

## **SISTEM KEAMANAN RUANG SERVER MENGGUNAKAN TEKNOLOGI BIOMETRIK *FACE RECOGNITION* DAN *FINGERPRINT***

**Alfiana Zakiah**

Fakultas Teknik, Program Studi Teknik Elektro

Universitas Muria Kudus

Email: 201852001@std.umk.ac.id

### **ABSTRAK**

Penelitian ini ditujukan untuk memperbaiki kekurangan skripsi yang telah dilakukan oleh (Nurwjaksana & Candra, 2021) yang berjudul “Akses Keluar Masuk Ruang Server Menggunakan RFID Yang Diimplementasikan Untuk Keamanan”. Dalam penelitian yang sudah dilakukan tersebut mendapatkan hasil berupa alat sistem keamanan ruang server yang hanya dapat diakses oleh pemilik kartu RFID. Namun dalam penelitian tersebut terdapat beberapa kekurangan diantaranya: akses masuk menggunakan RFID yang mana masih menggunakan kartu bisa saja lupa membawa kartu tersebut bahkan hilang dan tidak adanya sistem keamanan pintu jika terjadi pembobolan. Dengan kekurangan yang dimiliki pada sistem keamanan ruang server yang sudah dibuat, penulis bermaksud memperbaiki kekurangan pada alat tersebut dengan membuat sistem keamanan ruang server dengan menggunakan teknologi biometrik yaitu *face recognition* dan *fingerprint* dilengkapi dengan deteksi pembobolan pintu menggunakan sensor *magnetic door switch* MC-38. Jika terdeteksi pembobolan pintu maka alarm dari *buzzer* akan menyala dan mengirim notifikasi ke Telegram. Hasil penelitian ini adalah berupa alat sistem keamanan ruang server yang hanya bisa diakses oleh orang yang sudah terdaftar pada sistem. Sensor kamera mampu mendeteksi wajah mulai jarak 20cm sampai 80cm dapat menangkap citra wajah dengan baik Hasil pengujian *fingerprint* yang didapatkan sensor sidik jari bekerja dengan baik dengan tingkat keberhasilan 100%. Deteksi pembobolan pintu menggunakan sensor *magnetic door switch* MC-38 berfungsi sesuai prinsip kerja, jika terjadi pembukaan pintu tanpa melalui sistem akses sensor *magnetic door switch* MC-38 mampu mengirimkan sinyal ke ESP32-Cam untuk menyalakan *buzzer* dan mengirim pesan ke Telegram.

**Kata kunci** : sistem keamanan, ESP32-Cam, *face recognition*, *Fingerprint*, sensor *magnetic door switch* MC38, bot Telegram.

### **ABSTRACT**

*This research is aimed at correcting the shortcomings of the thesis that has been carried out by (Nurwjaksana & Candra, 2021) entitled "Incoming and Out of Access Server Room Using RFID Implemented for Security". In the research that has been done, the results are in the form of a server room security system tool that can only be accessed by the owner of the RFID card. However, in this study there were several drawbacks including: entry access using RFID which still uses a card to enter the room, it is possible to forget to bring the card and even lose it and there is no door security system in the event of a break-in. With the deficiencies that have in the safe security system that has been made, the author intends to fix the deficiencies in the tool by creating a server room security system using biometric technology, namely face recognition and fingerprints equipped with door break-in detection using the MC38 door sensor. If a door sensor is detected, the alarm from the buzzer will turn on and send a notification to Telegram. The results of this study are in the form of a server room security system tool that can only be accessed by people who have registered with the system. The camera sensor is capable of detecting faces from a distance of 20cm to 80cm and can capture facial images properly. The results of the fingerprint test obtained by the fingerprint sensor work well with a 100% success rate. Door breaking detection using the MC38 door sensor functions according to the working principle, if the door is opened without going through the access system it can turn on the buzzer and send messages to Telegram.*

**Keywords:** *security system, ESP32-Cam, face recognition, Fingerprint, door sensor MC38, bot Telegram.*

## 1. PENDAHULUAN

Ruang server merupakan ruangan khusus yang digunakan untuk menyimpan server (aplikasi dan *database*), perangkat jaringan (*router, hub, switch*) dan perangkat lainnya yang terkait dengan operasional sistem sehari-hari seperti UPS, CCTV dan lain-lain. Sebuah ruang server yang hanya boleh diakses oleh orang-orang tertentu harus memiliki standar keamanan yang tinggi agar dapat melindungi perangkat - perangkat didalamnya seperti *database* dan akses masuk dari orang-orang yang tidak berkepentingan (Bahri & Suhardiyanto, 2018).

