# PENGEMBANGAN PURWARUPA SISTEM KONTROL AKSES DAN PRESENSI BERBASIS *RADIO FREQUENCY IDENTIFICATION* (RFID) DAN SIDIK JARI (*FINGERPRINT*) PADA LABORATORIUM TEKNIK ELEKTRO UNIVERSITAS KRISTEN INDONESIA

*[1]Maria Helena Putri Nira, [2]Susilo, [3]Stepanus**
*[1,2,3]Program Studi Teknik Elektro Fakultas Teknik Universitas Kristen Indonesia*
*Jl. Mayjen Sutoyo No.2 Cawang, Jakarta Timur 13630, DKI Jakarta*
[2]susilo.suwarno@uki.ac.id, [3]stepanus@uki.ac.id,
**Corresponding author*: [1]putriniraaaa@gmail.com

**Abstrak**

*Laboratorium sebagai fasilitas akademik membutuhkan sistem kontrol akses dan presensi yang efisien serta aman. Sistem manual yang ada masih rawan kecurangan dan memakan waktu. Penelitian ini merancang dan mengimplementasikan sistem kontrol akses dan presensi berbasis IoT menggunakan RFID dan fingerprint, dilengkapi manajemen waktu serta mekanisme fail-safe. Metode kuantitatif dengan pendekatan model eksperimental dan simulasi berdasarkan sistem nyata. Sistem dikembangkan dengan ESP32 sebagai mikrokontroler utama, RC522 dan R503 sebagai autentikasi kartu dan sidik jari, DS3231 sebagai manajemen waktu, serta MQ2 sebagai mekanisme fail-safe untuk deteksi asap. Output ditampilkan melalui LCD 16×2 I2C dan website monitoring. Hasil pengujian menunjukkan RC522 memiliki akurasi tinggi dalam membaca UID kartu terdaftar, R503 memiliki tingkat penerimaan 0% terhadap user tidak terdaftar dan tingkat penolakan 30% terhadap user terdaftar, DS3231 mampu membatasi akses sesuai jadwal, serta MQ2 bekerja baik dalam mendeteksi asap. Waktu respons interlock cepat dan konsisten dibandingkan website, sehingga interlock lebih stabil dan dapat diandalkan sebagai mekanisme utama dalam keadaan darurat.Dengan demikian, penelitian ini berhasil mengembangkan sistem kontrol akses dan presensi yang efisien, aman, dan terintegrasi IoT.*

**Kata Kunci:** *Kontrol akses, Presensi, Multi-Factor Authentication, Manajemen Waktu, Fail-Safe*

**Abstract**

*Laboratories as academic facilities require efficient and secure access control and attendance systems. Existing manual methods remain vulnerable to fraud and are time-consuming. This study designs and implements an IoT-based access control and attendance system using RFID and fingerprint authentication, complemented by time management and fail-safe mechanisms. A quantitative method with experimental modeling and simulation based on real systems was applied. The prototype was developed with ESP32 as the main microcontroller, RC522 and R503 for card and fingerprint authentication, DS3231 for time management, and MQ2 as a fail-safe smoke detection mechanism. System outputs were displayed through an LCD 16×2 I2C and a monitoring website. Test results show RC522 achieved high accuracy in reading registered card UIDs, R503 recorded 0% acceptance for unregistered users and 30% rejection for registered users, DS3231 successfully restricted access according to schedules, and MQ2 performed reliably in smoke detection. The interlock response time was faster and more consistent than the website, making it more stable and dependable in emergencies. Thus, this research successfully developed an efficient, secure, and IoT-integrated access control and attendance system.*

***Keywords*:** *Access Control, Attendance, Multi-Factor Authentication, Time Management, Fail-Safe*

## PENDAHULUAN

Laboratorium sebagai salah satu fasilitas akademik untuk mendukung proses penelitian dan percobaan menyebabkan akses ke dalam laboratorium harus dikontrol dan presensi kehadiran harus dipantau untuk meningkatkan efektivitas dan keamanan laboratorium. Namun, dalam operasionalnya sistem presensi yang digunakan masih secara manual tentu tidak menutup kemungkinan terjadinya rekayasa kehadiran (titip absen) dengan persentase kecurangan sekitar 60% [1]. Selain itu, tidak adanya kontrol akses membuat tingkat keamanan rendah karena tidak ada mekanisme untuk membatasi siapa saja yang mengakses laboratorium sesuai aturan yang ditetapkan. Presensi manual sendiri sudah tidak relevan dengan era digital saat ini. Presensi manual menggunakan kertas dianggap kurang efisien dan rawan kecurangan [2]. Kontrol akses yang tidak memadai menyebabkan tidak adanya teknik keamanan mendasar yang bisa mengontrol siapa saja yang mengakses laboratorium sesuai aturan dan mekanisme yang sudah ditetapkan [3].

Sebelum melakukan penelitian, peneliti melakukan studi literatur terkait kontrol akses dan sistem presensi. Penelitian berjudul ***A New Model of The Student Attendance Monitoring System Using RFID Technology*** oleh Mutammimul Ula ddk pada *Journal of Physics: Conference Series,* volume 1807, nomor 1 [4]. Mengangkat masalah mengenai presensi manual yang kurang efisien dengan merancang dan menguji prototipe berbasis Arduino dan RFID *reader* untuk melihat kinerja pembacaan dan penyimpanan data presensi. Dengan sistem ini proses presensi menjadi lebih cepat dan langsung tersimpan di database namun, sistem ini memiliki keterbatasan masih menggunakan SFA dan belum terintegrasi IoT dan kontrol akses. Meskipun demikian, hasil penelitian menunjukkan sistem presensi yang dirancang berhasil dan mampu mencatat data presensi secara otomatis ke *database.*

Di tahun 2022, Bukhari dkk melakukan penelitian berjudul ***Rancang Bangun Prototipe Pintu Cerdas Terintegrasi Sistem Absensi Berbasis Mikrokontroler Arduino*** dalam jurnal *Proceeding* Seminar Nasional Politeknik Negeri Lhokseumawe, volume 6, nomor 1, halaman 122-127 [5]. Penelitin ini untuk mengatasi ketiadaan kontrol akses yang terintegrasi presensi yang menyebabkan kurang efisien dan tingkat keamanan rendah melalui perancangan sistem pintu cerdas menggunakan Arduino. Melalui perancangan *hardware, software* serta pengujian, menunjukan sistem mampu mampu menggabungkan fungsi keamanan pintu dan presensi dalam satu perangkat dengan terintegrasi IoT. Namun, sistem ini masih menggunakan SFA sehingga masih rawan kecurangan. Hasil penelitian ini menunjukkan sistem dapat bekerja dengan baik untuk mengontrol pintu dan mencatat presensi kehadiran berdasarkan hasil baca RFID.

Md. Saidur Rahman ddk melakukan penelitian lain berjudul ***Fingerprint Based Biometric Attendance System*** di tahun 2023 pada jurnal *Section A-Research paper of European Chemical Bulletin,* volume 12, nomor S3, halaman 184-190 [6]. Merancang sistem presensi berbasis Arduino Mega 2560 menggunkan modul modul sidik jari, RTC untuk mencatat waktu. Bekerja dengan cara mencocokkan sidik jari dengan yang tersimpan di *database*. Sistem ini juga memungkinkan pengiriman notifikasi SMS kepada orang tua. Namun, penelitian ini belum terintegrasi dengan IoT dan

menggunakan modul tambahan untuk penyimpanan dan pengiriman data. Selain itu, RTC hanya digunakan untuk pencatatan waktu bukan untuk manajemen waktu. Hasil dari penelitian ini mampu melakukan proses identifikasi pengguna, mencatat waktu kehadiran dan mengirim notifikasi SMS kepada orang tua.

Lalu ditahun 2024, Ahmad Anwar Zainuddin dkk juga melakukan penelitian dengan judul ***Innovative IoT Smart Lock System: Enhancing Security with Fingerprint and RFID Technology*** di tahun 2024 dalam *Malaysian Journal of Science and Advanced Technology,* volume 4, nomor 4, halaman 360-365 [7]. Melihat kunci pintu konvensional yang kurang aman, penelitian ini merancang sistem kontrol akses berbasis purwarupa dengan mengintegrasikan RFID dan *fingerprint* terhubung dengan IoT. Dengan mengintegrasikan dua metode autentikasi RFID dan *fingerprint* dapat meningkatkan tingkat keamanan. Namun, penelitian ini sangat bergantung pada koneksi jaringan. Hasil pengujian menunjukkan sistem ini mampu menggabungkan RFID dan *fingerprint* dengan baik serta meningkatkan keamanan dan efisiensi

Lalu, Timothy Oktovialenta, Susilo dan Stepanus melakukan penelitian dengan judul ***Rancang Bangun Purwarupa Smart Attendance system Berbasis Teknologi Internet Of Things (Iot)*** pada tahun 2025 dalam Jurnal Ilmiah Program Studi Teknik Elektro, volume 8, nomor 1, halaman 22-34 [8]. Penelitian ini merancang sistem presensi berbasis RFID dan pengenalan wajah yang terintegrasi Iot melalui *Google Sheets* dan *Telegram* untuk mengatasi masalah presensi konvensional yang rentan terhadap kesalahan, manipulasi dan kurang efisien. Sistem ini dilengkapi dengan LCD dan *buzzer* sebagai indikator keberhasilan atau kegagalan yang diuji menggunakan metode kuantitatif melalui pemodelan simulasi dan uji eksperimental. Sistem ini memungkinkan data kehadiran bisa dipantau namun, penggunaan ESP32 *Cam* sangat dipengaruhi cahaya dan belum ada manajemen waktu. Hasil pengujian menunjukkan sistem ini mampu membaca UID, mengambil wajah dan mengirimkan data kehadiran.

Berdasarkan studi literatur tersebut terlihat beberapa *gap* antara penelitian terdaluhu dengan kebutuhan saat ini yakni masih menggunakan SFA, tidak terintegrasi IoT, masih berfokus pada presensi dan kontrol akses serta tidak adanya mekanisme *fail-safe* dan manajemen waktu. Oleh karena itu, penelitian ini akan memanfaatkan RFID dan *fingerprint* sebagai *multi-factor authentication* kontrol akses dan sistem presensi yang dilengkapai dengan manajemen waktu dan fitur *fail-safe* yang terintegrasi IoT

## KERANGKA TEORI

### 2.1 Sistem Kontrol Akses Autentikasi

#### 2.1.1 Sistem Kontrol Akses

Kontrol akses adalah mekanisme atau kebijakan untuk mengatur, membatasi, dan memantau siapa yang berhak mengakses sumber daya tertentu dan dalam kondisi tertentu. Penelitian ini menggunakan model *Attribute-Based Access Control* (ABAC) [9]. Dengan atribut yang digunakan ialah *user attributes* merujuk pada yang dimiliki pengguna, *environmental attributes* merujuk pada kondisi sistem, juga *data attributes* dalam hal ini ialah informasi nama dan waktu presensi. Semua atribut ini akan dikelola oleh *policy engine* untuk memberikan izin/hak akses terhadap pengguna.

