SENAFTI
SEMINAR NASIONAL MAHASISWA
FAKULTAS TEKNOLOGI INFORMASI

6th Seminar Nasional Mahasiswa Fakultas Teknologi Informasi (SENAFTI)
20 September 2025 – Jakarta, Indonesia
Volume 4, Nomor 2, September 2025 - ISSN 2962-8628 (*online*)

SISTEM KEAMANAN PINTU DENGAN 2 LANGKAH AUTENTIKASI BERBASIS IOT

Ragil Prabawijaya[1*], Jan Everhard Riwurohi[2], Irawan[3], Yani Prabowo[4]

[1,2,3,4] Program Studi Sistem Komputer, Fakultas Teknologi Informasi, Universitas Budi Luhur, Jakarta, Indonesia

Email: [1*]2013500083@student.budiluhur.ac.id, [2] jan.everhard@budiluhur.ac.id, [3]irawan@budiluhur.ac.id, [4]yani.prabowo@budiluhur.ac.id
(* : corresponding author)

Abstrak- Keamanan ruang fisik merupakan aspek yang sangat penting di berbagai lingkungan seperti laboratorium, kantor, gudang, dan ruang penyimpanan yang menyimpan data atau peralatan bernilai tinggi. Tujuan penelitian ini adalah mengembangkan sistem kontrol akses yang menggabungkan password dan fingerprint, dengan tambahan notifikasi instan melalui Telegram dan pencatatan aktivitas di Google Sheets agar pemantauan keamanan lebih praktis. Penelitian ini menggunakan metode perancangan dan pengujian prototipe sistem kontrol akses berbasis mikrokontroler dengan pendekatan eksperimen. Sistem kontrol akses konvensional, seperti kunci mekanik, memiliki keterbatasan karena rentan hilang, diduplikasi, atau disalahgunakan sehingga tidak lagi mampu memberikan perlindungan maksimal. Untuk menjawab tantangan ini, penelitian ini merancang sistem kontrol akses berbasis mikrokontroler dengan metode autentikasi ganda yang menggabungkan *password* dan *fingerprint* sebagai bentuk *two-factor authentication* demi meningkatkan lapisan keamanan. Sistem menggunakan Arduino Mega sebagai pengendali utama autentikasi dan ESP32 sebagai modul konektivitas jaringan untuk mengirimkan notifikasi secara *real-time* melalui aplikasi Telegram sekaligus mencatat seluruh aktivitas ke Google Sheets sebagai basis data daring. Tiga profil pengguna dengan *password* dan identitas sidik jari yang telah didaftarkan sebelumnya diterapkan dalam sistem ini. Jika autentikasi berhasil, akses pintu akan diberikan secara otomatis, sedangkan apabila terjadi kesalahan *input password* atau *fingerprint* lebih dari tiga kali berturut-turut, sistem akan memblokir akses, mengaktifkan buzzer, mengirimkan peringatan ke Telegram, serta menambahkan *log* pada Google Sheets untuk dokumentasi dan pemantauan lebih lanjut. Selain itu, sistem juga dilengkapi sensor ultrasonik yang mampu mendeteksi upaya pembobolan pintu secara fisik tanpa autentikasi sah. Sistem menunjukkan akurasi autentikasi 98% dengan *respons* <2 detik, notifikasi *real-time* ke Telegram, dan pencatatan otomatis di *Google Sheets*. Fitur penguncian dan deteksi pembobolan bekerja efektif, meski sistem bergantung pada koneksi internet. Secara keseluruhan, kinerja cepat, akurat, dan layak diterapkan pada fasilitas dengan keamanan tinggi.