Penelitian ini ditujukan untuk memperbaiki kekurangan skripsi yang telah dilakukan oleh (Nurwajaksana & Candra, 2021) yang berjudul “Akses Keluar Masuk Ruang Server Menggunakan RFID Yang Diimplementasikan Untuk Keamanan”. Dalam penelitian yang sudah dilakukan tersebut mendapatkan hasil berupa alat sistem keamanan ruang server yang hanya dapat diakses oleh pemilik kartu RFID. Namun dalam penelitian tersebut terdapat beberapa kekurangan diantaranya: akses masuk menggunakan RFID yang mana masih menggunakan kartu untuk masuk ke ruangan bisa saja lupa membawa kartu tersebut bahkan hilang dan tidak adanya sistem keamanan pintu jika terjadi pembobolan.

Cara kerja sistem ini adalah untuk masuk ke ruang server menggunakan 2 input yaitu pengenalan wajah dan sidik jari bagi pengguna yang sudah terdaftar pada sistem. Kedua input ini dirancang dengan logika AND untuk membuka *solenoid door lock*. Selanjutnya sistem akan menunggu pintu terbuka 10 detik. Setelah pintu terbuka sistem akan menunggu pintu tertutup selama 15 detik, jika lebih dari 15 detik maka buzzer akan hidup. Jika lebih dari 15 detik pintu belum tertutup maka buzzer akan *ON* untuk mengingatkan agar pintu segera ditutup kembali. Setelah pintu tertutup buzzer akan *OFF* dan sensor pintu akan aktif *LOW*. Sistem ini dilengkapi dengan alarm dan notifikasi Telegram jika terjadi pembobolan pintu. Pembobolan pintu yang dimaksud adalah proses membuka pintu secara paksa tanpa melalui akses *face recognition* dan *fingerprint* yang dideteksi oleh sensor *magnetic door switch* MC-38. Saat pintu terbuka sensor dalam keadaan *normally open* yang mana jika seseorang masuk tanpa melalui akses kedua input, maka sistem akan menyalakan alarm dan mengirim notifikasi Telegram sebagai notifikasi tanda bahaya.

## 2. METODOLOGI PENELITIAN

Dalam penelitian yang telah dilakukan, penulis menggunakan metode “*Research And Development (R&D)*” yang berarti Penelitian dan Pengembangan. Pengertian Penelitian dan Pengembangan atau *Research And Development (R&D)* sering diartikan sebagai suatu proses atau langkah – langkah untuk mengembangkan suatu produk baru atau menyempurnakan produk yang telah ada. Dalam penelitian yang telah dilakukan, penulis menggunakan metode “*Research And Development (R&D)*” yang berarti Penelitian dan Pengembangan. Pengertian Penelitian dan Pengembangan atau *Research And Development (R&D)* sering diartikan sebagai suatu proses atau langkah – langkah untuk mengembangkan suatu produk baru atau menyempurnakan produk yang telah ada. Penelitian ini dimulai dari melakukan beberapa tahapan dalam perancangan serta pengembangan dari alat yang akan dibuat yaitu sebagai berikut:

### 2.1. Studi Literatur

Studi literatur merupakan tahapan yang dilakukan dengan cara mencari referensi landasan teori yang relevan dengan kasus atau permasalahan yang akan diteliti. Referensi tersebut bisa dicari dari buku, jurnal artikel laporan penelitian, dan situs – situs online di internet. Output yang dihasilkan dari studi literatur ialah terkoleksinya referensi yang relevan dengan rumusan masalah.