#### 2.1.2 Konsep Autentikasi

Autentikasi adalah proses memverifikasi identitas pengguna

sebelum diberi akses ke sumber daya. Proses autentikasi melibatkan 3 faktor utama di antaranya, faktor pengetahuan terkait informasi yang diketahui oleh pengguna, faktor kepemilikan berhubungan dengan benda fisik yang dimiliki oleh pengguna, dan faktor keberadaan yang menggunakan karakteristik biologis unik (biometrik) untuk memverifikasi pengguna [10].

**2.2 Mikrokontroler**

Mikrokontroler adalah sebuah komputer kecil yang dikemas dalam bentuk *chip* berupa IC (*Integrated Circuit*) yang melakukan tugas memberikan sinyal *output* setelah menerima sinyal *input* [11]. Pada umumnya sinyal *input* mikrokontroler berasal dari sensor yang merupakan informasi dari lingkungan sedangkan *output* ditunjukan kepada aktuator yang dapat melakukan suatu tugas tertentu [12].

**2.3 *Radio Frequency Identification***

*Radio Frequency Identification* (RFID) adalah teknologi yang mendeteksi identitas tanpa perlu menggunakan kabel secara otomatis dan efisien. Komponen utamanya terdiri dari *tag* RFID sebagai penyimpan data identitas, *reader/scanner* sebagai pembaca sinyal lalu mengirim data ke mikrokontroler, dan *antenna* sebagai pemancar gelombang radio dari *reader* [13]. Dalam penelitian ini juga dilakukan perhitungan terkait akurasi pembacaan RFID. Perhitungan akurasi diperlukan untuk mengevaluasi sistem berkerja dengan benar sesuai dengan kasus penggunaan yang sudah diberikan menggunakan rumus 2.1 [14].

$$\frac{Jumlah\ Tag\ Berhasil\ Dibaca}{Total\ Percobaan\ Baca} \times 100\% \quad (2.1)$$

Berdasarkan persamaan 2.1, nilai akurasi dinyatakan dalam bentuk persentase (%). Nilai akurasi yang tinggi menunjukkan bahwa seluruh percobaan pembacaan RFID berhasil dilakukan tanpa kegagalan begitupun sebaliknya.

**2.4 *Fingerprint Biometric***

*Fingerprint biometric* adalah teknologi identifikasi menggunakan sidik jari sebagai metode autentikasi. *Fingerprint biometric* menawarkan akurasi tinggi, keamanan dan kepraktisan untuk mengidentifikasi identitas. Proses dimulai dengan *image acquisition* untuk menangkap gambar sidik jari menggunakan sensor untuk masuk ke tahap *prepocessing* meningkatkan citra sebelum dianalisis [15].

Dalam penelitian ini perhitungan akurasi *fingerprint* dapat dilakukan dengan menghitung *False Acceptance Rate* (FAR) dan *False Rejection Rate* (FRR). FAR menunjukkan persentase kesalahan sistem dalam menerima pengguna tidak sah. Sedangkan FRR menunjukkan persentase kesalahan sistem dalam menolak pengguna sah. Persamaan FAR dan FRR ditunjukkan dalam persamaan 2.2 dan 2.3 [16].

$$FAR = \frac{FA}{FA+TR} \times 100\% \quad (2.2)$$

$$FRR = \frac{FR}{TA+FR} \times 100\% \quad (2.3)$$

Keterangan:

$FAR$ : *False Acceptance Rate* (tingkat penerimaan palsu)
$FA$ : *False Acceptance* (pengguna tidak sah diterima)
$TR$ : *True Rejection* (pengguna tidak sah ditolak)
$FRR$ : *False Rejection Rate* (tingkat penolakan palsu)
$FR$ : *False Rejection* (pengguna sah ditolak)
$TA$ : *True Acceptance* (pengguna sah diterima)

Berdasarkan persamaan 2.2, semakin kecil nilai FAR, maka semakin baik tingkat keamanan sistem biometrik karena peluang pengguna yang tidak sah

memperoleh akses menjadi lebih rendah. Berdasarkan persamaan 2.3, semakin kecil nilai FRR, maka semakin baik performa sistem, karena pengguna yang sah dapat dikenali dengan lebih konsisten.

### 2.5 *Crossing Number Method*

*Crossing number* (CN) *method* adalah metode untuk identifikasi struktur piksel dalam citra biner yang sudah melewati proses *thinning*, berdasarkan jumlah perubahan transisi 0 dan 1 diantara delapan piksel tetangganya [17]. CN *method* akan menghitung berapa cabang garis yang bertemu pada satu piksel. Dalam *fingerprint* terdapat titik ciri khas atau *minutiae* berupa *ridge ending* (ujung garis) dan *bifurcation* (percabangan garis) yang dipakai sebagai fitur utama identifikasi sidik jari. Perhitungan CN *method* menggunakan rumus 2.4 [17] :

$$CN\,(p) = \frac{1}{2}\sum_{i=1}^{8}\left|p_i - p_{i+1}\right| \quad (2.4)$$

Keterangan:

$CN\,(p)$ : nilai *Crossing Number* pada piksel pusat $p$.

$p_i$ : nilai piksel tetangga ke-$i$ pada citra biner (bernilai 0 atau 1).

$p_{i+1}$ : nilai piksel tetangga berikutnya yang berurutan mengelilingi piksel pusat.

CN *method* akan menginterpretasi nilai 1 untuk *ridge ending*, 2 untuk piksel normal pada garis, 3 untuk *bifurcation*. Dalam *fingerprint* tingkat akurasinya sangat bergantung pada ketepatan deteksi *miunutiae,* dengan CN *method* memungkinkan peneliti untuk mendeteksi *minutiae* tersebut.

### 2.6 *Smart Card*

*Smart card* adalah kartu plastik berukuran kecil yang memiliki *chip* untuk menyimpan, memproses, dan mengelola data secara aman. *Smart card* ini digunakan untuk mengidentifikasi dan mengautentikasi identitas pemegang kartu, melakukan transaksi pembayaran serta digunakan dalam kontrol akses untuk membuka pintu, gerbang atau ruangan tertentu.

### 2.7 Mekanisme *Fail-Safe*

*Fail-safe* adalah mekanisme yang dirancang untuk mendeteksi potensi masalah dari kegagalan atau kerusakan dan mengambil tindakan untuk menghindari risiko [18]. Mekanisme ini mengutamakan keselamatan pengguna saat ada keadaan darurat, dan ini dilengkapi dengan sensor atau perangkat yang memantau kinerja sistem secara *real-time.*

Pada penelitian ini mekanisme *fail-safe* berfokus pada pendeteksi dini terhadap kondisi *emergency* menggunakan sensor MQ2 sebagai pemicu. Sensor akan mendeteksi keberadaan asap/gas secara *real-time*. Jika sensor MQ2 mendeteksi nilai asap/gas ≥ 450 sistem akan masuk ke dalam kondisi *emergency.* Saat MQ2 mendeteksi keberadaan asap/gas turun menjadi < 250, sistem akan kembali ke kondisi aman. Dengan *output* kondisi sistem akan dikirim ke *website dashboard* dengan status aman, dan sistem kembali beroperasi normal.

### 2.8 *Internet of Things* (IoT)

*Internet of things* (IoT) adalah jaringan perangkat fisik yang tertanam dengan perangkat lunak dan teknologi lain untuk berkomunikasi secara *real-time.* Secara umum, arsitektur IoT terdiri dari 4 lapisan utama yakni [19], *perception layer* untuk mengumpulkan data, *network layer* untuk konektivitas melalui internet, WiFi, atau *Bluetooth, application layer* untuk menampilkan atau memproses data yang diterima sebelumnya, dan *interface layer* yang menunjukkan interaksi dengan pengguna dan antar perangkat. Dalam penelitian ini *platform* IoT yang digunakan ialah *web-based* Iot *platform*

menggunakan XAMPP (Apache, MySQL dan PHP).

**2.9 Metode Analisis Statistik**

Analisa statistik digunakan untuk mengolah dan menginterpretasikan data hasil pengujian sehingga dapat menggambarkan performa sistem. Analisa statistik dalam penelitian ini difokuskan pada pengujian waktu respons sistem.

**2.9.1 Rata-Rata**

Dalam bagian ini akan dihitung rata-rata waktu respons dari *interlock* dan *website* untuk membandingkan waktu respons mana yang lebih cepat menggunakan rumus 2.5 dan 2.6 [20].

$$T_{respons} = T_{Output} - T_{input} \quad (2.5)$$

$$\bar{x} = \frac{x_1 + x_2 + \ldots + x_n}{n} \quad (2.6)$$

Keterangan:

$T_{respons}$ : Waktu respons sistem/*delay* $(s)$
$T_{input}$ : Waktu *input* $(s)$
$T_{Output}$ : Waktu *output* $(s)$
$\bar{x}$ : Rata-rata $(s)$
$x_n$ : Nilai dari setiap titik data
$n$ : Jumlah titik data

Semakin kecil nilai rata-rata menunjukkan semakin cepat waktu respons yang diberikan oleh sistem, sebaliknya semakin tinggi nilai rata-rata menunjukkan semakin lama waktu respons yang diberikan oleh sistem.

**2.9.2 Simpangan Baku**

Perhitungan simpangan baku digunakan untuk menggambarkan tingkat penyebaran data terhadap nilai rata-rata. Nilai simpangan baku dapat dinyatakan dengan rumus 2.7 [20].

$$s = \sqrt{\frac{\sum_{i=1}^{n}\left(x_i - \bar{x}\right)^2}{n}} \quad (2.7)$$

Keterangan:

$s$ : Simpangan baku $(s)$
$x_i$ : Nilai dari setiap titik data
$\bar{x}$ : Rata-Rata $(s)$
$n$ : Jumlah titik data

Karena sifat matematisnya, simpangan baku tidak pernah bernilai negatif sehingga interpretasi hanya berfokus pada besar kecilnya nilai. Nilai ini menjadi indikator konsistensi sistem:

- Jika $\sigma < \bar{x}$, variasi data rendah dan sistem stabil.
- Jika $\sigma \geq \bar{x}$, variasi data tinggi dan data tidak konsisten.