Kata Kunci: Arduino Mega, ESP32, Keypad, Fingerprint, Password, Notifikasi

DOOR SECURITY SYSTEM WITH TWO-STEP AUTHENTICATION BASED ON IOT

Abstract- *Physical space security is a crucial aspect in various environments such as laboratories, offices, warehouses, and storage rooms that hold valuable data or equipment. The purpose of this study is to develop an access control system that combines password and fingerprint authentication, complemented by instant notifications via Telegram and activity logging in Google Sheets to facilitate practical security monitoring. Conventional access control systems, such as mechanical keys, have limitations because they are prone to being lost, duplicated, or misused, thus failing to provide maximum protection. To address this challenge, this study designed a microcontroller-based access control system using dual authentication methods—password and fingerprint—as a form of two-factor authentication to enhance security layers. The system employs Arduino Mega as the primary controller for authentication and ESP32 as the network connectivity module to send real-time notifications through the Telegram application and record all activities in Google Sheets as an online database. Three user profiles with pre-registered passwords and fingerprints were implemented in the system. When authentication is successful, door access is granted automatically; however, if incorrect password or fingerprint entries occur more than three times consecutively, the system blocks access, activates a buzzer, sends a security alert to Telegram, and logs the event in Google Sheets for further monitoring and documentation. Additionally, the system is equipped with an ultrasonic sensor to detect unauthorized physical attempts to breach the door. The system demonstrated an authentication accuracy of 98% with a response time of less than two seconds, real-time Telegram notifications, and automatic data logging to Google Sheets. Locking and intrusion detection features functioned effectively, although the system depends on an internet connection. Overall, the system performed quickly, accurately, and is feasible for application in high-security facilities.*

Keywords: *Arduino Mega, ESP32, Keypad, Fingerprint, Password, Notification*

1. PENDAHULUAN

Perkembangan teknologi yang semakin pesat telah mendorong inovasi dalam sistem keamanan, khususnya pada lokasi yang menyimpan aset bernilai tinggi seperti laboratorium, pusat data, perkantoran, dan fasilitas umum[1]. Penelitian-penelitian sebelumnya umumnya hanya menggunakan satu metode autentikasi, seperti password atau kartu RFID, sehingga tingkat keamanan masih rendah karena mudah diretas, hilang, atau disalahgunakan, meski metode konvensional seperti kunci mekanik dan kartu akses masih sering dipakai karena biaya yang relatif rendah dan kemudahan penggunaannya, cara ini memiliki kekurangan, di antaranya rawan hilang, dicuri, atau disalahgunakan. Selain itu, kebanyakan sistem lama tidak memiliki fitur pencatatan riwayat akses secara otomatis, sehingga mempersulit proses investigasi ketika terjadi pelanggaran keamanan.

Penelitian ini merancang sebuah sistem keamanan pintu dengan mekanisme autentikasi ganda (two-factor authentication) yang memadukan verifikasi biometrik sidik jari dengan input kata sandi melalui keypad. Sistem ini dikendalikan oleh Arduino Mega yang berfungsi memproses masukan dari sensor, menampilkan informasi pada layar LCD, serta mengoperasikan relay dan buzzer[2]. Untuk mendukung konektivitas dan pemantauan jarak jauh, digunakan modul ESP32 DevKit v1 yang terhubung dengan Arduino melalui komunikasi serial, mengirim notifikasi ke aplikasi Telegram, dan menyimpan seluruh data aktivitas pengguna di Google Sheets berbasis cloud yang dapat diakses kapan saja secara online.

Untuk meningkatkan perlindungan fisik, sistem ditambahkan sensor ultrasonik yang dapat mendeteksi upaya pembobolan di sekitar pintu. Apabila terdeteksi, sistem akan mengirim peringatan secara real-time dan merekam insiden sebagai pelanggaran[3]. Kombinasi sensor biometrik, mikrokontroler, layanan cloud, dan aplikasi mobile membuat sistem ini menjadi solusi keamanan yang modern, ekonomis, fleksibel, serta mampu mendukung pengawasan jarak jauh yang relevan dengan kebutuhan masa kini.