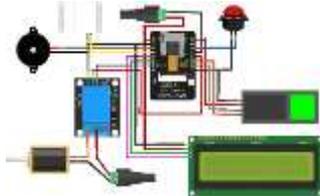
## 2.2. Perancangan Hardware

Pada tahap ini merupakan tahap perancangan hardware dari sistem keaman yang akan dibuat, pada tahap ini akan dilakukan beberapa tahapan diantaranya perancangan diagram sistem keamanan ruang server, perancangan wiring atau pengkabelan komponen, dan perancangan *box*.

### 2.1.1. Perancangan Wiring Hardware

Setelah selesai dengan perancangan hardware, maka akan dilanjutkan pada tahapan perancangan *wiring* atau pengkabelan dari semua komponen yang digunakan.

1. *Power supply* memberi sumber tegangan terhadap ESP32-CAM dan relay, sehingga peralatan dapat berfungsi dengan baik.
2. ESP32-CAM sebagai pusat kontrol yang menerima input dari pengenalan wajah yang menggunakan kamera OV2640 dan sidik jari menggunakan sensor *fingerprint* FPM10A untuk membuka *solenoid door lock* bagi yang sudah terdaftar pada sistem.
3. *Buzzer* digunakan sebagai alat pemberitahuan jika pengenalan wajah dan sidik jari yang diinputkan oleh sensor sesuai atau tidak sesuai. Maka saat *solenoid* terbuka artinya input sudah sesuai dan akan ada bunyi dari *buzzer* sebagai output kemudian data orang yang masuk akan dikirimkan melalui Telegram.
4. Sensor *magnetic door switch* MC-38 berfungsi memberikan informasi tentang keadaan pintu kepada mikrokontroler. Pada saat keadaan pintu terkunci secara otomatis posisi dari sensor pintu dalam keadaan *normally close*, jika pada posisi pintu terkunci namun sensor pintu dalam keadaan *normally open* maka artinya pintu tersebut dibuka secara paksa. Dengan demikian dapat mendeteksi adanya pihak tak berkepentingan yang masuk secara paksa melalui pintu tersebut, maka *buzzer* akan menyala kemudian informasi tersebut akan dikirimkan ke pemilik melalui Telegram.
5. LCD digunakan sebagai *interface* yang menampilkan informasi terkait sistem.
6. *Push button* digunakan sebagai tombol pembuka kunci dari dalam ruangan.



**Gambar 1. Wiring Diagram / Pengkabelan Dari Hardware**

### 2.1.2. Perancangan Software



**Gambar 2. Flowchart Pendaftaran ID Pengguna**

Gambar 2. merupakan diagram alir proses pendaftaran ID pengguna yang dijelaskan bahwa pendaftaran ID dimulai dari mengirim pesan melalui bot Telegram. Kemudian sistem akan mengecek kapasitas *database* untuk mengambil nomor slot kosong pada *database* secara berurutan 1 sampai 5, namun jika slot sudah penuh maka akan direspon pesan Telegram “invalid”. Setelah itu dilakukan proses pembuatan *unique ID* untuk nama, wajah, dan sidik jari. Kemudian melakukan proses pendaftaran wajah dengan mengambil sampel citra wajah yang disimpan pada ID wajah. Setelah itu melakukan pendaftaran sidik jari yang disimpan pada ID sidik jari. Setelah ID nama, wajah, dan sidik jari sudah terkumpul maka sistem akan menyimpan data tersebut ke dalam *database*. Berikut adalah cara melakukan pendaftaran, penghapusan, dan *monitoring* ID pengguna:

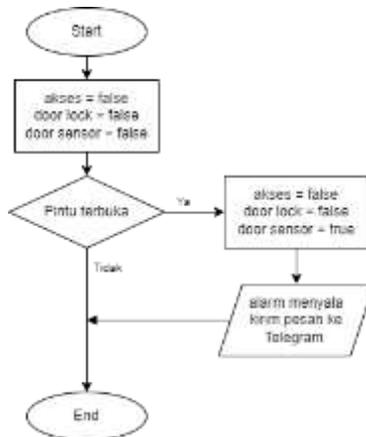
#### 1. Proses pendaftaran ID pengguna

- Buka bot Telegram Ruang server\_skrripsi.
- Ketik “daftar <nama>” kemudian kirim. Tunggu sampai muncul balasan “pendaftaran diproses”.
- Perhatikan instruksi pada LCD. Arahkan wajah pada kamera sampai proses pendaftaran wajah selesai yang ditampilkan pada status bar LCD sampai muncul keterangan “selesai”. Ketika alat mendeteksi sebuah wajah dengan model MTMN maka sampel wajah akan di *enroll* atau disimpan dengan *unique ID* pada *database*.
- Setelah *face recognition* selesai selanjutnya masuk pendaftaran sidik jari, pada LCD muncul tulisan “Tempelkan jari”. Tempelkan jari pada sensor *fingerprint* sampai sensor mendapatkan ID yang disimpan ke *database*. Proses pendaftaran selesai.

#### 2. Proses penghapusan ID pengguna

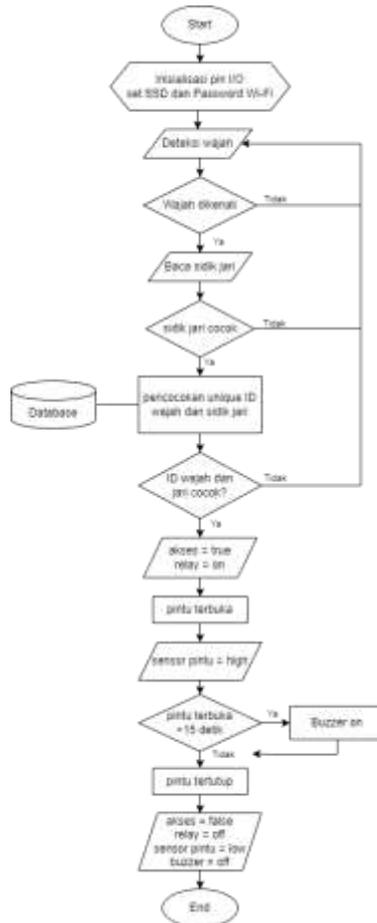
- Buka bot Telegram Ruang server\_skrripsi.
- Ketik “hapus <nama>” kemudian kirim.
- Tunggu sampai muncul balasan “penghapusan berhasil”.
- Selesai.

3. Proses monitoring ID pengguna yang terdaftar pada sistem
- Buka bot Telegram Ruang server\_skripsi.
  - Ketik “lihat” kemudian kirim.
  - Tunggu sampai muncul balasan yang memberikan informasi pengguna terdaftar, slot terpakai, dan slot tersisa.



**Gambar 2. Perancangan Proses Deteksi Pembobolan Pintu**

Gambar 3. merupakan gambar diagram alir perancangan proses jika terdeteksi pembobolan pintu pada ruang server. Pada keadaan normal pintu tertutup akses, *solenoid door lock*, dan sensor pintu dalam keadaan *false*. Pada saat pintu terbuka maka sensor *magnetic door switch* MC-38 dalam keadaan *normally open* dan pada saat pintu tertutup sensor pintu dalam keadaan *normally close*, pada setiap keadaan tersebut sensor *magnetic door switch* MC-38 akan memberikan informasi tentang keadaan pintu kepada mikrokontroler. Pada saat keadaan pintu terkunci secara otomatis posisi dari sensor *magnetic door switch* MC-38 dalam keadaan *normally close*, jika pada posisi pintu terkunci namun sensor *magnetic door switch* MC-38 dalam keadaan *normally open* tanpa melalui akses *face recognition* dan *fingerprint* maka artinya pintu tersebut dibuka secara paksa. Dengan demikian sensor pintu dalam keadaan *true* yang mendeteksi adanya pihak tak berkepentingan masuk secara paksa melalui pintu tersebut sehingga sensor *magnetic door switch* MC-38 akan mengirimkan sinyal ke mikrokontroler untuk mengaktifkan alarm dari *buzzer* dan mengirim notifikasi berupa pesan singkat ke Telegram.