Analisis simpangan baku digunakan untuk menilai sistem yang diuji bekerja secara konsisten.

**2.9.3 Koefisien Variasi**

Perhitungan ini akan membandingkan tingkat keragaman relatif antar variabel (*interlock* dan *website*) yang berbeda. Nilai koefisien variasi dapat dinyatakan melalui persamaan 2.8 [21].

Keterangan:

$CV =$
$CV$ : Ko
$\sigma$ Sir
$\bar{x}$ Ra

Dalam konteks industri, $CV$ menjadi indikator penting untuk menilai konsistensi dan keandalan sistem dengan melihat

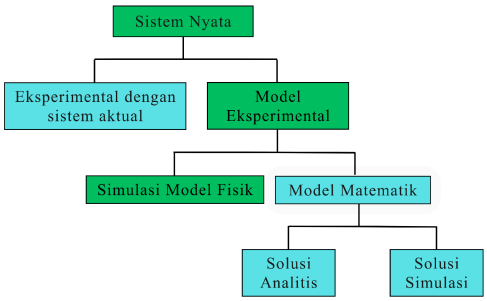
- Jika $CV \leq 10\%$, menunjukkan variasi sangat rendah sehingga sistem dapat dikategorikan konsisten dan stabil.
- Jika $CV$ bernilai 10% - 20%, menunjukkan variasi sedang yang masih dapat diterima.
- Jika $CV > 20\%$, menunjukkan variasi tinggi sehingga sistem dianggap tidak konsisten.

## METODE PENELITIAN

**3.1 Metode Penelitian**

Penelitian ini menggunakan metode kuantitatif yakni metode yang mengutamakan pengukuran dan analisis data untuk menguji dan menelaah korelasi tiap variable [22]. Metode ini dilengkapi

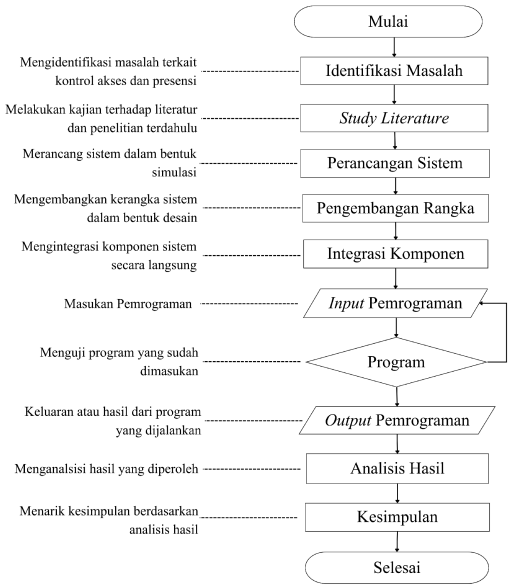
dengan pendekatan model eksperimental dan simulasi berdasarkan sistem nyata sebagaimana ditunjukkan pada Gambar 1**.** Pendekatan ini dilakukan melalui pengembangan model fisik untuk merancang sistem kontrol akses dan presensi mahasiswa.




*Gambar 1 Metode Penelitian[8]*

## 3.2 Tahapan Penelitian

Berdasarkan Gambar 2, penelitian ini melalui beberapa tahapan penelitian mulai dari identifikasi masalah hingga memperoleh kesimpulan di akhir penelitian.

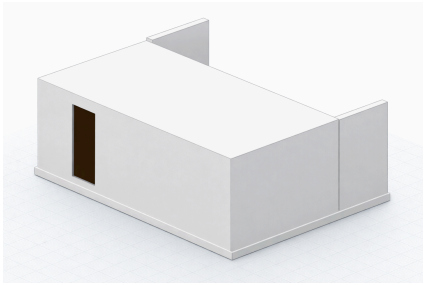



*Gambar 2 Tahapan Penelitian*

### 3.2.1 Waktu dan Tempat Penelitian

Penelitian ini dimulai dari bulan Februari 2026 hingga Juni 2026 bertempat di Ruang Laboratorium Arus Lemah Prodi Teknik Elektro Universitas Kristen Indonesia.

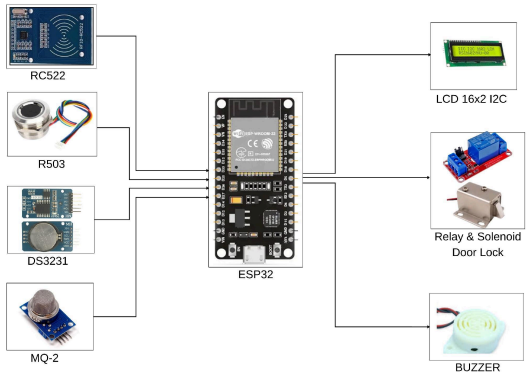
## 3.3 Perancangan Sistem



*Gambar 3 Desain 3D*

Gambar 3 menampilkan desain 3D dari penelitian ini yang menampung RC522 Masuk, R503 dan LCD 16×2 I2C di bagian depan, RC522 keluar dan MQ2 disisi samping, dan komponen lainnya di bagian dalam purwarupa.

### 3.3.1 Perancangan Perangkat Keras



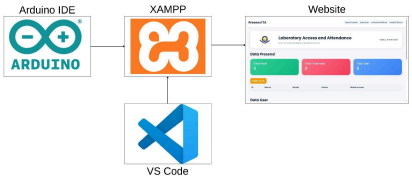

*Gambar 4 Perangkat Keras*

Berdasarkan Gambar 4 penelitian ini melibatkan beberapa perangkat keras, yakni

1. Perangkat *input* dalam sistem ini terdiri dari RC522 frekuensi 13,56 MHz dengan antarmuka SPI/I2C/UART [23] digunakan sebagai autentikasi awal. *Fingerprint Reader* R503 yang merupakan sensor kapasitif berkomunikasi melalui UART [23] sebagai tahap kedua autentikasi. RTC DS3231 yang berfungsi mencatat waktu secara presisi melalui antarmuka I2C [24] untuk pembatasan akses sesuai jadwal, serta *Smoke Detector* MQ-2 berperan sebagai pemicu *emergency mode*.

2. Mikrokontroler ESP32 merupakan mikroprosesor *embedded* dengan dukungan WiFi dan *Bluetooth* [25]. Dalam penelitian ini, ESP32 berfungsi sebagai pusat kendali yang menghubungkan komponen *input* dengan perangkat *output*.
3. Perangkat *output* terdiri dari *relay* 1 *channel* yang berfungsi sebagai saklar elektronik untuk mengendalikan beban bertegangan tinggi melalui sinyal kontrol rendah [26], solenoid *door lock* 12 V untuk membuka dan mengunci pintu secara otomatis, LCD 16×2 I2C yang menampilkan status autentikasi dan informasi sistem serta *buzzer* sebagai alarm peringatan ketika sistem masuk ke *emergency mode*.

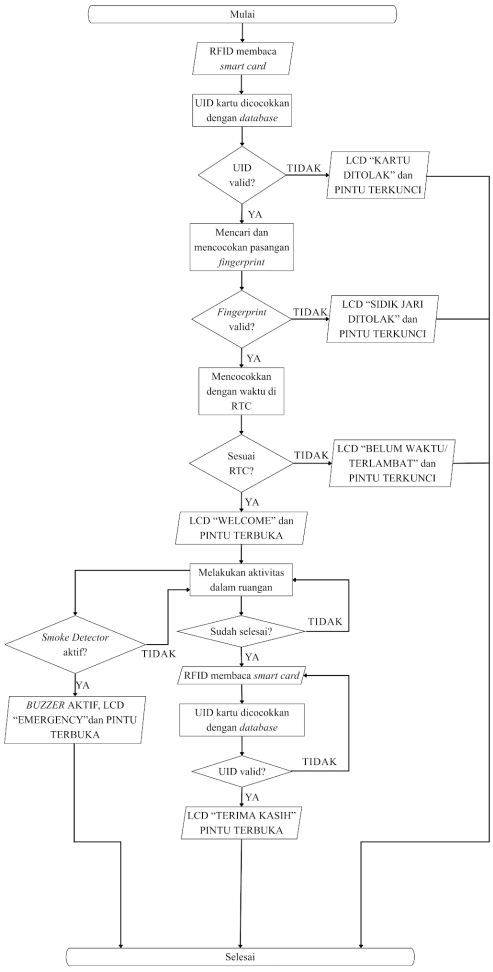
### 3.3.2 Perancangan Perangkat Lunak




*Gambar 5 Perangkat Lunak*

Berdasarkan Gambar 5 penelitian ini melibatkan beberapa perangkat lunak, yakni Arduino IDE digunakan untuk menuliskan kode yang akan mengontrol komponen, XAMPP digunakan untuk membangun *platform* IoT dalam menghubungkan mikrokontroler dengan sistem *monitoring, Visual Studio Code (*VS *Code*) sebagai pemrograman untuk *platform* IoT dan *Website* sebagai perangkat IoT untuk memantau proses aautentikasi dan kondisi sistem.

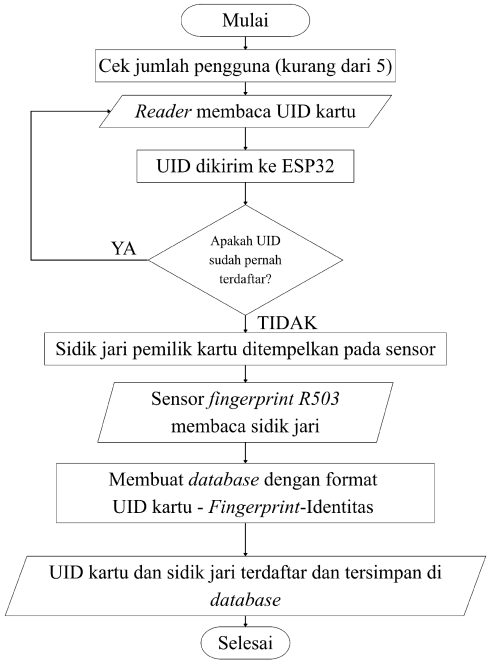
## 3.5 Mekanisme Kerja Alat




*Gambar 6 Mekanisme Kerja Alat*

Berdasarkan Gambar 6 alat ini bekerja dalam beberapa kasus penggunaan yang dibuat oleh peneliti untuk menggambarkan *input* dan *output* dari interaksi antar pengguna dan komponen alat.