2. METODE PENELITIAN

2.1 Jenis Penelitian

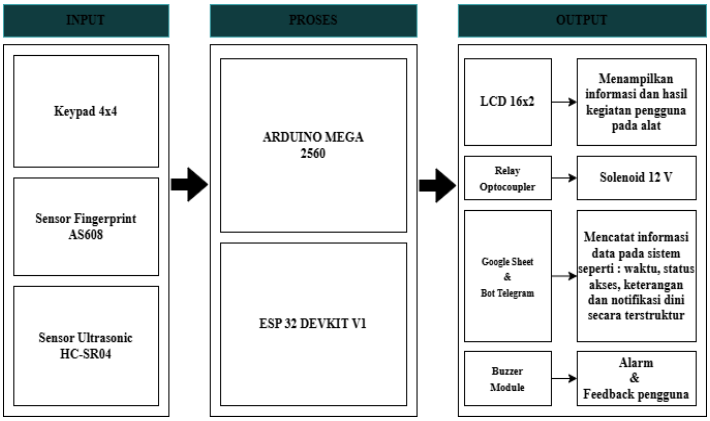
Penelitian ini menggunakan pendekatan eksperimen, di mana sistem keamanan pintu dengan autentikasi ganda menggabungkan kata sandi dan sidik jari diuji secara langsung untuk menilai tingkat kinerja, ketepatan, dan reliabilitasnya. Data yang dianalisis bersifat primer, diperoleh langsung dari hasil kerja sistem selama pengujian, dengan kata sandi yang telah ditanamkan pada mikrokontroler dan data biometrik yang tersimpan di modul sensor sidik jari. Proses uji dilakukan untuk mengamati respons sistem terhadap masukan pengguna, baik pada kondisi akses diizinkan maupun ditolak, sehingga dapat dianalisis kemampuan autentikasi secara real time serta efektivitas kolaborasi antara komponen perangkat keras dan perangkat lunak.

2.2 Penerapan Metode

a) Metode eksperimen dalam penelitian ini diterapkan melalui serangkaian langkah terstruktur guna memastikan sistem keamanan berjalan. Proses tersebut mencakup tahapan sebagai berikut:
b) Tahap persiapan dengan memprogram kata sandi pada Arduino Mega, mendaftarkan sidik jari pada modul sensor fingerprint, serta merangkai komponen pendukung seperti keypad, LCD, relay, buzzer, sensor ultrasonik, dan modul ESP32.
c) Uji autentikasi menggunakan masukan yang benar maupun salah untuk menilai tingkat keberhasilan, mekanisme penolakan, konsistensi, dan waktu respon sistem.
d) Proses pemantauan dan pencatatan melalui verifikasi notifikasi real time pada aplikasi Telegram serta pemeriksaan log aktivitas yang tersimpan di Google Sheets.
e) Uji keamanan tambahan dengan memanfaatkan sensor ultrasonik untuk mendeteksi percobaan pembobolan yang disimulasikan.
f) Analisis data dari hasil pengujian guna mengevaluasi ketepatan autentikasi, stabilitas kinerja, serta efektivitas integrasi antara perangkat keras dan perangkat lunak.

2.3 Diagram Blok

Diagram ini menyajikan ringkasan keterkaitan antara input, proses, dan output pada sistem. Gambar 1 menampilkan alur blok diagram yang menggambarkan susunan serta interaksi komponen perangkat keras dalam menjalankan fungsi sistem.

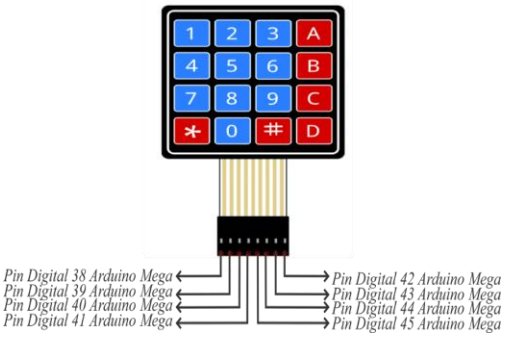


Gambar 1. Diagram Blok

2.4 Perancangan Sistem

a. Keypad 4x4

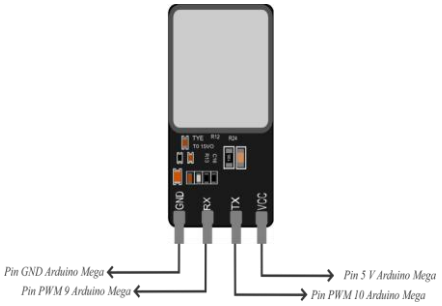
Keypad 4x4 adalah perangkat input yang terdiri dari 16 tombol yang tersusun dalam konfigurasi matriks 4 baris dan 4 kolom. Setiap tombol terletak di persimpangan antara satu baris dan satu kolom. Tidak ada komponen aktif seperti IC atau LED yang memerlukan catu daya tambahan. Keypad 4x4 berperan sebagai alat input yang digunakan untuk memasukkan kode akses ke dalam sistem [4]. Pada Gambar 2 menampilkan rangkaian perangkat keras dari Keypad 4x4.



