Electrician : Jurnal Rekayasa dan Teknologi Elektro
Vol. 20 No. 02, e-ISSN:2549-3442 http://dx.doi.org/10.23960/elc.v20.n2.3009

Desain dan Implementasi Sistem Keamanan Pintu Menggunakan Autentikasi Multi-Modal Sidik Jari dan Keypad Berbasis IoT

Tole Sutikno[1*], Wahidin Ridwan[1], Watra Arsadiando[2]

[1]Teknik Elektro, Fakultas Teknologi Industri, Universitas Ahmad Dahlan, Yogyakarta, 55191, Indonesia
[2]Embedded System and Power Electronic Research Group (ESPERG), Yogyakarta, 55198, Indonesia

Received: 05-12-2025
Accepted: 10-02-2026

Keywords:
Kontrol akses pintu; fingerprint; keypad; IoT; Telegram.

Corespondent Email:
tole@te.uad.ac.id

Abstrak. *Sistem keamanan pintu konvensional memiliki keterbatasan, seperti risiko kehilangan kunci, potensi duplikasi, dan tidak tersedianya pemantauan jarak jauh. Penelitian ini mengembangkan sistem kontrol akses pintu berbasis Internet of Things (IoT) dengan autentikasi multi-modal menggunakan sensor sidik jari sebagai metode utama dan keypad sebagai metode alternatif. Sistem dilengkapi notifikasi real-time melalui aplikasi Telegram untuk memantau aktivitas akses. Perangkat dirancang menggunakan mikrokontroler ESP32, sensor fingerprint, keypad, solenoid door lock, dan integrasi Telegram Bot API. Pengujian dilakukan pada lima pengguna terdaftar dengan total 30 percobaan autentikasi sidik jari pada kondisi jari normal, basah, dan berdebu, serta 30 percobaan menggunakan sidik jari tidak terdaftar. Selain itu, dilakukan 15 percobaan PIN benar dan 15 percobaan PIN salah pada keypad. Hasil menunjukkan bahwa autentikasi sidik jari bekerja optimal pada kondisi normal. Namun, mengalami penurunan performa pada kondisi basah dan berdebu dengan nilai True Acceptance Rate (TAR) sebesar 56,7% dan False Rejection Rate (FRR) sebesar 43,3%. Seluruh sidik jari tidak terdaftar berhasil ditolak tanpa false acceptance. Autentikasi keypad menunjukkan kinerja konsisten, sementara notifikasi Telegram berhasil dikirim pada sebagian besar skenario dengan waktu tunda 2,5–3,8 detik. Sistem ini meningkatkan keamanan dan fleksibilitas akses pintu berbasis IoT.*

Abstract. *Conventional door security systems have limitations, including the risk of key loss, the possibility of duplication, and the lack of remote monitoring. This study developed an Internet of Things (IoT)-based door access control system with multimodal authentication, using a fingerprint sensor as the primary method and a keypad as an alternative. The system is equipped with real-time notifications via the Telegram application to monitor access activity. The device was designed using an ESP32 microcontroller, a fingerprint sensor, a keypad, a solenoid door lock, and Telegram Bot API integration. Testing was conducted on five registered users with a total of 30 fingerprint authentication attempts under normal, wet, and dusty conditions, as well as 30 attempts using unregistered fingerprints. In addition, 15 correct PIN attempts and 15 incorrect PIN attempts were conducted on the keypad. The results showed that fingerprint authentication worked optimally under normal conditions. However, performance decreased under wet and dusty conditions with a True Acceptance Rate (TAR) of 56.7% and a False Rejection Rate (FRR) of 43.3%. All unregistered fingerprints were successfully rejected without false acceptance. Keypad authentication performed consistently, and Telegram notifications were successfully delivered in most scenarios, with a delay of 2.5–3.8 seconds. This system enhances the security and flexibility of IoT-based door access.*

1. PENDAHULUAN

Sistem keamanan konvensional yang masih mengandalkan kunci fisik memiliki berbagai kelemahan, seperti mudah hilang, mudah diduplikasi, dan rentan dibobol [1]. Kondisi ini membuat tingkat keamanannya semakin dipertanyakan, terutama pada lingkungan rumah modern yang menuntut perlindungan lebih baik [2]. Penelitian sebelumnya menunjukkan bahwa kelemahan kunci fisik menjadi alasan utama berkembangnya teknologi kontrol akses berbasis digital dan *Internet of Things* IoT [3].

Seiring perkembangan teknologi, konsep *smart home* mulai diterapkan secara luas, termasuk pada sistem pengamanan pintu otomatis [4]. Berbagai perangkat cerdas dikembangkan untuk meningkatkan kenyamanan, efisiensi, serta keamanan pengguna [5]. Salah satu teknologi yang banyak digunakan adalah sistem kontrol akses elektronik, yang dapat mengatur proses masuk dan keluar secara lebih terstruktur dibandingkan kunci mekanis [6]. Perkembangan ini membuka peluang penerapan metode autentikasi yang lebih modern dan akurat [7].

Autentikasi biometrik, khususnya berbasis sidik jari, menjadi salah satu solusi yang menawarkan tingkat keamanan tinggi [8]. Sidik jari memiliki karakteristik unik bagi tiap individu, sehingga sulit dipalsukan dan sangat efektif untuk proses identifikasi [9]. Selain biometrik, penggunaan *keypad* sebagai autentikasi tambahan juga dapat meningkatkan tingkat keamanan melalui kombinasi faktor verifikasi [10]. Pendekatan multifaktor ini membantu meminimalkan risiko akses ilegal.

Selain itu, kemajuan teknologi IoT memungkinkan perangkat keamanan dapat dipantau dan dikendalikan dari jarak jauh melalui jaringan internet [11], [12]. Integrasi IoT pada sistem kontrol akses memberikan kemampuan *monitoring real-time*, pengelolaan pengguna secara dinamis, serta peningkatan fleksibilitas operasi sistem[13]. Dengan adanya konektivitas ini, pengguna dapat memeriksa status pintu maupun melakukan kontrol akses secara lebih efisien [14].