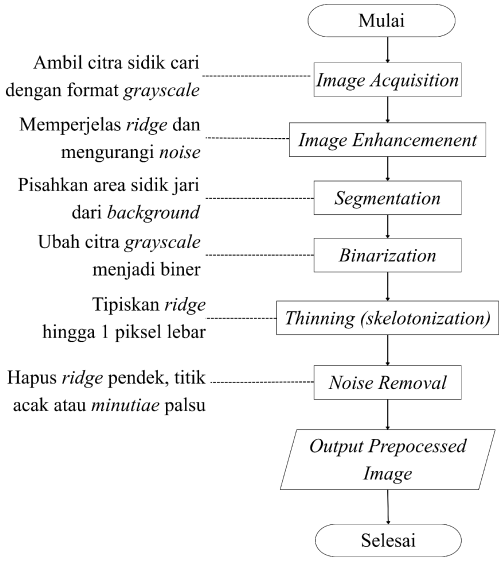
### 3.5.1 Mekanisme Pendaftaran




*Gambar 7 Mekanisme Pendaftaran*

Berdasarkan Gambar 7 dijelaskan mekanisme pendaftaran data pengguna sebelum alat digunakan untuk menyimpan informasi terkait kecocokkan RFID dan *fingerprint.*

### 3.5.2 Mekanisme Prepocessing Citra




*Gambar 8 Mekanisme Prepocessing*

Setelah *fingerprint* sudah berhasil di *scan, fingerprint* tersebut belum bisa dianalisis menggunakan *crossing number method. Prepocessing* citra *fingerprint* perlu dilakukan sesuai Gambar 8 agar citra *fingerprint* siap dianalisis menggunakan metode *crossing number*.

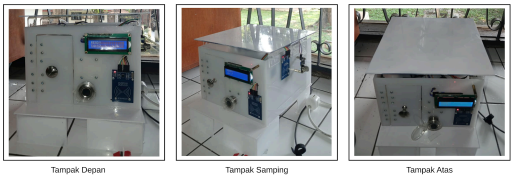
### 3.6 Teknik Analisis Data

Bagian ini membahas pengolahan data hasil pengujian komponen sistem kontrol akses dan autentikasi. Evaluasi dilakukan terhadap performa RFID RC522 menggunakan persamaan 2.1 untuk mengukur akurasi pembacaan UID, serta modul R503 melalui persamaan 2.2 dan 2.3 untuk menilai kemampuan menolak pengguna tidak sah dan menerima pengguna sah. Nilai CN method pada persamaan 2.4 digunakan untuk menjelaskan proses analisis citra sidik jari R503. Selain itu, waktu respons sistem dianalisis secara statistik dengan parameter rata-rata, simpangan baku, dan koefisien variasi guna menilai representasi, sebaran, dan konsistensi hasil. Seluruh data ditampilkan dalam bentuk tabel dan grafik agar interpretasi performa sistem lebih jelas.

## HASIL DAN PEMBAHASAN

### 4.1 Hasil Perancangan Purwarupa

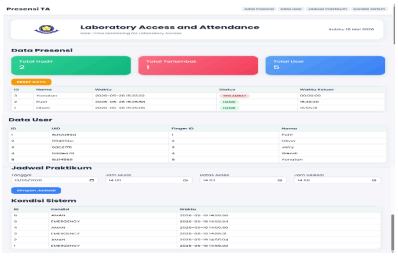
#### 4.1.1 Bentuk Fisik Purwarupa




*Gambar 9 Hasil Purwarupa*

Purwarupa yang telah dirancang dapat dilihat di Gambar 9. Dengan posisi RC522, LCD dan R503 ditempatkan di depan sebagai autentikasi masuk, RC522 keluar dan MQ-2 ditempatkan di sisi kanan luar untuk memudahkan proses pengujian, lalu sisanya ditempatkan di bagian dalam purwarupa.

#### 4.1.2 Tampilan *Website Dashboard*




*Gambar 10 Tampilan Website Dashboard*

Gambar 10 menunjukkan tampilan *website dasboard* yang telah dirancang. Dalam *website* akan menampilkan beberapa informasi yang dapat di *monitoring* secara *real-time* diantaranya:

a. Panel Kehadiran. Pada bagian ini berisi informasi total kehadiran, total terlambat dan total *user* yang didaftarkan.
b. Data presensi, berisi informasi terkait kehadiran *user.*
c. Tombol Reset Data, untuk mengembalikan ulang semua informasi yang telah tersimpan di *website* ke kondisi awal.
d. Data *user,* berisi informasi terkait *user* mencakup nama, UID kartu serta ID sidik jari untuk proses pencocokan data saat *user* melakukan autentikasi.
e. Jadwal praktikum. *Website* ini juga menyediakan fitur pengaturan jadwal secara *real-time.*
f. Kondisi sistem, sebagai tampilan jika terjadi kondisi *emergency.*

## 4.2 Pengujian Sistem

### 4.2.1 Pengujian Jarak Baca RC522

Pengujian jarak baca RC522 bertujuan untuk menentukan batas jangkau efektif RC522 dalam membaca kartu. Percobaan ini menggunakan 5 kartu yang sudah terdaftar. Hasil pengujian ini dapat dilihat dalam Tabel 1.

Berdasarkan Tabel 1 menunjukkan RC522 mampu membaca kartu dengan jarak 0 cm hingga 1 cm dan tidak dapat membaca kartu dengan jarak lebih dari 1 cm. Dengan hasil tersebut menunjukkan RC522 mampu membaca kartu dengan jarak tertentu.

*Tabel 1 Pengujian Jarak Baca RC522*

| No | UID Kartu | Jarak Baca (cm) | Hasil Pengujian |
|---|---|---|---|
| 1 | 6d12a69d | 0 | Terbaca |
| 2 | 6d12a69d | 1 | Terbaca |
| 3 | 6d12a69d | 2 | Tidak Terbaca |
| 4 | 6d12a69d | 3 | Tidak Terbaca |
| 5 | 6d12a69d | 4 | Tidak Terbaca |
| 6 | 6d12a69d | 5 | Tidak Terbaca |
| 7 | 694f15bc | 0 | Terbaca |
| 8 | 694f15bc | 1 | Terbaca |
| 9 | 694f15bc | 2 | Tidak Terbaca |
| 10 | 694f15bc | 3 | Tidak Terbaca |
| 11 | 694f15bc | 4 | Tidak Terbaca |
| 12 | 694f15bc | 5 | Tidak Terbaca |
| 13 | 6dc27f5 | 0 | Terbaca |
| 14 | 6dc27f5 | 1 | Terbaca |
| 15 | 6dc27f5 | 2 | Tidak Terbaca |
| 16 | 6dc27f5 | 3 | Tidak Terbaca |
| 17 | 6dc27f5 | 4 | Tidak Terbaca |
| 18 | 6dc27f5 | 5 | Tidak Terbaca |
| 19 | 6ddea78 | 0 | Terbaca |
| 20 | 6ddea78 | 1 | Terbaca |
| 21 | 6ddea78 | 2 | Tidak Terbaca |
| 22 | 6ddea78 | 3 | Tidak Terbaca |
| 23 | 6ddea78 | 4 | Tidak Terbaca |
| 24 | 6ddea78 | 5 | Tidak Terbaca |
| 25 | 6df4568 | 0 | Terbaca |
| 26 | 6df4568 | 1 | Terbaca |
| 27 | 6df4568 | 2 | Tidak Terbaca |
| 28 | 6df4568 | 3 | Tidak Terbaca |
| 29 | 6df4568 | 4 | Tidak Terbaca |
| 30 | 6df4568 | 5 | Tidak Terbaca |

### 4.2.2 Pengujian RC522 Masuk

Pengujian RC522 di pintu masuk bertujuan untuk memastikan keandalan RC522 dalam membaca UID kartu yang sudah terdaftar dalam sistem. Pengujian dilakukan dengan 10 kartu berbeda dengan kondisi 5 kartu terdaftar dan 5 lainnya tidak terdaftar. Setiap kartu akan ditempelkan pada RC522 masuk dengan indikator keberhasilan akan ditampilkan di LCD 16×2 I2C.

Berdasarkan hasil pengujian pada Tabel 2 dari 30 percobaan dengan 5 kartu terdaftar dan 5 kartu tidak terdaftar, secara keseluruhan diperoleh hasil pengujian

yang sesuai dengan indikator keberhasilan. Kartu yang terdaftar berhasil dibaca UID kartunya pada *serial monitor* dan LCD 16×2 I2C menampilkan "Tempelkan Jari," lalu bagi kartu yang tidak terdaftar UID kartunya juga akan terbaca pada *serial monitor* dan LCD 16×2 I2C menampilkan "Kartu Ditolak."

Dari data Tabel 2 tingkat akurasi untuk RFID masuk dapat dihitung menggunakan rumus 2.1:

$$\frac{Jumlah\,Tag\,Berhasil\,Dibaca}{Total\,Percobaan\,Baca} \times 100\%$$
$$= \frac{30}{30} \times 100\%$$
$$= 100\%$$

Dari nilai akurasi 100% menunjukkan bahwa RC522 beroperasi dengan baik dalam kondisi pengujian terkendali. Hasil ini menunjukkan bahwa RC522 memiliki tingkat akurasi tinggi dalam membaca UID kartu. Namun, meskipun hasil pengujian sempurna, perlu dicatat bahwa pengujian dilakukan dalam kondisi ideal, kartu dalam keadaan yang baik tidak mengalami kerusakan, dengan jarak baca 0 cm yang sesuai dengan hasil pengujian pada Tabel 1 untuk hasil yang baik.