Gambar 2. Rangkaian Keypad 4x4

b. Sensor Fingerprint AS608

Sensor Fingerprint AS608 merupakan sensor sidik jari yang sering diterapkan dalam sistem pengenalan dan verifikasi identitas. Sensor ini berfungsi dengan cara memindai dan memverifikasi pola sidik jari seseorang untuk memastikan bahwa orang yang mencoba mengakses sistem atau perangkat sudah terdaftar. Jika pemindaian berhasil, maka kunci pintu akan terbuka melalui solenoid *door lock* [2]. AS608 dilengkapi dengan berbagai fitur yang menjadikannya ideal untuk aplikasi keamanan, seperti sistem kontrol akses pintu, absensi, dan perangkat lain yang membutuhkan verifikasi identitas secara biometri. Pada Gambar 3 menampilkan rangkaian perangkat keras dari *Fingerprint AS608*.



Gambar 3. Rangkaian sensor *Fingerprint AS608*

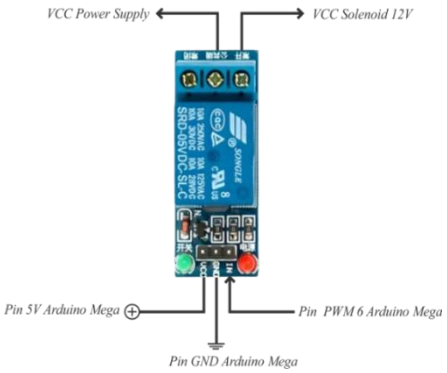
c. Sensor Ultrasonic HC-SR04

Sensor ultrasonik HC-SR04 merupakan sensor pengukur jarak yang bekerja dengan memanfaatkan gelombang suara ultrasonik. Sensor ini banyak digunakan dalam berbagai aplikasi, seperti sistem robotika, alat bantu parkir, pengukuran ketinggian, serta sistem keamanan yang membutuhkan kemampuan deteksi keberadaan objek atau pengukuran jarak secara non-kontak. HC-SR04 menggunakan gelombang ultrasonik dengan frekuensi 40 kHz untuk mendeteksi keberadaan objek di depannya [5] Prinsip kerjanya adalah dengan memancarkan gelombang suara melalui *transmitter*, kemudian mendeteksi pantulan gelombang tersebut melalui *receiver***.**

Gambar 4. Rangkaian Sensor Ultrasonic HC-SR04

d. Relay Module Optocoupler

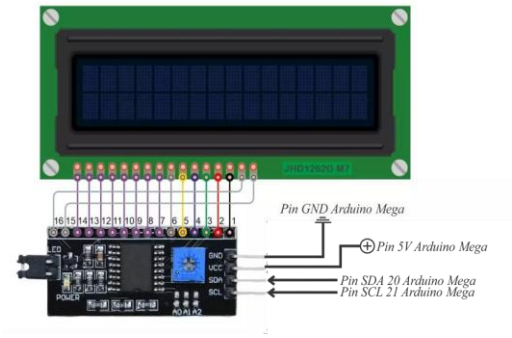
Relay module dengan optocoupler adalah komponen elektronik yang memungkinkan pengendalian perangkat bertegangan tinggi atau sirkuit lain dengan memisahkan sirkuit kontrol dan sirkuit daya tinggi, untuk mencegah kerusakan pada komponen kontrol[6]. Optocoupler berfungsi untuk mengalihkan sinyal dari mikrokontroler ke relay tanpa menghubungkan langsung sirkuit kontrol dengan beban bertegangan tinggi[7].