Berdasarkan studi literatur yang ada, penelitian sistem keamanan pintu berbasis IoT masih berfokus pada penggunaan autentikasi tunggal biometrik atau sekadar integrasi perangkat keras. Perancangan skema autentikasi multi-modal yang terstruktur, khususnya yang dilengkapi mekanisme pengambilan keputusan yang jelas, masih belum banyak dibahas secara mendalam. Selain itu, metode autentikasi berlapis yang dirancang secara sistematis untuk meningkatkan keamanan dan keandalan sistem juga masih relatif terbatas. Oleh karena itu, penelitian ini mengusulkan mekanisme autentikasi berlapis berbasis kondisi pada sistem keamanan pintu berbasis IoT. Autentikasi sidik jari digunakan sebagai metode utama, sedangkan autentikasi keypad diaktifkan sebagai mekanisme alternatif ketika terjadi kegagalan pembacaan biometrik.

2. TINJAUAN PUSTAKA

Sistem IoT memungkinkan perangkat fisik saling berkomunikasi dan dimonitor secara *real-time* melalui jaringan [15]. Arsitektur IoT yang melibatkan perangkat *edge* (mikrokontroler), *gateway*, dan layanan *cloud* telah banyak diadopsi pada aplikasi smart home, termasuk sistem kontrol akses pintu untuk meningkatkan fleksibilitas pemantauan dan manajemen pengguna [16]. Pemanfaatan IoT juga memungkinkan integrasi notifikasi *real-time* sebagai mekanisme pemantauan jarak jauh [17].

Metode autentikasi untuk sistem keamanan pintu juga terus berkembang [18]. Teknologi biometrik mulai menggantikan metode konvensional yang kurang aman [19]. Sidik jari menjadi salah satu biometrik yang paling banyak digunakan karena unik, stabil, dan akurat [20], [21]. Beberapa penelitian menambahkan *keypad* PIN sebagai metode cadangan. Tujuannya adalah memastikan pengguna tetap dapat mengakses sistem ketika pembacaan sidik jari mengalami kegagalan [22].

Keamanan komunikasi dan keandalan perangkat IoT juga menjadi perhatian penting dalam penelitian [23]. Tantangan utama meliputi perlindungan data biometrik, keamanan transmisi jaringan, serta potensi kerentanan pada perangkat [24]. Karena itu, desain sistem harus menerapkan enkripsi, autentikasi aman, dan pemantauan aktivitas [25]. Selain itu, beberapa studi menekankan pentingnya pengujian performa pada kondisi nyata untuk memastikan konsistensi pembacaan sensor dan efektivitas notifikasi [26]. Penelitian

ini merespons kebutuhan tersebut dengan mengembangkan sistem kontrol akses IoT yang menggabungkan sidik jari, *keypad*, dan notifikasi *real-time*.

3. METODE PENELITIAN

3.1. Tinjauan Arsitektur Sistem

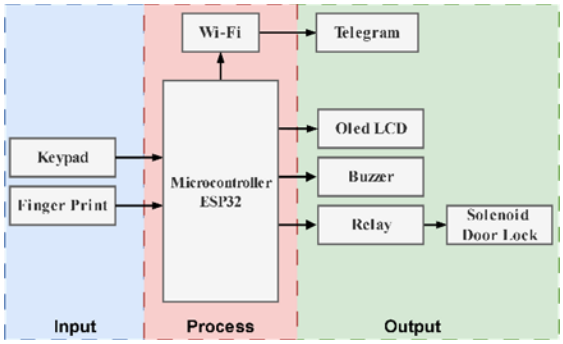
Sistem kontrol akses yang dikembangkan dirancang untuk menyediakan mekanisme autentikasi yang aman dan terhubung ke layanan IoT untuk pemantauan jarak jauh secara *real-time*. Sistem kontrol akses menggunakan mikrokontroler ESP32 sebagai pusat pemrosesan data. Mikrokontroler menerima input dari sensor sidik jari dan *keypad* sebagai metode autentikasi. Sistem menggunakan sensor sidik jari untuk membaca pola biometrik pengguna dengan akurasi tinggi. *Keypad* menyediakan input PIN sebagai opsi autentikasi alternatif. Mikrokontroler memproses data autentikasi melalui logika verifikasi berlapis untuk meningkatkan keamanan. Sistem mengirim status autentikasi ke aplikasi Telegram melalui koneksi Wi-Fi untuk pemantauan jarak jauh. Notifikasi memberikan informasi aktivitas akses kepada administrator secara *real-time*. Modul relay mengendalikan kunci pintu setelah autentikasi dinyatakan valid.

Sistem menerapkan mekanisme autentikasi berlapis berbasis kondisi (*condition-based layered authentication*). Pada tahap awal, sistem melakukan verifikasi menggunakan sidik jari. Apabila proses autentikasi biometrik gagal atau tidak valid, sistem secara otomatis mengaktifkan autentikasi berbasis PIN melalui keypad. Pendekatan ini dirancang untuk meningkatkan keandalan sistem dengan tetap mempertahankan tingkat keamanan yang memadai. Diagram blok sistem yang ditujukkan pada Gambar 1 dengan alur data dari sensor ke mikrokontroler secara jelas.

3.2. Implementasi Perangkat Keras dan Perangkat Lunak

Subsistem perangkat keras terdiri dari mikrokontroler ESP32, sensor sidik jari, *keypad*, solenoid kunci pintu, relay dan modul daya. ESP32 berfungsi sebagai pengontrol pusat untuk semua operasi dan menangani konektivitas Wi-Fi untuk komunikasi IoT. Sensor sidik jari membaca pola sidik jari selama pendaftaran dan verifikasi, lalu mengirimkan hasil pencocokan ke ESP32. Sedangkan, *keypad* menangkap input PIN numerik untuk autentikasi alternatif jika finger print tidak bisa digunakan atau bermasalah. Selanjutya, solenoid mengontrol mekanisme penguncian fisik pintu dan menerima perintah aktivasi setelah verifikasi berhasil. Catu daya menyediakan tegangan stabil ke semua modul, memastikan keandalan sistem selama pengoperasian. Representasi skematik sistem yang diusulkan ditunjukkan pada Gambar 2.

Perangkat lunak dikembangkan menggunakan Arduino IDE. ESP32 menginisialisasi modul fingerprint, *keypad*, LCD, buzzer, relay, serta koneksi Wi-Fi. Program menerapkan dua metode autentikasi independen biometrik atau PIN. Ketika fingerprint dipilih, ESP32 mencocokkan data sidik jari dengan database internal modul. Jika fingerprint tidak valid, sistem memungkinkan pengguna beralih ke autentikasi berbasis PIN. Modul *keypad* membaca input numerik dan membandingkannya dengan PIN yang tersimpan. Jika PIN salah, buzzer memberikan umpan balik berupa dua bunyi pendek. Setelah autentikasi berhasil melalui salah satu metode, program mengirimkan notifikasi ke Telegram menggunakan bot API dan mengaktifkan relay untuk membuka pintu. Struktur kontrol program mengikuti urutan proses seperti yang ditunjukkan pada Gambar 3.