*Tabel 2 Pengujian RC522 Masuk*

| No | UID Kartu | Status Kartu | LCD | Hasil |
|---|---|---|---|---|
| 1 | 6d12a69d | Terdaftar | Tempelkan Jari | Berhasil |
| 2 | 6d12a69d | Terdaftar | Tempelkan Jari | Berhasil |
| 3 | 6d12a69d | Terdaftar | Tempelkan Jari | Berhasil |
| 4 | 694f15bc | Terdaftar | Tempelkan Jari | Berhasil |
| 5 | 694f15bc | Terdaftar | Tempelkan Jari | Berhasil |
| 6 | 694f15bc | Terdaftar | Tempelkan Jari | Berhasil |
| 7 | 6dc27f7 | Terdaftar | Tempelkan Jari | Berhasil |
| 8 | 6dc27f7 | Terdaftar | Tempelkan Jari | Berhasil |
| 9 | 6dc27f7 | Terdaftar | Tempelkan Jari | Berhasil |
| 10 | 6ddea78 | Terdaftar | Tempelkan Jari | Berhasil |
| 11 | 6ddea78 | Terdaftar | Tempelkan Jari | Berhasil |
| 12 | 6ddea78 | Terdaftar | Tempelkan Jari | Berhasil |
| 13 | 6df4568 | Terdaftar | Tempelkan Jari | Berhasil |
| 14 | 6df4568 | Terdaftar | Tempelkan Jari | Berhasil |
| 15 | 6df4568 | Terdaftar | Tempelkan Jari | Berhasil |
| 16 | d5431f7 | Tidak Terdaftar | Kartu Ditolak | Berhasil |
| 17 | d5431f7 | Tidak Terdaftar | Kartu Ditolak | Berhasil |
| 18 | d5431f7 | Tidak Terdaftar | Kartu Ditolak | Berhasil |
| 19 | 1f8a16a | Tidak Terdaftar | Kartu Ditolak | Berhasil |
| 20 | 1f8a16a | Tidak Terdaftar | Kartu Ditolak | Berhasil |
| 21 | 1f8a16a | Tidak Terdaftar | Kartu Ditolak | Berhasil |
| 22 | 587acFEB630 | Tidak Terdaftar | Kartu Ditolak | Berhasil |
| 23 | 587acFEB630 | Tidak Terdaftar | Kartu Ditolak | Berhasil |
| 24 | 587acFEB630 | Tidak Terdaftar | Kartu Ditolak | Berhasil |
| 25 | 003D7C60 | Tidak Terdaftar | Kartu Ditolak | Berhasil |
| 26 | 003D7C60 | Tidak Terdaftar | Kartu Ditolak | Berhasil |
| 27 | 003D7C60 | Tidak Terdaftar | Kartu Ditolak | Berhasil |
| 28 | 40A0E861 | Tidak Terdaftar | Kartu Ditolak | Berhasil |
| 29 | 40A0E861 | Tidak Terdaftar | Kartu Ditolak | Berhasil |
| 30 | 40A0E861 | Tidak Terdaftar | Kartu Ditolak | Berhasil |

### 4.2.3 Keberhasilan R503

Pengujian keberhasilan R503 bertujuan untuk mengukur tingkat keberhasilan R503 serta mengevaluasi Tingkat kesalahan penerimaan (FAR) dan kesalahan penolakan (FRR) terhadap pengguna.

Berdasarkan hasil pengujian R503 pada Tabel 3 dari 30 percobaan dapat dilihat bahwa:

- *True Acceptance*: 7 percobaan menggunakan sidik jari terdaftar

dengan ID sesuai dan nilai *confidence* ≥ 80, *serial monitor* menampilkan *fingerprint valid.*

- *False Rejection:* 3 percobaan menggunakan sidik jari terdaftar dengan ID yang sesuai dan nilai *confidence* <80, *serial monitor* menampilkan *confidence* rendah (ditolak) dan LCD 16×2 I2C menampilkan "Akses Ditolak."
- *True Rejection:* 3 percobaan menggunakan sidik jari terdaftar dengan ID yang tidak sesuai dan nilai *confidence* <80, LCD 16×2 I2C menampilkan "Akses Ditolak."
- *True Rejection:* 7 percobaan menggunakan sidik jari terdaftar dengan ID yang tidak sesuai dan nilai *confidence* ≥ 80, LCD 16×2 I2C menampilkan "Ditolak," dan *serial monitor* menampilkan respons *finger* salah.
- *True Rejection:* 10 percobaan menggunakan sidik jari tidak terdaftar, *serial monitor* menampilkan sidik jari ditolak dan LCD 16×2 I2C menampilkan "Sidik Jari Ditolak."

*Tabel 3 Pengujian R503*

| No | *User* | ID | Status | *Confidence* | LCD | Hasil |
|---|---|---|---|---|---|---|
| 1 | 1 | 1 | Terdaftar - ID sesuai | 84 | - | TA |
| 2 | 1 | 1 | Terdaftar - ID sesuai | 80 | - | TA |
| 3 | 2 | 2 | Terdaftar - ID sesuai | 91 | - | TA |
| 4 | 2 | 2 | Terdaftar - ID sesuai | 89 | - | TA |
| 5 | 3 | 3 | Terdaftar - ID sesuai | 370 | - | TA |
| 6 | 3 | 3 | Terdaftar - ID sesuai | 101 | - | TA |
| 7 | 4 | 4 | Terdaftar - ID sesuai | 74 | Akses Ditolak | FR |
| 8 | 4 | 4 | Terdaftar - ID sesuai | 84 | - | TA |
| 9 | 5 | 5 | Terdaftar - ID sesuai | 65 | Akses Ditolak | FR |
| 10 | 5 | 5 | Terdaftar - ID sesuai | 78 | Akses Ditolak | FR |
| 11 | 1 | 5 | Terdaftar - ID tidak sesuai | 54 | Akses Ditolak | TR |
| 12 | 1 | 5 | Terdaftar - ID tidak sesuai | 68 | Akses Ditolak | TR |
| 13 | 2 | 4 | Terdaftar - ID tidak sesuai | 70 | Akses Ditolak | TR |
| 14 | 2 | 4 | Terdaftar - ID tidak sesuai | 81 | Ditolak | TR |
| 15 | 3 | 3 | Terdaftar - ID tidak sesuai | 81 | Ditolak | TR |
| 16 | 3 | 3 | Terdaftar - ID tidak sesuai | 94 | Ditolak | TR |
| 17 | 4 | 2 | Terdaftar - ID tidak sesuai | 84 | Ditolak | TR |
| 18 | 4 | 2 | Terdaftar - ID tidak sesuai | 87 | Ditolak | TR |
| 19 | 5 | 1 | Terdaftar - ID tidak sesuai | 81 | Ditolak | TR |
| 20 | 5 | 1 | Terdaftar - ID tidak sesuai | 95 | Ditolak | TR |
| 21 | 6 | 6 | Tidak terdaftar | - | Sidik Jari Ditolak | TR |
| 22 | 6 | 6 | Tidak terdaftar | - | Sidik Jari Ditolak | TR |
| 23 | 7 | 7 | Tidak terdaftar | - | Sidik Jari Ditolak | TR |
| 24 | 7 | 7 | Tidak terdaftar | - | Sidik Jari Ditolak | TR |
| 25 | 8 | 8 | Tidak terdaftar | - | Sidik Jari Ditolak | TR |
| 26 | 8 | 8 | Tidak terdaftar | - | Sidik Jari Ditolak | TR |
| 27 | 9 | 9 | Tidak terdaftar | - | Sidik Jari Ditolak | TR |
| 28 | 9 | 9 | Tidak terdaftar | - | Sidik Jari Ditolak | TR |
| 29 | 10 | 10 | Tidak terdaftar | - | Sidik Jari Ditolak | TR |
| 30 | 10 | 10 | Tidak terdaftar | - | Sidik Jari Ditolak | TR |

Dari data tersebut dapat dihitung tingkat akurasi *fingerprint* untuk mengukur presentase kesalahan R503 dalam menerima pengguna yang tidak terdaftar melalui rumus 2.2. Dengan jumlah *false accept* (kesalahan penerimaan) adalah 0 dan jumlah total *impostor attempts* (total percobaan pengguna yang tidak terdaftar) adalah 10

$$FAR = \frac{FA}{FA+TR} \times 100\%$$

$$FAR = \frac{0}{0+20} \times 100\%$$

$$FAR = 0\%$$

Dari data tersebut juga dihitung tingkat akurasi *fingerprint* untuk mengukur presentase kesalahan R503 dalam menolak pengguna yang sudah terdaftar melalui rumus 2.3. Dengan jumlah *false reject* (kesalahan penolakan) adalah 3 dan jumlah total *genuite attempts* (total percobaan pengguna yang terdaftar) adalah 10.

$$FRR = \frac{FR}{TA+FR} \times 100\%$$

$$FRR = \frac{3}{7+3} \times 100\%$$

$$FRR = 30\%$$

Dengan nilai FAR 0% menunjukan R503 cukup akurat dalam menolak pengguna yang tidak terdaftar namun, nilai FRR 30% menunjukkan bahwa dari 7 percobaan dengan sidik jari terdaftar, 2 diantaranya ditolak karena nilai *confidence* tidak mencapai 80. Juga dilakukan analisis terhadap citra *fingerprint* untuk menjelaskan kemampuan baca R503 menggunakan cn *method* melalui rumus 3-2. Sebelum melakukan perhitungan dilakukan *preprocessing* sesuai Gambar 8 dan memperoleh hasil di Gambar 11.

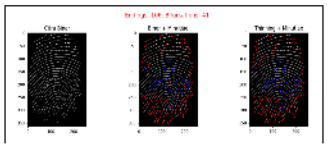



*Gambar 11 Hasil Prepocessing*

Dengan citra hasil *preprocessing* ini, analisis *minutiae* dapat dilakukan menggunakan cn *method* melalui rumus 2.4:

$$CN\,(p) = \frac{1}{2}\sum_{i=1}^{8}\left|p_i - p_{i+1}\right|$$

dimana $p_i$ adalah tetangga biner di sekitar biner pusat. Dalam perhitungan ini digunakan alat bantu Python untuk memudahkan perhitungan dengan prinsip yang sama sesuai rumus cn *method.* Python akan membaca dan menganalisis hasil *preprocessing* dengan mandai titik *minutiae* berupa *ridge ending* = 1 dan *bifurcation* = 3.



*Gambar 12 Hasil Perhitungan CN Method*

Berdasarkan Gambar 12 menjelaskan hasil perhitungan cn *method.* Titik *minutiae* yang diperoleh berupa *ridge ending* (CN=1) yang ditandai dengan warna merah dan *bifurcation* (CN=2) yang ditandai dengan warna biru. Dari hasil perhitungan, terdeteksi jumlah *ridge endings* sebesar 106 dan *bifurcation* sebesar 41 dengan jumlah 147 titik. Hal ini sejalan dengan cara kerja R503 yang mengambil dan menganalisis *minutiae* citra jari sidik jari lalu dibandingkan dengan citra yang sudah tersimpan sebelumnya. Dengan demikian, CN *method* tidak hanya untuk menganalisis citra sidik jari, tetapi juga menjelaskan mekanisme dasar R503 dalam proses autentikasi sidik jari.