Gambar 5. Rangkaian Relay Module Optocoupler

e. LCD 16x2

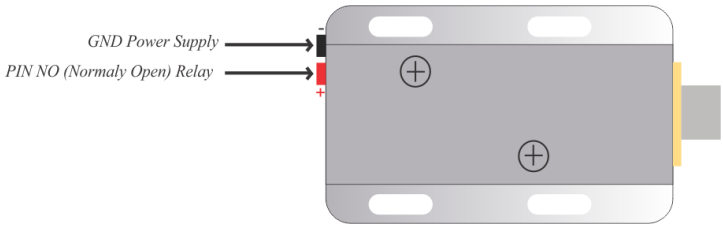
LCD 16x2 berperan sebagai media tampilan utama yang menyampaikan informasi kepada pengguna selama sistem berjalan. Modul ini terdiri dari dua baris dan enam belas kolom karakter, dengan tampilan latar berwarna hijau dan huruf berwarna hitam, serta dilengkapi lampu latar (backlight) untuk meningkatkan keterbacaan dalam kondisi cahaya minim. PIN Layar LCD dengan I2C menunjukkan informasi mengenai keadaan sistem [8]. LCD 16×2 biasanya memerlukan 16 pin untuk kontrolnya, yang bisa sangat boros. Oleh karena itu, digunakan driver khusus yang memungkinkan LCD dikendalikan melalui modul I2C (Inter-Integrated Circuit).



Gambar 6. Rangkaian LCD 16x2

f. Solenoid 12 V

Solenoid pintu 12V adalah komponen elektronik yang digunakan untuk mengendalikan mekanisme pembukaan atau penutupan pintu dengan menggunakan daya listrik 12 volt. Selenoid pintu bekerja dengan prinsip elektromagnetik, di mana medan magnet yang dihasilkan saat arus listrik mengalir melalui selenoid akan menarik atau mendorong bagian tertentu dari mekanisme pintu, sehingga membuka atau menutup pintu[9]. Solenoid door ini berfungsi untuk mengunci pintu secara otomatis, menggantikan peran kunci tradisional saat pintu ingin dibuka atau ditutup[10].



Gambar 7. Rangkaian Solenoid 12V

g. ESP32 Devkit V1

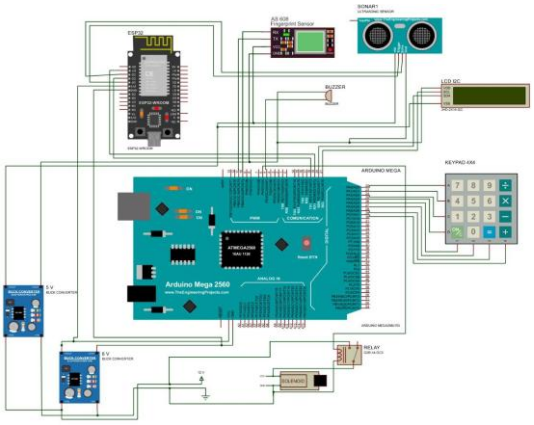
ESP32 Devkit V1 merupakan mikrokontroler yang diperkenalkan oleh Espressif Systems dan merupakan penerus dari mikrokontroler ESP8266. Mikrokontroler ini menawarkan modul WiFi on-chip yang dapat digunakan untuk membuat sistem aplikasi Internet of Things dengan mudah, ESP32 berfungsi sebagai pengolah data yang diperoleh dari sensor, kemudian mengirimkan data tersebut ke *Google Spreadsheet.*

Gambar 8. Rangkaian ESP32 Devkit V1

2.5 Perancangan Sistem

Gambar 9 menampilkan rangkaian sistem pengamanan pintu berbasis IoT ini memadukan sensor sidik jari AS608, Arduino Mega 2560, dan Keypad 4x4 sebagai media verifikasi akses. ESP32 berfungsi mengirim

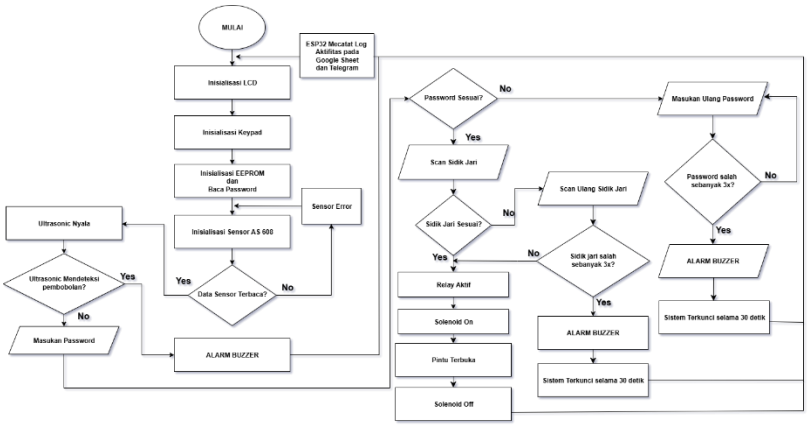
notifikasi melalui Telegram, sementara Relay Optocoupler bersama Solenoid 12V mengoperasikan mekanisme pembukaan pintu. Komponen pendukung seperti sensor ultrasonik, LCD, buzzer, serta modul daya turut digunakan, dengan seluruh data pengguna direkam secara real-time di Google Sheets.