Gambar 1. Diagram blok sistem kontrol pengaman pintu berbasis IoT

3.3. Metode Pengujian dan Evaluasi Kinerja

Pengujian sistem dilakukan untuk mengevaluasi kinerja mekanisme autentikasi yang diusulkan. Pengujian melibatkan sejumlah pengguna terdaftar yang masing-masing melakukan beberapa kali percobaan autentikasi menggunakan sidik jari dan keypad. Setiap

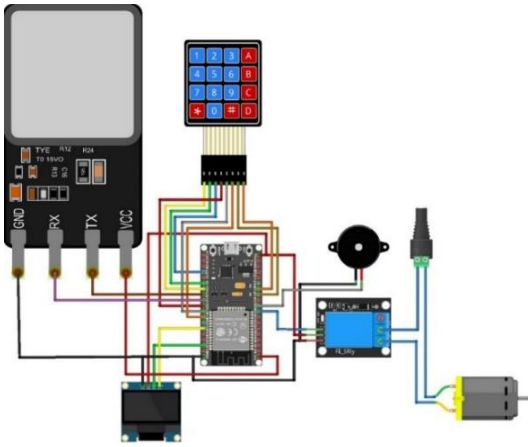
percobaan dicatat sebagai autentikasi berhasil atau gagal.

Untuk mengevaluasi kinerja autentikasi sistem, digunakan beberapa parameter standar pada sistem biometrik, yaitu True Acceptance Rate (TAR), False Acceptance Rate (FAR), dan False Rejection Rate (FRR). TAR didefinisikan sebagai rasio jumlah autentikasi valid yang berhasil diterima terhadap total percobaan autentikasi valid. FAR menyatakan rasio jumlah autentikasi tidak valid yang keliru diterima sistem terhadap total percobaan autentikasi tidak valid. Sementara itu, FRR menunjukkan rasio penolakan autentikasi yang seharusnya valid, yang dihitung sebagai komplemen dari TAR. Perhitungan ketiga parameter tersebut dirumuskan sebagai berikut:

$$\text{TAR} = \frac{Total\ percobaan\ autentikasi\ valid}{Jumlah\ autentikasi\ valid\ yang\ diterima} \quad (1)$$

$$\text{FAR} = \frac{Jumlah\ autentikasi\ tidak\ valid\ yang\ diterima}{Total\ percobaan\ autentikasi\ tidak\ valid} \quad (2)$$

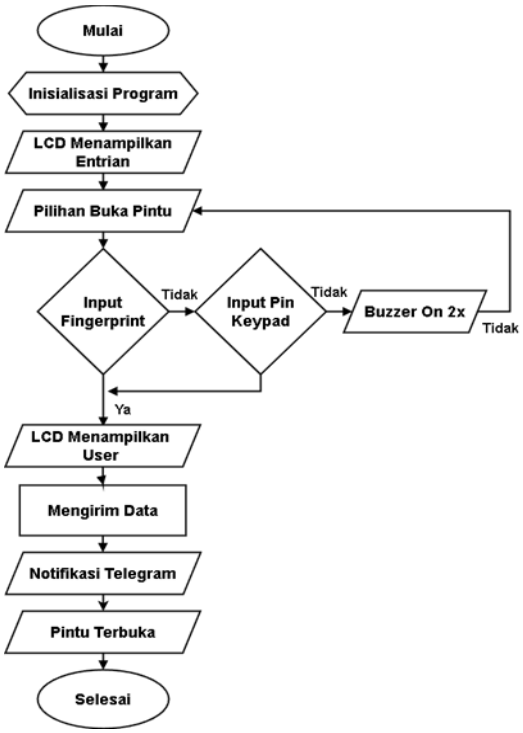
$$\text{FRR} = 1 - TAR \quad (3)$$



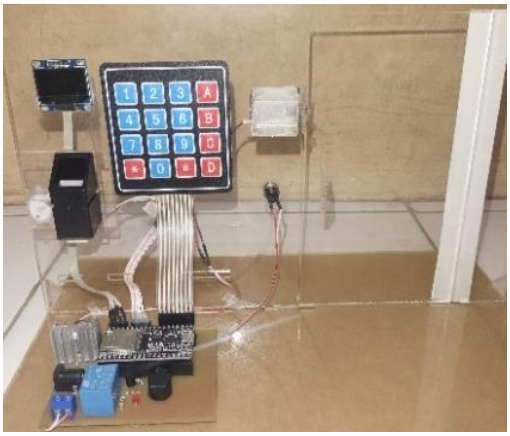
Gambar 2. Skematik sistem yang diusulkan

4. HASIL DAN PEMBAHASAN

Prototipe sistem pengaman pintu yang telah dikembangkan ditunjukkan pada Gambar 4. Perangkat ini terdiri dari modul ESP32, sensor sidik jari, *keypad* numerik, solenoid lock, buzzer, dan layar OLED yang dirakit pada satu kesatuan rangkaian. Seluruh komponen sudah diuji untuk memastikan koneksi listrik dan komunikasi data berjalan stabil. Prototipe ini menjadi dasar pelaksanaan seluruh skenario pengujian, termasuk pengujian autentikasi fingerprint, verifikasi PIN, dan pengiriman notifikasi ke Telegram.



Gambar 3. Diagram Alir Sistem



Gambar 4. Prototipe sistem pengaman pintu yang telah dikembangkan

4.1. Pengujian Fingerprint

Pengujian sensor fingerprint dilakukan menggunakan sidik jari yang telah terdaftar pada sistem untuk mengevaluasi kemampuan autentikasi pengguna yang sah. Selain itu, pengujian juga dilakukan untuk mengamati respons sistem terhadap variasi kondisi permukaan jari. Pengujian melibatkan lima pengguna terdaftar dengan total 30 percobaan, di mana setiap pengguna diuji pada kondisi jari

normal, basah, dan berdebu. Gambar 5(a). menunjukkan salah satu hasil percobaan ketika sidik jari yang dimasukkan sesuai dengan data yang terdaftar. Ketika sidik jari yang dimasukkan sesuai dengan data yang terdaftar, LCD akan menampilkan status kunci terbuka. Tampilan saat ID sidik jari terverifikasi dapat dilihat pada Gambar 5(b).