### 4.2.4 Pengujian RC522 Keluar

Pengujian keberhasilan baca RC522 di pintu keluar bertujuan untuk memastikan keandalan RC522 membaca UID kartu yang sudah berhasil memperoleh hak akses terhadap ruangan. RC522 mendapat *supply* tegangan 3,3V.

Pengujian dilakukan dengan 5 kartu berbeda dengan kondisi:

- 2 UID kartu sudah memperoleh akses masuk dan sesuai waktu keluar.
- 2 UID kartu sudah memperoleh akses masuk dan tidak sesuai waktu keluar.
- 1 UID kartu belum memperoleh akses masuk dan sesuai waktu keluar.

Berdasarkan hasil pengujian pada Tabel 4 dari 30 percobaan dengan 2 kartu yang sudah memperoleh akses masuk dan keluar sesuai jadwal, 2 lainnya kartu yang sudah masuk dan keluar tidak sesuai jadwal, lalu sisanya 1 kartu yang belum pernah memperoleh akses masuk dan keluar sesuai dengan jadwal, yang secara keseluruhan diperoleh hasil yang sesuai dengan indikator keberhasilan yakni sebagai berikut:

- UID kartu yang sudah memperoleh akses masuk dan keluar sesuai jadwal, *serial monitor* akan menampilkan UID keluar dengan respons keluar berhasil dan LCD 16×2 I2C menampilkan "Terima Kasih."
- UID kartu yang sudah memperoleh akses masuk namun keluar tidak sesuai jadwal, *serial monitor* akan menampilkan UID keluar dengan respons belum boleh keluar dan LCD 16×2 I2C menampilkan "Belum Boleh Keluar."
- UID kartu yang belum pernah memperoleh akses masuk dan keluar sesuai jadwal, *serial monitor* akan menampilkan UID keluar dengan respons belum pernah masuk dan LCD menampilkan "Kartu Ditolak."

*Tabel 4 Pengujian RC522 Keluar*

| No | UID | Status | Waktu | LCD | *Relay* | Hasil |
|---|---|---|---|---|---|---|
| 1 | 6d12a69d | Sudah Masuk | Sesuai | Terima Kasih | ON | Berhasil |
| 2 | 6d12a69d | Sudah Masuk | Sesuai | Terima Kasih | ON | Berhasil |
| 3 | 6d12a69d | Sudah Masuk | Sesuai | Terima Kasih | ON | Berhasil |
| 4 | 6d12a69d | Sudah Masuk | Sesuai | Terima Kasih | ON | Berhasil |
| 5 | 6d12a69d | Sudah Masuk | Sesuai | Terima Kasih | ON | Berhasil |
| 6 | 6d12a69d | Sudah Masuk | Sesuai | Terima Kasih | ON | Berhasil |
| 7 | 694f15bc | Sudah Masuk | Sesuai | Terima Kasih | ON | Berhasil |
| 8 | 694f15bc | Sudah Masuk | Sesuai | Terima Kasih | ON | Berhasil |
| 9 | 694f15bc | Sudah Masuk | Sesuai | Terima Kasih | ON | Berhasil |
| 10 | 694f15bc | Sudah Masuk | Sesuai | Terima Kasih | ON | Berhasil |
| 11 | 694f15bc | Sudah Masuk | Sesuai | Terima Kasih | ON | Berhasil |
| 12 | 694f15bc | Sudah Masuk | Sesuai | Terima Kasih | ON | Berhasil |
| 13 | 6dc27f5 | Sudah Masuk | Belum | Belum Boleh Keluar | OFF | Berhasil |
| 14 | 6dc27f5 | Sudah Masuk | Belum | Belum Boleh Keluar | OFF | Berhasil |

| | | | | | | |
|---|---|---|---|---|---|---|
| 15 | 6dc27f5 | Sudah Masuk | Belum | Belum Boleh Keluar | OFF | Berhasil |
| 16 | 6dc27f5 | Sudah Masuk | Belum | Belum Boleh Keluar | OFF | Berhasil |
| 17 | 6dc27f5 | Sudah Masuk | Belum | Belum Boleh Keluar | OFF | Berhasil |
| 18 | 6dc27f5 | Sudah Masuk | Belum | Belum Boleh Keluar | OFF | Berhasil |
| 19 | 6ddea78 | Sudah Masuk | Belum | Belum Boleh Keluar | OFF | Berhasil |
| 20 | 6ddea78 | Sudah Masuk | Belum | Belum Boleh Keluar | OFF | Berhasil |
| 21 | 6ddea78 | Sudah Masuk | Belum | Belum Boleh Keluar | OFF | Berhasil |
| 22 | 6ddea78 | Sudah Masuk | Belum | Belum Boleh Keluar | OFF | Berhasil |
| 23 | 6ddea78 | Sudah Masuk | Belum | Belum Boleh Keluar | OFF | Berhasil |
| 24 | 6ddea78 | Sudah Masuk | Belum | Belum Boleh Keluar | OFF | Berhasil |
| 25 | 6df4568 | Belum Masuk | Sesuai | Kartu Ditolak | OFF | Berhasil |
| 26 | 6df4568 | Belum Masuk | Sesuai | Kartu Ditolak | OFF | Berhasil |
| 27 | 6df4568 | Belum Masuk | Sesuai | Kartu Ditolak | OFF | Berhasil |
| 28 | 6df4568 | Belum Masuk | Sesuai | Kartu Ditolak | OFF | Berhasil |
| 29 | 6df4568 | Belum Masuk | Sesuai | Kartu Ditolak | OFF | Berhasil |
| 30 | 6df4568 | Belum Masuk | Sesuai | Kartu Ditolak | OFF | Berhasil |

Dari data Tabel 4 tingkat akurasi untuk RFID keluar dapat dihitung menggunakan rumus 2.1:

$$\frac{Jumlah\ Tag\ Berhasil\ Dibaca}{Total\ Percobaan\ Baca} \times 100\%$$
$$= \frac{30}{30} \times 100\%$$
$$= 100\%$$

Dari nilai akurasi 100% menunjukkan bahwa RC522 beroperasi dengan baik dalam kondisi pengujian terkendali. Hasil ini menunjukkan bahwa RC522 memiliki tingkat akurasi tinggi dalam membaca UID kartu. Namun, meskipun hasil pengujian sempurna, perlu dicatat bahwa pengujian dilakukan dalam kondisi ideal, kartu dalam keadaan yang baik tidak mengalami kerusakan, dengan jarak baca 0 cm yang sesuai dengan hasil pengujian pada Tabel 1 untuk hasil yang baik.

### 4.2.5 Keberhasilan RTC DS3231

Pengujian RTC dilakukan untuk memastikan modul RTC dapat meberikan waktu yang valid sesuai dengan jadwal. Pengujian ini dilakukan dengan kombinasi validasi RC522 masuk dan R503 dengan 30 kali percobaan. Indikator keberhasilan jika RC522 masuk dan R503 valid dan sesuai waktu di jadwal maka LCD 16×2 I2C akan menampilkan "Selamat Datang," lalu jika RC522 masuk dan R503 valid dan tidak sesuai waktu di jadwal maka LCD 16×2 I2C akan menampilkan "Belum Waktu/Terlambat." Selain itu RTC DS3231 juga digunakan dalam memvalidasi waktu keluar, *user* hanya diperbolehkan untuk keluar dari ruangan jika sudah lewat dari waktu yang ditentukan.

*Tabel 5 Pengujian RTC DS3231*

| No | *User* | Waktu Masuk | LCD | *Relay* | Hasil |
|---|---|---|---|---|---|
| 1 | 1 | Belum Mulai | Belum Waktu Mulai | *OFF* | Berhasil |
| 2 | 1 | Belum Mulai | Belum Waktu Mulai | *OFF* | Berhasil |
| 3 | 2 | Belum Mulai | Belum Waktu Mulai | *OFF* | Berhasil |
| 4 | 2 | Belum Mulai | Belum Waktu Mulai | *OFF* | Berhasil |
| 5 | 3 | Belum Mulai | Belum Waktu Mulai | *OFF* | Berhasil |
| 6 | 3 | Belum Mulai | Belum Waktu Mulai | *OFF* | Berhasil |
| 7 | 4 | Belum Mulai | Belum Waktu Mulai | *OFF* | Berhasil |
| 8 | 4 | Belum Mulai | Belum Waktu Mulai | *OFF* | Berhasil |
| 9 | 5 | Belum Mulai | Belum Waktu Mulai | *OFF* | Berhasil |
| 10 | 5 | Belum Mulai | Belum Waktu Mulai | *OFF* | Berhasil |
| 11 | 1 | Sesuai Waktu | Selamat Datang | *ON* | Berhasil |
| 12 | 1 | Sesuai Waktu | Selamat Datang | *ON* | Berhasil |
| 13 | 2 | Sesuai Waktu | Selamat Datang | *ON* | Berhasil |
| 14 | 2 | Sesuai Waktu | Selamat Datang | *ON* | Berhasil |
| 15 | 3 | Sesuai Waktu | Selamat Datang | *ON* | Berhasil |
| 16 | 3 | Sesuai Waktu | Selamat Datang | *ON* | Berhasil |
| 17 | 4 | Sesuai Waktu | Selamat Datang | *ON* | Berhasil |
| 18 | 4 | Sesuai Waktu | Selamat Datang | *ON* | Berhasil |
| 19 | 5 | Sesuai Waktu | Selamat Datang | *ON* | Berhasil |
| 20 | 5 | Sesuai Waktu | Selamat Datang | *ON* | Berhasil |
| 21 | 1 | Setelah Waktu | Terlambat | *OFF* | Berhasil |
| 22 | 1 | Setelah Waktu | Terlambat | *OFF* | Berhasil |
| 23 | 2 | Setelah Waktu | Terlambat | *OFF* | Berhasil |
| 24 | 2 | Setelah Waktu | Terlambat | *OFF* | Berhasil |
| 25 | 3 | Setelah Waktu | Terlambat | *OFF* | Berhasil |
| 26 | 3 | Setelah Waktu | Terlambat | *OFF* | Berhasil |
| 27 | 4 | Setelah Waktu | Terlambat | *OFF* | Berhasil |
| 28 | 4 | Setelah Waktu | Terlambat | *OFF* | Berhasil |
| 29 | 5 | Setelah Waktu | Terlambat | *OFF* | Berhasil |
| 30 | 5 | Setelah Waktu | Terlambat | *OFF* | Berhasil |

Hasil pengujian DS3231 menunjukkan bahwa DS3231 mampu menjaga konsistensi waktu dengan baik. Sistem mampu mengautentikasi jadwal yang telah ditentukan.