Gambar 9. Rangakaian Keseluruhan Sistem

2.6 Flowchart Keseluruhan

Flowchart ini menjelaskan tahapan kerja sistem keamanan pintu. Saat perangkat dihidupkan, mikrokontroler menjalankan proses inisialisasi, termasuk mengaktifkan komunikasi serial dengan sensor AS608 dan memuat data sidik jari yang tersimpan. Pengguna diminta memasukkan kata sandi 4 digit, kesalahan hingga tiga kali akan memicu alarm dan mengunci sistem selama 30 detik. Jika kata sandi benar, sistem melanjutkan ke tahap verifikasi sidik jari dengan aturan kesalahan yang sama. Apabila kedua verifikasi berhasil, mikrokontroler mengaktifkan relay untuk menyalurkan arus ke solenoid sehingga pintu terbuka. Dari sisi dalam gudang, pintu dapat dibuka hanya dengan menekan switch tanpa perlu memasukkan kata sandi.. Flowchart tersebut dapat dilihat pada Gambar 10.



Gambar 10. Flowchart Keseluruhan

Gambar diatas ini merupakan flowchart keseluruhan sistem yang sudah dijelaskan sebelumnya.

3. HASIL DAN PEMBAHASAN

3.1 Hasil Rancangan Alat

Pada Gambar 11. Bisa dilihat merupakan visual dari alat keseluruhan, yang mana pada bagian depan alat terdapat komponen interface untuk komunikasi antara sistem dan pengguna,

Gambar 11. Hasil rancangan Alat

3.2 Pengujian sensor Fingerprint AS608

Tabel 1. Pengujian sensor *Fingerprint AS608*

No. ID	Jari Yang Terdaftar	Jari Yang Dipindai	Status Pencocokan	Output Sistem
1	Ibu Jari	Ibu Jari	Cocok	Relay Aktif
2	Jari Telunjuk	Jari Telunjuk	Cocok	Relay Aktif
3	Jari Tengah	Jari Tengah	Cocok	Relay Aktif
4	Ibu Jari	Jari Telunjuk	Tidak Cocok	Akses ditolak
5	Jari Telunjuk	Ibu Jari	Tidak Cocok	Akses ditolak
6	Jari Tengah	Jari Kelingking	Tidak Cocok	Akses ditolak

Pada tabel 1 terdapat pengujian pada sensor Fingerprint AS 608 jika sidik jari yang dipindai sesuai dengan profile_password yang dimasukan. Jadi sidik jari yang dipindai harus sesuai dengan password yang di masukan, begitu pula pada sidik jari yang tidak terdaftar maka sistem akan menolak permintaan akses dari sidik jari yang tidak sesuai permintaan dan tidak terdaftar.

3.3 Pengujian Keypad 4x4

Tabel 2. Pengujian keypad 4x4

No.	Input Yang dimasukan	Respon Pada LCD	Status Validasi
1	1111	"Pass Accepted"	Lanjut Ke Fingerprint
2	2222	"Pass Accepted"	Lanjut Ke Fingerprint
3	3333	"Pass Accepted"	Lanjut Ke Fingerprint
4	1234	"Wrong Password"	Ditolak
5	5678	"Wrong Password"	Ditolak

Sesuai dengan data pengujian pada tabel 2 di atas bisa dikatakan bahwa keypad 4x4 bekerja sesuai dengan algoritma dan juga sesuai dengan fungsinya pada sistem ini. data EEPROM yang digunakan dan membaca password ada 3 profile yang disimpan secara permanen, sehingga tetap tersedia meskipun alat dimatikan, EEPROM menyimpan data dalam bentuk byte di alamat tertentu.