Hasil pengujian menunjukkan bahwa pada kondisi jari normal, seluruh sidik jari terdaftar berhasil dikenali oleh sistem dan mengaktifkan solenoid kunci pintu. Namun, pada kondisi jari basah dan berdebu, sistem mengalami beberapa kegagalan autentikasi meskipun sidik jari berasal dari pengguna yang sah. Kondisi ini menyebabkan pintu tetap terkunci sebagai mekanisme keamanan.

Pada sistem yang dirancang mencapai nilai TAR sebesar 56,7% dan FRR sebesar 43,3% seperti yang ditunjukkan pada Tabel 1. Seluruh kejadian false rejection terjadi pada kondisi jari yang tidak ideal, menunjukkan bahwa performa sensor fingerprint dipengaruhi oleh faktor lingkungan dan kualitas citra sidik jari yang diterima sensor.

(a) (b)

Gambar 5. Tampilan LCD (a) Sidik jari benar (b) Kunci pintu tebuka

Selanjutnya pengujian sidik jari tidak terdaftar dilakukan sebanyak 30 kali percobaan menggunakan lima ID pengguna berbeda dengan variasi kondisi jari, yaitu normal,

Tabel 1. Data pengujian sensor fingerprint ID sidik jari benar

ID Pengguna	Percobaan ke-	Kondisi Jari	Hasil Sistem	Solenoid Terbuka	Keterangan
ID 1	1	Normal	Valid	Ya	Pintu Terbuka
	2	Normal	Valid	Ya	Pintu Terbuka
	3	Normal	Valid	Ya	Pintu Terbuka
	4	Berdebu	Tidak Valid	Tidak	Percobaan masuk
	5	Basah	Tidak Valid	Tidak	Tidak Terbaca
	6	Basah	Tidak Valid	Tidak	Tidak Terbaca
ID 2	1	Normal	Valid	Ya	Pintu Terbuka
	2	Normal	Valid	Ya	Pintu Terbuka
	3	Normal	Valid	Ya	Pintu Terbuka
	4	Berdebu	Tidak Valid	Tidak	Tidak Terbaca
	5	Berdebu	Valid	Ya	Pintu terbuka
	6	Basah	Tidak Valid	Tidak	Percobaan masuk
ID 3	1	Normal	Valid	Ya	Pintu Terbuka
	2	Normal	Valid	Ya	Pintu Terbuka
	3	Normal	Valid	Ya	Pintu Terbuka
	4	Basah	Tidak Valid	Tidak	Tidak Terbaca
	5	Berdebu	Tidak Valid	Tidak	Percobaan masuk
	6	Basah	Tidak Valid	Tidak	Tidak Terbaca
ID 4	1	Normal	Valid	Ya	Pintu Terbuka
	2	Normal	Valid	Ya	Pintu Terbuka
	3	Normal	Valid	Ya	Pintu Terbuka
	4	Berdebu	Tidak Valid	Tidak	Percobaan masuk
	5	Basah	Tidak Valid	Tidak	Tidak Terbaca
	6	Berdebu	Tidak Valid	Tidak	Percobaan masuk
ID 5	1	Normal	Valid	Ya	Pintu Terbuka
	2	Normal	Valid	Ya	Pintu Terbuka
	3	Normal	Valid	Ya	Pintu Terbuka
	4	Berdebu	Tidak Valid	Tidak	Percobaan masuk
	5	Basah	Tidak Valid	Tidak	Tidak Terbaca
	6	Basah	Tidak Valid	Tidak	Tidak Terbaca

berdebu, dan basah. Gambar 6 menampilkan salah satu hasil dari rangkaian percobaan tersebut saat sistem menerima sidik jari yang tidak valid. Seluruh percobaan menghasilkan status tidak valid dan solenoid door lock tidak pernah terbuka. Hal ini menunjukkan bahwa sistem mampu secara konsisten menolak akses dari sidik jari yang tidak terdaftar, baik pada kondisi jari normal maupun pada kondisi lingkungan yang kurang ideal seperti berdebu dan basah seperti ditunjukkan pada Tabel 2. Ketika sidik jari yang dimasukkan tidak terdaftar LCD menampilkan pesan anda tidak terdaftar dan meminta pengguna untuk menempelkan sidik jari kembali.

Pada beberapa percobaan dengan kondisi jari basah, sistem memberikan keterangan tidak terbaca, yang mengindikasikan adanya gangguan kualitas citra sidik jari akibat kelembapan. Meskipun demikian, kondisi tersebut tidak menyebabkan kesalahan autentikasi karena sistem tetap tidak membuka kunci. Secara keseluruhan, hasil pengujian ini menunjukkan bahwa mekanisme autentikasi sidik jari memiliki tingkat keamanan yang tinggi dengan tingkat keberhasilan penolakan akses sebesar 100% terhadap seluruh sidik jari yang tidak terdaftar.

4.2. Pengujian Keypad

Pengujian keypad dilakukan dengan dua kondisi, yaitu memasukkan PIN yang terdaftar dan PIN yang tidak terdaftar dalam sistem. Pengujian ini bertujuan untuk memastikan bahwa mekanisme autentikasi keypad bekerja sesuai dengan fungsi yang diharapkan sebagai metode akses alternatif. Pengujian dengan PIN yang benar dilakukan sebanyak 15 kali menggunakan PIN yang telah terdaftar pada sistem. Gambar 7 menunjukkan salah satu hasil pengujian ketika PIN yang dimasukkan sesuai dengan data yang tersimpan. Dimana LCD menampilkan pesan kode benar dan solenoid door lock terbuka.

