. Pradana, "Rancangan radio frequency identification (rfid) smart door lock system berbasis internet of things untuk manajemen membership fitness center," *J. CoSciTech (Computer Sci. Inf. Technol.*, vol. 4, no. 2, pp. 359–365, Aug. 2023, doi: 10.37859/coscitech.v4i2.5126.

[7] A. N. M. Andreas and R. Arijanto, "Rancang Bangun Smart Home IoT dengan Integrasi Kunci Rfid dan Otomasi Elektronik," *bit-Tech*, vol. 7, no. 2, pp. 235–243, Dec. 2024, doi: 10.32877/bt.v7i2.1729.

[8] M. Wahyu Salfian, "Design of Door Security System using Rfid Based on IoT at Stmik Kaputama," *J. Artif. Intell. Eng. Appl.*, vol. 5, no. 1, pp. 604–610, Oct. 2025, doi: 10.59934/jaiea.v5i1.1367.

[9] Haris Asysyauqi, Moh. Ferdi Andriansyah, Lya Nurul Ulla, and Adi Sucipto, "Sistem Keamanan Pintu Otomatis Berbasis IoT dengan Teknologi RFID dan Aplikasi Mobile Menggunakan Metode Fuzzy Mamdani," *Modem J. Inform. dan Sains Teknol.*, vol. 3, no. 2, pp. 42–50, Apr. 2025, doi: 10.62951/modem.v3i2.405.

[10] U. Handasah, R. Afdila, A. Sani, R. Hendrawan, and M. Hamid, "Development of a Two-Layer Secure IoT Locker System Using e-KTP RFID and Mobile OTP via Blynk Platform," *J. Technomaterial Phys.*, vol. 7, no. 2, Oct. 2025, doi: 10.32734/jotp.v7i2.22170.

[11] A. Febriansyah and A. Yunanda, "SIMULASI SISTEM KEAMANAN DAN KENDALI GERBANG OTOMATIS PADA PORTAL PERUMAHAN MENGGUNAKAN TEKNOLOGI TANPA KUNCI BERBASIS IOT," *J. Comput. Sci. Inf. Technol.*, vol. 2, no. 3, pp. 324–337, Jun. 2025, doi: 10.70248/jcsit.v2i3.2088.

[12] M. W. Aryadi, I. K. R. Arthana, and P. H. Suputra, "SMART LOCK SYSTEM BERBASIS IOT MENGGUNAKAN ESP32 UNTUK KEAMANAN AKSES PUSAT DATA (STUDI KASUS: UPA TIK UNDIKSHA)," *J. Inform. dan Tek. Elektro Terap.*, vol. 14, no. 1, Jan. 2026, doi: 10.23960/jitet.v14i1.8826.

[13] Muarif, Ade Sumaedi, and Mardiansyah, "Monitoring Suhu Ruangan Server Jaringan Hostpot Berbasis Mikrokontroler NodeMCU ESP8266 Dengan Thingspeak," *J. Inf. Comput.*, vol. 2, no. 1, pp. 17–27, Jan. 2024, doi: 10.32493/jicomisc.v2i1.38638.

[14] Rajin Nahampun, Sewaka, and Taswanda Taryo, "Rancang Bangun Smartlock Detection Berbasis Mikrokotroller Dan ESP8266 Sebagai Bahan Media Pembelajaran Laboratorium Teknik Informatika Dan Komputer," *J. Inf. Comput.*, vol. 3, no. 1, pp. 74–83, Jan. 2025, doi: 10.32493/jicomisc.v3i1.40778.