3.4 Pengujian Relay dan Solenoid

Tabel 3. Pengujian Relay Dan Solenoid

No.	Hasil Verifikasi	Waktu Relay Aktif (Detik)	Status Solenoid	Keterangan
1	Berhasil	5	Aktif	Pintu Terbuka
2	Gagal	0	Tidak Aktif	Pintu Tetap Terkunci

Dari data pada tabel 3 di atas terlihat jika relay aktif maka pintu terbuka, ini karena solenoid adalah aktuator yang inti besinya berfungsi untuk mengunci pintu, salah satu rangkaian VCC pada solenoid dari power supply di putus dan disambungkan ke pin NO (normally open) relay dan pada pin COM (Common) relay dihubungkan ke output VCC dari power supply, saat relay belum aktif jalur VCC ke solenoid terputus yang berarti solenoid tidak mendapat tegangan (pintu tertutup) dan bila relay aktif makan pin NO dan COM akan terhubung dan mengalirkan tegangan ke solenoid untuk menarik inti sehingga pintu bisa terbuka. Dari pengujian bisa dinyatakan bahwa relay dan solenoid bisa berfungsi dengan baik dan benar.

3.5 Pengujian LCD dan Buzzer

Pada pengujian ini terdapat scenario yang memeiliki output pada masing-masing komponen untuk menyelaraskan logika apa yang sedang berjalan.

Tabel 4. Pengujian *LCD* dan *Buzzer*

Skenario	Pesan Pada LCD	Suara Buzzer
Password Benar	"Pass Accepted"	Mati
Fingerprint Benar	"Fingerprint OK!"	Nyala Pendek
Password Salah	"Wrong Password"	Mati
Fingerprint Gagal	"Finger Wrong"	Mati
Akses Berhasil	"Silahkan Masuk"	Nyala Pendek
Password Error (3x percobaan gagal)	"PASS BLOCKED"	Nyala Panjang
Fingerpprint Error (3x Percobaan gagal)	"FINGER BLOCKED"	Nyala Panjang
Pintu di bobol	"INTRUDER DETECTED"	Nyala Panjang
Password dan fingerprint (BLOKED)	"HUBUNGI DEVELOPER"	Nyala Panjang

Pada data tabel 4 diatas terlihat bahwa LCD dan Buzzer bisa berfungsi sesuai dengan logika yang ada diprogram dan berjalan seperti yang diharapkan.

3.6 Pengujian Ultrasonic HC-SR04

Tabel 5. Pengujian sensor *Ultrasonic HC-SR04*

Jarak Objek (cm)	Status Sistem	Respon Yang Diharapkan	Hasil
>10	Terkunci	Tidak Ada Respon	Sesuai
<10	Terkunci	Buzzer Aktif dan Notifikasi	Sesuai
<10	Terbuka Sah	Tidak Ada Respon	Sesuai
Tidak Objek	Terkunci	Diam	Sesuai

Pada tabel 5 diatas ini merupakan pengujian komponen dari sistem keamanan pintu berbasis mikrokontroler yang memanfaatkan sensor ultrasonik untuk mendeteksi indikasi pembobolan. Saat akses belum terotorisasi dan terdeteksi objek berjarak ≤10 cm tanpa deteksi serupa dalam 10 detik terakhir, sistem menganggapnya sebagai ancaman. Sebagai tindak lanjut, sistem mengirimkan peringatan melalui komunikasi serial, mengirim notifikasi otomatis ke Telegram, dan merekam kejadian tersebut ke dalam database. Berikut adalah tabel hasil pengujian sensor ultrasonik HC-SR04.

4. KESIMPULAN

Hasil pengujian menunjukkan bahwa sistem kontrol akses dengan autentikasi ganda bekerja dengan cepat, rata-rata di bawah dua detik, dan memiliki akurasi mencapai 98%. Notifikasi terkirim secara langsung ke aplikasi Telegram, sementara pencatatan aktivitas berlangsung otomatis di Google Sheets. Mekanisme penguncian setelah tiga kali kesalahan autentikasi serta deteksi pembobolan fisik berjalan efektif, meskipun sistem tetap memerlukan koneksi internet untuk berfungsi optimal. Dengan performa tersebut, sistem ini dapat diterapkan pada fasilitas yang membutuhkan perlindungan tingkat tinggi.