Berdasarkan Tabel 5 semua hasil percobaan memperoleh indikator berhasil dalam membatasi akses sesuai jadwal yang sudah diatur. LCD akan menampilkan "Belum Waktu," jika

autentikasi sebelum waktu jadwal dimulai, lalu "Terlambat" jika autentikasi setelah melewati batas akses dan "*Welcome*" jika autentikasi sesuai jadwal. Selain itu, DS3231 juga digunakan dalam proses keluar, *user* hanya bisa keluar sesuai dengan waktu yang telah ditentukan dan divalidasi oleh DS3231. Kinerja DS3231 memiliki akurasi tinggi dalam menjaga waktu untuk memvalidasinya sesuai jadwal. Namun, DS3231 memiliki perbedaa beberapa detik dengan waktu *real-time.*

### 4.2.6 Keberhasilan Mekanisme *Fail-Safe*

Pengujian mekanisme *fail-safe* untuk memastikan sistem mampu memberikan respons yang tepat terhadap kondisi keamanan dalam ruangan. Tabel 6 menampilkan jarak deteksi MQ-2 menggunakan asap dan gas. Dalam percobaan berikutnya digunakan gas sebagai pemicu MQ-2 dalam mengaktifkan *emergency mode* dengan jarak konsisten 1 cm.

*Tabel 6 Jarak Deteksi MQ-2*

| Pemicu | Jarak Deteksi (cm) | Hasil |
|---|---|---|
| Asap | 1 | Tidak Terdeteksi |
| | 2 | Terdeksi |
| | 3 | Terdeksi |
| | 4 | Tidak Terdeteksi |
| | 5 | Tidak Terdeteksi |
| Gas | 1 | Terdeksi |
| | 2 | Terdeksi |
| | 3 | Terdeksi |
| | 4 | Tidak Terdeteksi |
| | 5 | Tidak Terdeteksi |

Dari hasil pengujian pada Tabel 7 menunjukkan keberhasilan MQ-2 dalam mendeteksi keberadaan asap dan memberi *output* yang sesuai dengan indikator keberhasilan. Pintu terbuka atau *relay ON* dan LCD menampilkan "*Emergency*!" serta *buzzer ON* saat nilai asap sudah melewati batas yang ditetapkan. Hal ini menunjukkan bahwa MQ-2 bekerja dengan baik dalam mendeteksi keberadaan asap. Asap yang di deteksi pada nilai ≥ 450 dan akan kembali normal < 250, menunjukkan bahwa sistem ini bukan hanya untuk kontrol akses dan presensi tapi juga memiliki fitur keamanan yang memastikan *user* tidak terjebak dalam ruangan saat terjadi kebakaran.

*Tabel 7 Pengujian MQ2*

| No | Nilai MQ2 | *Buzzer* | LCD | *Relay* | Hasil |
|---|---|---|---|---|---|
| 1 | 85 | *OFF* | - | *OFF* | Berhasil |
| 2 | 89 | *OFF* | - | *OFF* | Berhasil |
| 3 | 92 | *OFF* | - | *OFF* | Berhasil |
| 4 | 96 | *OFF* | - | *OFF* | Berhasil |
| 5 | 99 | *OFF* | - | *OFF* | Berhasil |
| 6 | 102 | *OFF* | - | *OFF* | Berhasil |
| 7 | 105 | *OFF* | - | *OFF* | Berhasil |
| 8 | 109 | *OFF* | - | *OFF* | Berhasil |
| 9 | 110 | *OFF* | - | *OFF* | Berhasil |
| 10 | 112 | *OFF* | - | *OFF* | Berhasil |
| 11 | 116 | *OFF* | - | *OFF* | Berhasil |
| 12 | 129 | *OFF* | - | *OFF* | Berhasil |
| 13 | 162 | *OFF* | - | *OFF* | Berhasil |
| 14 | 216 | *OFF* | - | *OFF* | Berhasil |
| 15 | 328 | *OFF* | - | *OFF* | Berhasil |
| 16 | 453 | *ON* | *EMERGENCY!* | *ON* | Berhasil |
| 17 | 464 | *ON* | *EMERGENCY!* | *ON* | Berhasil |
| 18 | 475 | *ON* | *EMERGENCY!* | *ON* | Berhasil |
| 19 | 479 | *ON* | *EMERGENCY!* | *ON* | Berhasil |
| 20 | 480 | *ON* | *EMERGENCY!* | *ON* | Berhasil |

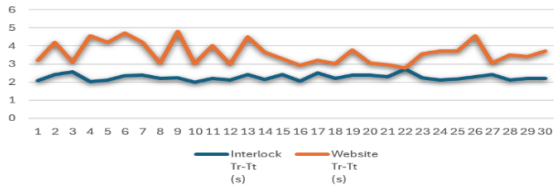
| | | | | | |
|---|---|---|---|---|---|
| 21 | 499 | *ON* | *EMERGENCY!* | *ON* | Berhasil |
| 22 | 505 | *ON* | *EMERGENCY!* | *ON* | Berhasil |
| 23 | 511 | *ON* | *EMERGENCY!* | *ON* | Berhasil |
| 24 | 528 | *ON* | *EMERGENCY!* | *ON* | Berhasil |
| 25 | 619 | *ON* | *EMERGENCY!* | *ON* | Berhasil |
| 26 | 656 | *ON* | *EMERGENCY!* | *ON* | Berhasil |
| 27 | 867 | *ON* | *EMERGENCY!* | *ON* | Berhasil |
| 28 | 982 | *ON* | *EMERGENCY!* | *ON* | Berhasil |
| 29 | 1293 | *ON* | *EMERGENCY!* | *ON* | Berhasil |
| 30 | 1143 | *ON* | *EMERGENCY!* | *ON* | Berhasil |

### 4.2.7 Keberhasilan Waktu Respons

Pengujian waktu respons sistem bertujuan untuk memastikan bahwa sistem berfungsi dengan baik saat terjadi *emergency* dengan mengukur lama waktu sistem memberikan *output*. Pengujian ini berfokus pada waktu respons interlock dan website dengan menghitung *delay* dan kestabilan sistem.

*Tabel 8 Pengujian Waktu Respons*

| No | Interlock Tr-Tt (s) | Website Tr-Tt (s) |
|---|---|---|
| 1 | 2,08 | 3,21 |
| 2 | 2,4 | 4,2 |
| 3 | 2,55 | 3,1 |
| 4 | 2,02 | 4,56 |
| 5 | 2,11 | 4,18 |
| 6 | 2,34 | 4,7 |
| 7 | 2,37 | 4,2 |
| 8 | 2,21 | 3,05 |
| 9 | 2,23 | 4,8 |
| 10 | 2 | 3,01 |
| 11 | 2,21 | 4,02 |
| 12 | 2,1 | 2,98 |
| 13 | 2,4 | 4,51 |
| 14 | 2,13 | 3,64 |
| 15 | 2,4 | 3,3 |
| 16 | 2,06 | 2,93 |
| 17 | 2,5 | 3,19 |
| 18 | 2,2 | 3,01 |
| 19 | 2,37 | 3,78 |
| 20 | 2,37 | 3,04 |
| 21 | 2,3 | 2,96 |
| 22 | 2,7 | 2,78 |
| 23 | 2,23 | 3,56 |
| 24 | 2,1 | 3,71 |
| 25 | 2,17 | 3,72 |
| 26 | 2,3 | 4,56 |
| 27 | 2,4 | 3,04 |
| 28 | 2,1 | 3,5 |
| 29 | 2,21 | 3,4 |
| 30 | 2,2 | 3,7 |
| Rata-Rata ($\bar{x}$) | 2,26 | 3,61 |
| Varian ($\sigma^2$) | 0,03 | 0,36 |
| Simpangan baku ($\sigma$) | 0,16 | 0,60 |
| Koefisien Variasi ($CV$) | 7% | 17% |




*Gambar 13 Perbandingan Waktu Respons Interlock dan Website*

Gambar 13 menunjukkan grafik dari perbandingan waktu respons *interlock* dan *website* yang diperoleh berdasarkan hasil di Tabel 7. Dari 30 percobaan, rata-rata waktu respons dihitung berdasarkan selisih antar waktu *output* dan waktu *input* sesuai rumus 2.6. Dalam pengujian ini, waktu *input* ($T_{input}$) ditetapkan sebagai 0 detik, sehingga rumus perhitungan waktu respons dapat ditulis menjadi

$$T_{respons} = T_{output}$$

Pengujian waktu respons diuji dalam 30 kali percobaan dengan hasil rata-rata waktu respons *interlock* 2,26s dan *website* 3,61s. Hasil ini menunjukkan waktu respons *interlock* lebih cepat dibandingkan waktu respons *website.* Selain itu, dilakukan analisis untuk mengetahui konsistensi waktu respons sistem menggunakan rumus 2.7.

$$\sigma = \sqrt{\frac{\sum_{i=1}^{n}\left(x_i - \bar{x}\right)^2}{n}}$$

Dari rumus tersebut diperoleh hasil bahwa, nilai simpangan baku *interlock* 0,16 sedangkan *website* 0,60. Nilai simpangan baku *website* lebih besar dibandingkan *interlock.* Hal ini menunjukkan bahwa hasil pengujian *website* lebih berfluktuasi dibandingkan *interlock,* dengan adanya pengujian yang jauh lebih cepat maupun lambat dibandingkan dengan rata-rata. Variasi ini menandakan bahwa *website* kurang konsisten, sehingga stabilitasnya lebih rendah dibandingkan dengan *interlock.* Juga dilakukan perhitungan koefisien variasi untuk menilai tingkat kestabilan sistem menggunakan rumus 2.8.

$$CV = \frac{\sigma}{\bar{x}} \times 100\%$$

Dari perhitungan tersebut diperoleh bahwa, nilai $CV$ *interlock* sebesar 7% berada di bawah 10%, sehingga *interlock* dapat dikategorikan sebagai variasi sangat rendah. Artinya waktu respons *interlok* tidak hanya konsisten tetapi juga relatif stabil terhadap rata-rata. Dengan demikian, *interlock* dianggap memiliki performa yang handal. Berbeda dengan *interlock,* $CV$ *website* bernilai 17%, nilai ini berada dalam rentang 10% - 20%, yang menunjukkan variasi sedang. Meskipun masih dapat diterima, hasil ini menunjukkan bahwa *website* memiliki fluktuasi waktu respons yang lebih besar dibandingkan *interlock.*

Dalam konteks *emergency mode,* perbedaan ini memiliki implikasi penting. *Interlock* memiliki respons yang lebih cepat dan stabil memberikan jaminan bahwa mekanisme *fail-safe* dapat berjalan segera setelah sensor MQ2 mendeteksi nilai asap/gas di udara. Sebaliknya, *website* menunjukkan waktu respons yang lebih lama dan bervariasi, yang dipengaruhi oleh kualitas jaringan Wi-Fi serta proses *auto-refresh* setiap 10 detik. Hal ini berpotensi menunda pembaruan status darurat pada *dashboard web*, sehingga dalam kondisi kritis, *interlock* menjadi mekanisme utama yang lebih dapat diandalkan.