Tabel 2. Pengujian sensor fingerprint ID sidik jari Salah

ID Pengguna	Percobaan ke-	Kondisi Jari	Hasil Sistem	Solenoid Terbuka	Keterangan
ID 1	1	Normal	Tidak Valid	Tidak	Pintu Tertutup
	2	Normal	Tidak Valid	Tidak	Pintu Tertutup
	3	Normal	Tidak Valid	Tidak	Pintu Tertutup
	4	Berdebu	Tidak Valid	Tidak	Tidak Terbaca
	5	Basah	Tidak Valid	Tidak	Tidak Terbaca
	6	Berdebu	Tidak Valid	Tidak	Tidak Terbaca
ID 2	1	Normal	Tidak Valid	Tidak	Pintu Tertutup
	2	Normal	Tidak Valid	Tidak	Pintu Tertutup
	3	Normal	Tidak Valid	Tidak	Pintu Tertutup
	4	Berdebu	Tidak Valid	Tidak	Tidak Terbaca
	5	Basah	Tidak Valid	Tidak	Tidak Terbaca
	6	Berdebu	Tidak Valid	Tidak	Tidak Terbaca
ID 3	1	Normal	Tidak Valid	Tidak	Pintu Tertutup
	2	Normal	Tidak Valid	Tidak	Pintu Tertutup
	3	Normal	Tidak Valid	Tidak	Pintu Tertutup
	4	Berdebu	Tidak Valid	Tidak	Tidak Terbaca
	5	Basah	Tidak Valid	Tidak	Tidak Terbaca
	6	Basah	Tidak Valid	Tidak	Tidak Terbaca
ID 4	1	Normal	Tidak Valid	Tidak	Pintu Tertutup
	2	Normal	Tidak Valid	Tidak	Pintu Tertutup
	3	Normal	Tidak Valid	Tidak	Pintu Tertutup
	4	Basah	Tidak Valid	Tidak	Tidak Terbaca
	5	Berdebu	Tidak Valid	Tidak	Tidak Terbaca
	6	Berdebu	Tidak Valid	Tidak	Tidak Terbaca
ID 5	1	Normal	Tidak Valid	Tidak	Pintu Tertutup
	2	Normal	Tidak Valid	Tidak	Pintu Tertutup
	3	Normal	Tidak Valid	Tidak	Pintu Tertutup
	4	Berdebu	Tidak Valid	Tidak	Tidak Terbaca
	5	Basah	Tidak Valid	Tidak	Tidak Terbaca
	6	Berdebu	Tidak Valid	Tidak	Tidak Terbaca

Gambar 6. Tampilan LCD ketika ID sidik jari salah

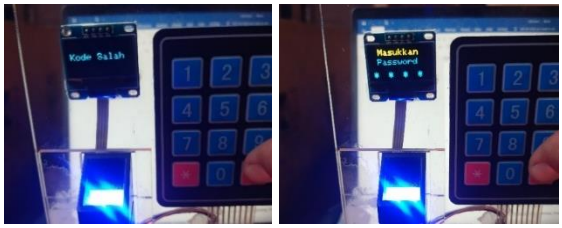
Seluruh percobaan dengan PIN yang benar berhasil diverifikasi oleh sistem, sehingga solenoid door lock dapat terbuka dengan baik. Hal ini menunjukkan bahwa sistem keypad memiliki tingkat keberhasilan 100% dalam memproses input PIN yang valid seperti yang ditunjukkan pada Tabel 3.

Selanjutnya, pengujian keypad dengan memasukkan PIN yang salah dilakukan sebanyak 15 kali menggunakan kombinasi PIN yang berbeda. Gambar 8 menampilkan salah satu kondisi ketika PIN yang dimasukkan tidak sesuai, di mana LCD menampilkan pesan kode salah dan solenoid door lock tetap tertutup. Pada kondisi ini, sistem menolak akses dan meminta pengguna untuk memasukkan ulang PIN. Seluruh input PIN yang salah berhasil ditolak oleh sistem tanpa membuka solenoid door lock. Dengan demikian, mekanisme autentikasi keypad menunjukkan tingkat keberhasilan 100% baik dalam menerima PIN yang benar maupun menolak PIN yang salah.

Gambar 7. Tampilan LCD password benar

Tabel 3. Pengujian PIN benar dan salah

No	Jenis Input	Percobaan ke-	PIN Dimasukkan	Status PIN	Solenoid Terbuka	Keterangan
1	Pin Benar	1	Normal	Valid	Ya	Pintu Terbuka
2	Pin Benar	2	Normal	Valid	Ya	Pintu Terbuka
3	Pin Benar	3	Normal	Valid	Ya	Pintu Terbuka
4	Pin Benar	4	Normal	Valid	Ya	Pintu Terbuka
5	Pin Benar	5	Normal	Valid	Ya	Pintu Terbuka
6	Pin Benar	6	Normal	Valid	Ya	Pintu Terbuka
7	Pin Benar	7	Normal	Valid	Ya	Pintu Terbuka
8	Pin Benar	8	Normal	Valid	Ya	Pintu Terbuka
9	Pin Benar	9	Normal	Valid	Ya	Pintu Terbuka
10	Pin Benar	10	Normal	Valid	Ya	Pintu Terbuka
11	Pin Benar	11	Normal	Valid	Ya	Pintu Terbuka
12	Pin Benar	12	Normal	Valid	Ya	Pintu Terbuka
13	Pin Benar	13	Normal	Valid	Ya	Pintu Terbuka
14	Pin Benar	14	Normal	Valid	Ya	Pintu Terbuka
15	Pin Benar	15	Normal	Valid	Ya	Pintu Terbuka
16	Pin Salah	1	Salah	Gagal	Tidak	Kode Salah
17	Pin Salah	2	Salah	Gagal	Tidak	Kode Salah
18	Pin Salah	3	Salah	Gagal	Tidak	Kode Salah
19	Pin Salah	4	Salah	Gagal	Tidak	Kode Salah
20	Pin Salah	5	Salah	Gagal	Tidak	Kode Salah
21	Pin Salah	6	Salah	Gagal	Tidak	Kode Salah
22	Pin Salah	7	Salah	Gagal	Tidak	Kode Salah
23	Pin Salah	8	Salah	Gagal	Tidak	Kode Salah
24	Pin Salah	9	Salah	Gagal	Tidak	Kode Salah
25	Pin Salah	10	Salah	Gagal	Tidak	Kode Salah
26	Pin Salah	11	Salah	Gagal	Tidak	Kode Salah
27	Pin Salah	12	Salah	Gagal	Tidak	Kode Salah
28	Pin Salah	13	Salah	Gagal	Tidak	Kode Salah
29	Pin Salah	14	Salah	Gagal	Tidak	Kode Salah
30	Pin Salah	15	Salah	Gagal	Tidak	Kode Salah



Gambar 8. Tampilan LCD password Salah

4.3. Pengujian Pengiriman Notifikasi Telegram

Pengujian pengiriman notifikasi melalui aplikasi Telegram dilakukan untuk mengevaluasi kemampuan sistem dalam memberikan informasi akses pintu secara real-time kepada pengguna seperti ditunjukkan pada Tabel 4. Pengujian dilakukan sebanyak 30 kali menggunakan autentikasi sidik jari dengan beberapa kondisi, yaitu kondisi normal, berdebu, dan basah. Parameter yang diamati meliputi status autentikasi, keberhasilan pengiriman notifikasi, serta waktu tunda (*delay*) pengiriman pesan. Berdasarkan hasil pengujian, ketika autentikasi sidik jari berhasil pada kondisi normal, sistem secara konsisten mengirimkan notifikasi Telegram yang menginformasikan bahwa pintu berhasil dibuka. Notifikasi yang diterima sesuai dengan informasi yang ditampilkan pada LCD, seperti ditunjukkan pada Gambar 9 pesan adanya akses masuk dan status pintu terbuka. Waktu tunda pengiriman notifikasi pada kondisi ini berada pada rentang sekitar 2,5 hingga 3,8 detik, yang menunjukkan bahwa sistem mampu memberikan informasi akses dengan waktu respons yang relatif cepat dan stabil.