DAFTAR PUSTAKA

[1] N. T. Somantri, Y. B. Zainal, R. Indrayanto, A. Charisma, and F. Haz, "Electron : Jurnal Ilmiah Teknik Elektro Prototipe Sistem Keamanan Buka Pintu dan Jendela Menggunakan Aplikasi Telegram Security System Prototype for Opening Doors and Windows Using the Telegram Application," *Jurnal Ilmiah Teknik Elektro*, vol. 5, no. Prototipe Sistem Keamanan Buka Pintu dan Jendela Menggunakan Aplikasi Telegram, pp. 225–233, Nov. 2024, doi: https://doi.org/10.33019/electron.v5i2.216.

[2] Y. Tama and A. Saputra, "Rancang Bangun Sistem Keamanan Rumah Berbasis IoT (Internet of Things) Menggunakan Arduino Mega 2560 Dengan ESP32," *Jurnal Teknik Informatika Unis*, vol. 10, no. 1, 2022.

[3] D. M. Sepudin and S. Abdullah, "Jurnal Restikom : Riset Teknik Informatika dan Komputer Sistem Keamanan Pintu Rumah Berbasis Internet of Things Berbasis NodeMCU ESP32 dan Telegram A B S T R A K," vol. 4, no. 3, pp. 93–99, 2022, [Online]. Available: https://restikom.nusaputra.ac.id

[4] E. Alfonsius, A. S. Ruitan, and D. Liuw, "Pengembangan Sistem Keamanan Pintu Menggunakan Metode Prototype Berbasis RFID dan Keypad 4x4 dengan Arduino Nano," *Jurnal Ilmiah Informatika dan Ilmu Komputer (JIMA-ILKOM)*, vol. 3, no. 2, pp. 110–123, Sep. 2024, doi: 10.58602/jima-ilkom.v3i2.33.

[5] Handson Technology, "Handson Technology User Guide HC-SR04 Ultrasonic Sensor Module User Guide User Guide: Ultrasonic Sensor V2.0," 2021. [Online]. Available: www.handsontec.com

[6] E. Suhardi Rahman, S. Gunawan Zain, and A. Hidayat Adam, "PENGEMBANGAN SISTEM KEAMANAN PINTU MENGGUNAKAN FINGERPRINT DENGAN SISTEM NOTIFIKASI BERBASIS INTERNET OF THINGS," Makassar, Dec. 2022. doi: https://doi.org/10.59562/metrik.v20i1.5484.

[7] Kurniasih Wahyuni, Rakhman Abdul, and Salamah Irma, "5," *Jurnal Riset Sistem Informasi Dan Teknik Informatika (JURASIK)*, vol. 5, no. Sistem Keamanan Pintu dan Jendela Rumah Berbasih IoT, pp. 266–274, Aug. 2022, doi: https://doi.org/10.30645/jurasik.v5i2.212.

[8] W. Raditya, A. Surahman, A. Budiawan, F. Amanda, N. Dwi Putri, and S. Yudha, "PENERAPAN SISTEM KEAMANAN GERBANG RUMAH BERBASIS TELEGRAM MENGGUNAKAN ESP8266," *Jurnal Teknik dan Sistem Komputer (JTIKOM)*, vol. 3, no. 2, p. 2022.

[9] R. Suwartika and G. Sembada, "Perancangan Sistem Keamanan Menggunakan Solenoid Door Lock Berbasis Arduino Uno pada Pintu Laboratorium di PT. XYZ," *Jurnal E-Komtek (Elektro-Komputer-Teknik)*, vol. 4, no. 1, pp. 62–74, Jun. 2020, doi: 10.37339/e-komtek.v4i1.217.

[10] H. Rayya Bramanta and Y. Santosa, "Rancang Bangun Modul Pengoperasian Motor Induksi dan Beban Resistif Menggunakan Solid State Relay (SSR)," Bandung, Aug. 2024. doi: https://doi.org/10.35313/irwns.v15i1.6197.