## SIMPULAN DAN SARAN

### 5.1 Kesimpulan

Berdasarkan hasil pengujian pada purwarupa yang telah dirancang diperoleh kesimpulan:

*a.* Penelitian ini berhasil merancang dan mengimplementasikan purwarupa sistem kontrol akses dan presensi laboratorium yang menggunakan multi-autentikasi dengan mekanisme pembatasan dan fitur keamanan darurat.

*b.* Berhasil merancang *website dashboard* IoT untuk menampilkan data *user, monitoring* data presensi dan kondisi sistem, serta fitur pengaturan jadwal secara *real-time.*

*c.* RC522 memiliki tingkat akurasi 100% dalam membaca UID kartu. *Fingerprint* R503 memiliki akurasi tinggi dengan persentase FAR 0% dan persentase FRR 30%. RTC DS3231 mampu membatasi akses sesuai dengan jadwal yang ditetapkan. Mekanisme *fail-safe* juga berhasil bekerja dengan baik dengan MQ2 mendeteksi keberadaan asap. Pengujian waktu respons pada kondisi *emergency mode* menunjukkan bahwa sistem *interlock* memiliki respons yang lebih cepat dan konsisten dibandingkan *website*.

### 5.2 Saran

Berdasarkan hasil penelitian diperoleh beberapa saran yang bisa dijadikan acuan untuk penelitian selanjutnya, diantaranya

1. Mengembangkan sistem yang tidak bergantung pada internet yakni menyediakan mode *offline* agar sistem tetap bekerja walau kondisi jaringan kurang memadai.
2. Menambahkan sensor penghitung orang di pintu untuk memastikan jumlah individu yang mengakses ruangan sesuai autentikasi, sehingga tidak ada celah dua orang masuk dalam satu autentikasi.

## DAFTAR PUSTAKA


[1] Y. Rafita, "Analisis Faktor-Faktor Yang Mempengaruhi Kecurangan Akademik (Titip Absen) Pada Mahasiswa S1 Fakultas Matematika Dan Ilmu Pengetahuan Alam Universitas Islam Indonesia," *Khazanah J. Mahasiswa*, pp. 25–37, 2013, doi: https://doi.org/10.20885/khazanah.vol5.iss2.art3.

[2] "Mengapa Absensi Manual Sudah Tidak Relevan Lagi di Era Digital," Kantor Kita. *Accessed*: Feb. 21, 2026. [*Online*]. *Available*: https://www.kantorkita.co.id/blog/mengapa-absensi-manual-sudah-tidak-relevan-lagi-di-era-digital/

[3] A. Prayitno, C. Chotimah, S. Nugraha, and T. Istanto, "Sistem Keamanan Pintu Laboratorium Perikanan Berbasis Mikrokontroler," *J. Ris. Rekayasa Elektro*, vol. 6, no. 1, pp. 1–12, 2024, doi: https://doi.org/10.30595/jrre.v6i1.19710.

[4] M. Ula, A. Pratama, Y. Asbar, W. Fuadi, R. Fajri, and R. Hardi, "*A New Model of The Student Attendance Monitoring System Using RFID Technology*," *J. Phys. Conf. Ser.*, vol. 1807, no. 1, 2021, doi: https://doi.org/10.1088/1742-6596/1807/1/012026.

[5] Bukhari, M. Razi, Azwar, and A. S. Ismy, "Rancang Bangun Prototipe Pintu Cerdas Terintegrasi Sistem Absensi Berbasis Mikrokontroler Arduino," *Proceeding Semin. Nas. Politek. Negeri Lhokseumawe*, vol. 6, no. 1, pp. 122–127, 2022, [Online]. Available: https://e-jurnal.pnl.ac.id/semnaspnl/article/view/3453/2774

[6] M. S. Rahman, K. Rumman, R. Ahmmed, M. Rahman, and M. Sarker, "*Fingerprint* Based Biometric Attendance," *Sect. A-Research Pap. Eur. Chem. Bull.*, vol. 12, no. S3, pp. 184–190, 2023, doi: 10.31838/ecb/2023.12.s3.026.

[7] A. Zainuddin *et al.*, "*Innovative IoT Smart Lock System : Enhancing Security with Fingerprint and* RFID *Technology,*" *Malaysian J. Sci. Adv. Technol.*, vol. 4, no. 4, pp. 360–365, 2024, doi: https://doi.org/10.56532/mjsat.v4i4.335.

[8] T. Oktovialenta, Susilo, and Stepanus, "Rancang Bangun Purwarupa S*mart Attendance System* Berbasis Teknologi *Internet of Things* (IoT)," *J. Ilm. Progr. Stud. Tek. Elektro*, vol. 8, no. 1, pp. 22–34, 2025, [Online]. Available: https://ejournal.uki.ac.id/index.php/lektrokom/article/view/7343

[9] M. Penelova, "Access Control Models," *Cybern. Inf. Technol.*, vol. 21, no. 4, pp. 77–104, 2021, doi: https://doi.org/10.2478/cait-2021-0044.

[10] I. Velasquez, A. Caro, and A. Rodriguez, "*Authentication Schemes and Methods: a Systematic Literature Review*," *Inf. Softw. Technol.*, vol. 90, pp. 30–27, 2017, doi:

https://doi.org/10.1016/j.infsof.2017.09.012.

[11] "Mikrokontroler," mediacenter.itbmg. *Accessed:* Feb. 22, 2026. [*Online*]. *Available:* https://mediacenter.itbmg.ac.id/mikrokontroler-pengertian-fungsi-dan-jenis-jenisnya/

[12] M. Kelemen, E. Prada, T. Kelemenova, L. Miková, I. Virgala, and T. Lipták, "*Embedded systems via using microcontrol*ler," *Appl. Mech. Mater.*, vol. 816, pp. 248–254, 2015, doi: https://doi.org/10.4028/www.scientific.net/AMM.816.248.

[13] M. Kaur, M. Sandhu, N. Mohan, and P. S. Sandhu, "RFID *Technology Principles, Advantages , Limitations & Its Applications*," *Int. J. Comput. Electr. Eng.*, vol. 3, no. 1, pp. 151–157, 2011.

[14] F. Candrasyah, A. Dinimaharawati, H. A. Shiddieqy, F. B. Fatahillah, and M. R. Aslam, "*Multi-Object Inventory System Using Ultra-High frequency radio Frequency Identification* (UHF RFID) *Based on Internet of Things*," *Int. J. Appl. Inf. Technol.*, vol. 08, no. 02, 2024, doi: http://dx.doi.org/10.25124/ijait.v8i2.9571.

[15] H. S, "*A systematic review on Fingerprint based Biometric Authentication System," International Conf. Emerg. Trends Inf. Technol. Eng. (ic-ETITE). IEEE*, pp. 1–4, 2020, doi: 10.1109/ic-ETITE47903.2020.342.

[16] A. Aftab, F. A. Khan, M. K. Khan, H. Abbas, W. Iqbal, and F. Riaz, "*Hand-based multibiometric systems: state-of-the-art and future challenges*," *PeerJ Comput. Sci.*, vol. 7, p. e707, 2021, doi: https://doi.org/10.7717/peerjcs.707.

[17] P. Puteaux and I. Tkachenko, "*Crossing Number Features : from Biometrics to Printed Character Matching*," *Int. Conf. Doc. Anal. Recognition.*, 2021.

[18] "*Failsafe System*s," Sapien. *Accessed:* Feb. 22, 2026. [*Online*]. *Available:* https://www.sapien.io/glossary/definition/failsafe-systems

[19] P. Gokhale, O. Bhat, and S. Bhat, "*Introduction of iot*," *Int. Adv. Res. J. Sci. Eng. Technol.*, vol. 5, no. 1, 2018.

[20] R. E. Walpole, R. H. Myers, S. L. Myers, and K. Ye, *Probability & Statistics for Engineers & Scientists*, 9th ed. Boston: Pearson Education, 2012.

[21] B. Rosner, *Fundamentals of Biostatistics*, 7th ed. Bostom: Brooks/Cole, Cengage Learning, 2011.

[22] J. W. Creswell, *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches*, Third edit. Thousand Oaks, California, USA: SAGE Publications, Inc, 2009.

[23] Elprocus, "RC522 RFID *Module : PinOut, Features, Specifications, Interfacing, Working Datasheet & Its Applications*," elprocus.com. *Accessed:* Feb. 23, 2026. [*Online*]. *Available:* https://www.elprocus.com/rc522-rfid-module/

[24] R. Ervani, "Modul RTC DS3231," RezArduino. *Accessed:* Feb. 23, 2026. [*Online*]. *Available*: https://arduino.rezaervani.com/2019/03/02/modul-rtc-ds3231/

[25] Ardutech, "Mengenal ESP32 Development Kit untuk IoT (*Internet of Things*),"

ardutech.com. *Accessed*: Feb. 23, 2026. [*Online*]. *Available*: https://www.ardutech.com/mengenal-esp32-development-kit-untuk-iot-internet-of-things/

[26] DigiWare, "*Relay Module 1 Channel 5V Active High or Low Trigger*," digiwarestore.com. *Accessed*: Feb. 22, 2026. [*Online*]. *Available*: https://digiwarestore.com/id/relay/relay-module-1-channel-5v-active-high-or-low-trigger-263130.html#:~:text=Modul relay 1 Channel ini,seperti Arduino atau Raspberry Pi.