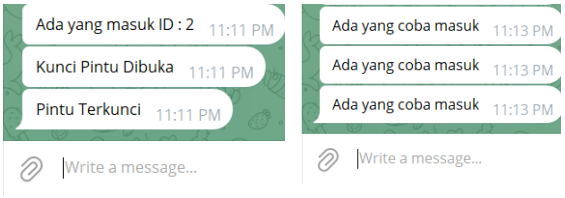
Pada kondisi sidik jari berdebu, sebagian besar proses autentikasi tidak berhasil. Meskipun demikian, sistem tetap mampu mengirimkan notifikasi Telegram dengan keterangan percobaan masuk sebagai bentuk peringatan adanya upaya akses yang tidak valid. Pengiriman notifikasi pada kondisi ini memiliki waktu tunda yang sangat singkat, yaitu kurang dari 0,1 detik, karena sistem tidak melanjutkan

Tabel 4. Pengujian notifikasi telegram

No	Jenis Akses	Kondisi Jari	Status Autentikasi	Notifikasi	Delay (detik)	Keterangan
1	Fingerprint	Normal	Berhasil	Terkirim	05,23	Pintu Terbuka
2	Fingerprint	Normal	Berhasil	Terkirim	03,20	Pintu Terbuka
3	Fingerprint	Normal	Berhasil	Terkirim	03,17	Pintu Terbuka
4	Fingerprint	Berdebu	Tidak	Terkirim	00,05	Percobaan masuk
5	Fingerprint	Basah	Tidak	Tidak	-	Tidak Terbaca
6	Fingerprint	Basah	Tidak	Tidak	-	Tidak Terbaca
7	Fingerprint	Normal	Berhasil	Terkirim	03,32	Pintu Terbuka
8	Fingerprint	Normal	Berhasil	Terkirim	02,56	Pintu Terbuka
9	Fingerprint	Normal	Berhasil	Terkirim	02,63	Pintu Terbuka
10	Fingerprint	Berdebu	Tidak	Tidak	-	Tidak Terbaca
11	Fingerprint	Berdebu	Berhasil	Terkirim	02,64	Pintu terbuka
12	Fingerprint	Basah	Tidak	Terkirim	00,04	Percobaan masuk
13	Fingerprint	Normal	Berhasil	Terkirim	02,70	Pintu Terbuka
14	Fingerprint	Normal	Berhasil	Terkirim	03,36	Pintu Terbuka
15	Fingerprint	Normal	Berhasil	Terkirim	02,65	Pintu Terbuka
16	Fingerprint	Basah	Tidak	Tidak	-	Tidak Terbaca
17	Fingerprint	Berdebu	Tidak	Terkirim	00,02	Percobaan masuk
18	Fingerprint	Basah	Tidak	Tidak	-	Tidak Terbaca
19	Fingerprint	Normal	Berhasil	Terkirim	03,07	Pintu Terbuka
20	Fingerprint	Normal	Berhasil	Terkirim	03,05	Pintu Terbuka
21	Fingerprint	Normal	Berhasil	Terkirim	02,91	Pintu Terbuka
22	Fingerprint	Berdebu	Tidak	Terkirim	00,02	Percobaan masuk
23	Fingerprint	Basah	Tidak	Tidak	-	Tidak Terbaca
24	Fingerprint	Berdebu	Tidak	Terkirim	00,03	Percobaan masuk
25	Fingerprint	Normal	Berhasil	Terkirim	03,81	Pintu Terbuka
26	Fingerprint	Normal	Berhasil	Terkirim	02,69	Pintu Terbuka
27	Fingerprint	Normal	Berhasil	Terkirim	02,50	Pintu Terbuka
28	Fingerprint	Berdebu	Tidak	Terkirim	00,02	Percobaan masuk
29	Fingerprint	Basah	Tidak	Tidak	-	Tidak Terbaca
30	Fingerprint	Basah	Tidak	Tidak	-	Tidak Terbaca

proses pembukaan kunci pintu. Hal ini menunjukkan bahwa sistem mampu memberikan peringatan dini kepada pengguna ketika terjadi percobaan akses yang tidak terotorisasi.

Sebaliknya, pada kondisi sidik jari basah, sensor fingerprint dalam beberapa percobaan tidak dapat membaca data sidik jari dengan baik, sehingga proses autentikasi tidak berjalan dan notifikasi Telegram tidak terkirim. Kondisi ini menunjukkan bahwa keberhasilan pengiriman notifikasi sangat bergantung pada proses pembacaan awal oleh sensor fingerprint. Meskipun terdapat keterbatasan pada kondisi tertentu, secara keseluruhan sistem notifikasi Telegram telah berfungsi efektif dalam memberikan informasi akses berhasil maupun peringatan percobaan masuk, sehingga mendukung penerapan sistem keamanan pintu berbasis IoT yang responsif dan informatif.



(a) (b)

Gambar 9. Notifikasi Aplikasi Telegaram (a) Ketika ID dan Passwod benar (b) Ketika ID dan Passwod Salah

4.4. Diskusi

Hasil pengujian menunjukkan bahwa sistem kontrol akses pintu berbasis IoT yang dikembangkan mampu menjalankan fungsi autentikasi dan pemantauan akses sesuai dengan rancangan. Parameter kinerja sistem yang mencakup autentikasi fingerprint, keypad, dan notifikasi Telegram dirangkum pada Tabel 5 sebagai dasar analisis diskusi ini. Autentikasi sidik jari bekerja optimal pada kondisi jari normal, namun performanya menurun pada kondisi basah dan berdebu. Hal ini tercermin dari nilai TAR sebesar 56,7% dan FRR sebesar 43,3%, di mana seluruh kejadian penolakan berasal dari kondisi jari yang tidak ideal. Temuan ini menegaskan bahwa kualitas citra sidik jari dan faktor lingkungan memiliki pengaruh signifikan terhadap keandalan autentikasi biometrik.