Gambar 3. Perancangan Proses Membuka Pintu

Gambar 4. merupakan gambar diagram alir proses membuka pintu ruang server. Dimulai dengan sistem melakukan koneksi Wi-Fi untuk terhubung ke Telegram. Kemudian melakukan proses deteksi wajah terlebih dahulu dengan mengarahkan wajah ke kamera. Selanjutnya ESP32-Cam akan terus menjalankan model MTMN untuk mendeteksi sebuah wajah. Jika wajah terdeteksi dengan model MTMN maka sampel wajah yang terdeteksi akan diambil kemudian dicocokkan. Dalam proses pencocokkan wajah sample citra wajah yang ada pada *database* akan diekstraksi lalu dilakukan pencocokkan dengan metode FRMN. Setelah proses pencocokkan wajah dan hasilnya wajah dapat dikenali selanjutnya adalah proses pencocokkan sidik jari menggunakan jari tangan yang sudah didaftarkan pada sistem. Sistem akan mencocokkan ID wajah dan ID sidik jari pengguna dengan database, jika keduanya dikenali maka *relay* akan aktif dan *solenoid door lock* akan terbuka. Sistem akan menunggu pintu dibuka selama 10detik. Jika pintu sudah terbuka maka sensor *magnetic door switch* MC-38 akan aktif *HIGH*. kemudian sistem menunggu pintu ditutup selama 15detik. Jika lebih dari 15 pintu belum tertutup maka *buzzer* akan *ON* untuk mengingatkan agar pintu segera ditutup kembali. Setelah pintu tertutup buzzer akan *OFF* dan sensor pintu akan aktif *LOW*.

### 3. HASIL DAN PEMBAHASAN

#### 3.1. Hasil Sistem Keamanan Ruang



Gambar 5. Box Sistem Keamanan Dalam Kondisi On

#### 3.2. Pengujian Sensor Kamera ESP32-Cam

Pada tahap ini dilakukan pengujian sensor kamera ESP32-Cam dengan cara menguji jarak objek pada kamera agar bisa menentukan keakuratan sensor ESP32-Cam saat melakukan pengenalan wajah. Posisi wajah dengan kamera harus berhadapan dan sejajar.

Tabel 1. Hasil Pengujian Jarak Sensor Kamera Dengan Wajah

No	Jarak Sensor Dan Wajah	Hasil Deteksi			Akurasi (%)
		Uji 1	Uji 2	Uji 3	
1	10cm	Tidak	Tidak	Tidak	100
2	20cm	Dikenali	Dikenali	Dikenali	100
3	30cm	Dikenali	Dikenali	Dikenali	100
4	40cm	Dikenali	Dikenali	Dikenali	100
5	50cm	Dikenali	Dikenali	Dikenali	100
6	60cm	Dikenali	Dikenali	Dikenali	100
7	70cm	Dikenali	Dikenali	Dikenali	100
8	80cm	Dikenali	Dikenali	Dikenali	100
9	90 cm	Tidak	Tidak	Tidak	100
10	100cm	Tidak	Tidak	Tidak	100

Pada Tabel 1. merupakan hasil dari pengujian jarak sensor kamera dengan wajah dari jarak terdekat 10cm sampai terjauh 100cm. Berdasarkan tabel tersebut pada jarak paling dekat yaitu 10cm objek wajah tidak dapat terdeteksi karena terlalu dekat jadi kamera tidak menangkap keseluruhan wajah. Wajah mulai terdeteksi pada jarak 20cm dan yang paling jauh adalah 80cm. Pada jarak lebih dari 80cm wajah tidak dapat terdeteksi oleh kamera.