Dari sisi keamanan, pengujian sidik jari tidak terdaftar menunjukkan bahwa sistem mampu menolak seluruh percobaan akses yang tidak sah, dengan nilai FAR sebesar 0% pada seluruh pengujian. Hasil ini mengindikasikan bahwa meskipun sistem masih mengalami keterbatasan dalam kenyamanan pengguna pada kondisi tertentu, mekanisme autentikasi fingerprint tetap efektif dalam mencegah akses tidak terotorisasi. Dengan demikian, sistem lebih mengutamakan aspek keamanan dibandingkan toleransi terhadap kondisi input yang buruk.

Keberadaan keypad sebagai metode autentikasi alternatif terbukti mampu mengatasi keterbatasan autentikasi biometrik. Seluruh pengujian menggunakan PIN yang benar berhasil membuka kunci, sementara seluruh PIN yang salah berhasil ditolak oleh sistem. Kinerja ini menunjukkan bahwa autentikasi keypad memiliki stabilitas tinggi dan dapat berfungsi sebagai fallback mechanism yang andal. Pendekatan ini memperkuat konsep mekanisme autentikasi berlapis berbasis kondisi, di mana sistem tidak sepenuhnya bergantung pada satu metode autentikasi saja. Integrasi notifikasi Telegram memungkinkan sistem memberikan informasi akses dan peringatan percobaan masuk secara real-time, dengan tingkat keberhasilan pengiriman sebesar 73,3%. Kegagalan pengiriman notifikasi sebagian besar terjadi pada kondisi sidik jari basah, ketika sensor tidak mampu membaca data sehingga proses autentikasi tidak berjalan. Variasi waktu tunda pengiriman notifikasi juga dipengaruhi oleh kondisi jaringan Wi-Fi. Meskipun demikian, hasil pengujian menunjukkan bahwa sistem telah mampu mendukung fungsi pemantauan jarak jauh secara efektif dalam skenario pengujian terbatas. Untuk meningkatkan keandalan sistem, pengujian lanjutan dengan jumlah pengguna yang lebih besar, variasi kondisi lingkungan yang lebih ekstrem, serta optimasi sensor dan mekanisme komunikasi data masih diperlukan.

Tabel 5. Keseluruhan dari Parameter Kinerja Sistem

Parameter	**Nilai**
Total uji fingerprint terdaftar	30 percobaan
True Acceptance Rate (TAR)	56,7% (17 dari 30 percobaan)

Parameter	Nilai
False Rejection Rate (FRR)	43,3% (13 dari 30 percobaan)
Total uji fingerprint tidak terdaftar	30 percobaan
False Acceptance Rate (FAR)	0% (0 dari 30 percobaan)
Keberhasilan keypad (PIN benar)	100% (15 dari 15 percobaan)
Keberhasilan notifikasi Telegram	73,3% (22 dari 30 percobaan)

5. KESIMPULAN

Penelitian yang dilakukan berhasil merancang dan mengimplementasikan sistem keamanan pintu berbasis IoT dengan mekanisme autentikasi berlapis yang mengintegrasikan sensor fingerprint sebagai metode utama dan keypad sebagai metode alternatif. Sistem ini dilengkapi dengan fitur notifikasi Telegram untuk memberikan informasi akses pintu secara real-time kepada pengguna, sehingga meningkatkan aspek keamanan dan pemantauan jarak jauh.

Hasil pengujian menunjukkan bahwa autentikasi fingerprint memiliki kinerja yang baik pada kondisi jari normal, namun mengalami penurunan performa pada kondisi jari basah dan berdebu akibat menurunnya kualitas citra sidik jari yang diterima sensor. Meskipun demikian, sistem secara konsisten mampu menolak seluruh upaya akses dari sidik jari yang tidak terdaftar dalam skenario pengujian yang dilakukan. Sementara itu, autentikasi berbasis keypad menunjukkan kinerja yang stabil dalam memverifikasi PIN yang benar maupun menolak PIN yang salah, sehingga efektif digunakan sebagai metode autentikasi cadangan ketika autentikasi biometrik mengalami kegagalan.

Pengujian notifikasi Telegram menunjukkan bahwa sistem mampu mengirimkan informasi akses pintu dan peringatan percobaan masuk dengan waktu tunda yang relatif singkat pada sebagian besar kondisi pengujian. Namun, pada kondisi tertentu seperti kegagalan pembacaan sidik jari akibat kelembapan, pengiriman notifikasi tidak selalu berhasil, yang mengindikasikan adanya keterbatasan pada tahap akuisisi data awal. Secara keseluruhan, sistem yang diusulkan telah berfungsi sesuai dengan tujuan perancangan dan menunjukkan keseimbangan antara keamanan, ketersediaan, dan kemudahan pemantauan, meskipun pengembangan lanjutan masih diperlukan untuk meningkatkan keandalan sistem pada berbagai kondisi lingkungan.

UCAPAN TERIMA KASIH

Terima kasih kepada Universitas Ahmad Dahlan dan Tim ESPERG yang telah memberi dukungan terhadap penelitian ini.

DAFTAR PUSTAKA

[1] R. H. Tidar, A. Madramsyah, H. A. D. Rimbawa, *et al*. Design and development of an IoT-based archive room security system integrating RFID and fingerprint authentication for military document protection. *Jurnal Mandiri IT* 2025;14:198–207. doi: 10.35335/mandiri.v14i1.440.

[2] M. A. Khan and K. Salah. IoT security: Review, blockchain solutions, and open challenges. *Future Generation Computer Systems* 2018;82:395–411. doi: 10.1016/j.future.2017.11.022.

[3] A. A. Zainuddin, Ammar Daniel Abd Rahman, Rizal Mohd Nor, *et al*. Innovative IoT Smart Lock System: Enhancing Security with Fingerprint and RFID Technology. *Malaysian Journal of Science and Advanced Technology* 2024;4:360–365. doi: 10.56532/mjsat.v4i4.335.

[4] M. Wahyu Salfian. Design of Door Security System using Rfid Based on IoT at Stmik Kaputama. *Journal of Artificial Intelligence and Engineering Applications (JAIEA)* 2025;5:604–610. doi: 10.59934/jaiea.v5i1.1367.

[5] S. Uppuluri and G. Lakshmeeswari. Review of Security and Privacy-Based IoT Smart Home Access Control Devices. *Wireless Personal Communications* 2024;137:1601–1640. doi: 10.1007/s11277-024-11405-8.

[6] D. Celestine. Smart Lock Systems: An Overview. *International Journal of Computer Applications* 2020;177:40–43. doi: 10.5120/ijca2020919882.

[7] X. Zhao, B. Zhong, and Z. Cui. Design of a Decentralized Identifier-Based Authentication and Access Control Model for Smart Homes. *Electronics* 2023;12:3334. doi: 10.3390/electronics12153334.

[8] W. Yang, S. Wang, N. M. Sahri, *et al*. Biometrics for Internet-of-Things Security: A Review. *Sensors* 2021;21:6163. doi: 10.3390/s21186163.

[9] W. Yang, S. Wang, J. Hu, *et al*. Security and Accuracy of Fingerprint-Based Biometrics:

A Review. *Symmetry* 2019;11:141. doi: 10.3390/sym11020141.

[10] R. W. Tambunan, A. A. Ar-Rafif, and M. Galina. Multi-Security System Based on RFID Fingerprint and Keypad to Access the Door. *ELKHA* 2022;14:125. doi: 10.26418/elkha.v14i2.57735.

[11] S. Budiyanto, F. Artadima Silaban, L. Medriavin Silalahi, *et al*. The automatic and manual railroad door systems based on IoT. *Indonesian Journal of Electrical Engineering and Computer Science* 2021;21:1847. doi: 10.11591/ijeecs.v21.i3.pp1847-1855.

[12] R. Fitriyan and S. Syafii. Development design of an IoT-based smart home monitoring system with security features. *Indonesian Journal of Electrical Engineering and Computer Science* 2024;34:788. doi: 10.11591/ijeecs.v34.i2.pp788-794.

[13] M. Khudhair Al-Gburi and L. Ali Abdul-Rahaim. Secure smart home automation and monitoring system using internet of things. *Indonesian Journal of Electrical Engineering and Computer Science* 2022;28:269. doi: 10.11591/ijeecs.v28.i1.pp269-276.

[14] M. Husni, H. T. Ciptaningtyas, R. R. Hariadi, *et al*. Integrated smart door system in apartment room based on internet. *TELKOMNIKA (Telecommunication Computing Electronics and Control)* 2019;17:2747. doi: 10.12928/telkomnika.v17i6.12322.

[15] W. A. Jabbar, T. K. Kian, R. M. Ramli, *et al*. Design and Fabrication of Smart Home With Internet of Things Enabled Automation System. *IEEE Access* 2019;7:144059–144074. doi: 10.1109/ACCESS.2019.2942846.

[16] O. Taiwo and A. E. Ezugwu. Internet of Things-Based Intelligent Smart Home Control System. *Security and Communication Networks* 2021;2021:1–17. doi: 10.1155/2021/9928254.

[17] Nurmuhlisa, A. Fauzi, and H. Sembiring. Internet-Based Smart Door Design of Things (IOT) with Visitor Access Controller Indoor. *Journal of Artificial Intelligence and Engineering Applications (JAIEA)* 2024;4:109–116. doi: 10.59934/jaiea.v4i1.566.

[18] T. C. H. Rhunn, A. F. M. Raffei, and N. S. A. Rahman. Internet of Things (IoT) Based Door Lock Security System. , in *2021 International Conference on Software Engineering & Computer Systems and 4th International Conference on Computational Science and Information Management (ICSECS-ICOCSIM)*, Pekan, Malaysia: IEEE, Aug. 2021, 6–9. doi: 10.1109/ICSECS52883.2021.00008.

[19] S. KAYA, E. AŞKAR AYYILDIZ, and M. AYYILDIZ. SMART DOOR LOCK DESIGN WITH INTERNET OF THINGS. *International Journal of 3D Printing Technologies and Digital Industry* 2022;6:201–206. doi: 10.46519/ij3dptdi.1074468.

[20] M. A. Al Rakib, M. M. Rahman, S. Uddin, *et al*. Fingerprint Based Smart Home Automation and Security System. *European Journal of Engineering and Technology Research* 2022;7:140–145. doi: 10.24018/ejeng.2022.7.2.2745.

[21] P. Shirisha, G. Satish Kumarr, K. Shivanjan, *et al*. IoT based wifi fingerprint door lock system with raspberry pi & webcam. *MATEC Web of Conferences* 2024;392:01066. doi: 10.1051/matecconf/202439201066.

[22] G. Sarbishaei, A. Masoud Aminian Modarres, F. Jowshan, *et al*. Smart Home Security: An Efficient Multi-Factor Authentication Protocol. *IEEE Access* 2024;12:106253–106272. doi: 10.1109/ACCESS.2024.3437294.

[23] C. N. S. V. Kumar, V. B. M, N. R, *et al*. Real Time Door Security System With Three Point Authentication. , in *2021 4th International Conference on Recent Trends in Computer Science and Technology (ICRTCST)*, Jamshedpur, India: IEEE, Feb. 2022, 228–233. doi: 10.1109/ICRTCST54752.2022.9782004.

[24] A. A. Zainuddin, Ammar Daniel Abd Rahman, Rizal Mohd Nor, *et al*. Innovative IoT Smart Lock System: Enhancing Security with Fingerprint and RFID Technology. *Malaysian Journal of Science and Advanced Technology* 2024;360–365. doi: 10.56532/mjsat.v4i4.335.

[25] A. T, B. Surekha, P. Subba Rao, *et al*. Arduino Based Secured Access Control in Smart Homes by Implementing Anomaly Detection in Fingerprint - Based Door Lock and Realtime Monitoring with OpenCV. , in *2024 International Conference on Sustainable Communication Networks and Application (ICSCNA)*, Theni, India: IEEE, Dec. 2024, 161–166. doi: 10.1109/ICSCNA63714.2024.10864215.

[26] M. A. Khan, K. Nisar, E. Lodhi, *et al*. Prototype Model of an IoT-based Digital and Smart Door Locking System with Enhanced Security. , in *2022 14th International Conference on Mathematics, Actuarial Science, Computer Science and Statistics*

(MACS), Karachi, Pakistan: IEEE, Nov. 2022, 1–7. doi: 10.1109/MACS56771.2022.10023385.