### 3.3. Pengujian Sensor Fingerprint FPM10A

Pada tahap ini dilakukan pengujian sensor *Fingerprint* FPM10A dengan cara menempelkan jari tangan pengguna ke permukaan sensor. Pengujian ini menggunakan jari jempol dan telunjuk guna memudahkan fleksibilitas tangan untuk menjangkau sensor. Pengujian ini dilakukan untuk mengetahui bahwa sensor telah bekerja dengan baik dan sesuai dengan sistem kerjanya. Hasil pengujian data tersebut akan disajikan dalam Tabel 2.

**Tabel 2. Pengujian Sensor Fingerprint FPM10A**

No	Pengujian	Jari Tangan	Hasil Deteksi		
			Uji 1	Uji 2	Uji 3
1	Orang ke-1	Telunjuk	Dikenali	Dikenali	Dikenali
		Jempol	Tidak	Tidak	Tidak
2	Orang ke-2	Telunjuk	Dikenali	Dikenali	Dikenali
		Jempol	Tidak	Tidak	Tidak
3	Orang ke-3	Jempol	Dikenali	Dikenali	Dikenali
		Telunjuk	Tidak	Tidak	Tidak
4	Orang ke-4	Jempol	Dikenali	Dikenali	Dikenali
		Telunjuk	Tidak	Tidak	Tidak
5	Orang ke-5	Jempol	Dikenali	Dikenali	Dikenali
		Telunjuk	Tidak	Tidak	Tidak

Dari hasil pengujian sensor *Fingerprint* pada Tabel 2. menunjukkan hasil bahwa tangan yang sudah didaftarkan dapat terdeteksi oleh sensor *fingerprint*. Sedangkan untuk jari yang belum didaftarkan tidak bisa terdeteksi oleh sensor. Dari 3 kali percobaan setiap pengguna sensor mampu mendeteksi dengan tingkat keberhasilan 100%.

### 3.4. Pengujian Akses Masuk Ruang

Pada tahap ini dilakukan pengujian akses masuk ruang server yang bertujuan untuk mengetahui kinerja sesuai dengan perancangan atau tidak meliputi pengujian kamera ESP-32 Cam dan pengujian sensor sidik jari. Pada pengujian ini semua rangkaian hardware sudah diinstalasi sebelumnya dan telah dilakukan pengetesan respon alat secara berkala.

**Tabel 3. Pengujian Akses Masuk Ruang**

No	Pengujian	Jarak kamera dan wajah	Jari Tangan	Validasi LCD	Akses Masuk		
					Uji 1	Uji 2	Uji 3
1	Orang ke-1	30cm	Telunjuk	fifi	Ya	Ya	Ya
2	Orang ke-2	50cm	Telunjuk	faza	Ya	Ya	Ya
3	Orang ke-3	30cm	Jempol	arda	Ya	Ya	Ya
4	Orang ke-4	50cm	Jempol	bima	Ya	Ya	Ya
5	Orang ke-5	30cm	Jempol	dina	Ya	Ya	Ya
6	Orang ke-6	30cm	Telunjuk	-	Tidak	Tidak	Tidak
7	Orang ke-7	50cm	Jempol	-	Tidak	Tidak	Tidak
8	Orang ke-8	30cm	Telunjuk	-	Tidak	Tidak	Tidak

Dari hasil pengujian sitem akses masuk ruang pada Tabel 3. menunjukkan bahwa orang ke 1 sampai 5 berhasil mendapatkan akses masuk ke ruang server karena sudah terdaftar pada sistem. Sedangkan orang ke 6 sampai 8 tidak mendapatkan akses masuk karena tidak terdaftar pada sistem. Pada saat pengguna mendapatkan akses masuk LCD berhasil memvalidasi nama sesuai dengan data pengguna. Setelah melakukan 3 kali uji coba sistem berjalan dengan baik dan sesuai dengan perancangan.

### 3.5. Pengujian Deteksi Pembobolan Pintu

Pada tahap ini dilakukan pengujian sensor *magnetic door switch* MC-38 yang digunakan sebagai deteksi jika terjadi pembobolan pintu. Pengujian ini dilakukan dengan membuka sementara solenoid door lock pada pintu kemudian membuat rekayasa pembukaan pintu tanpa melalui akses face recognition dan fingerprint. Pengujian dilakukan untuk mengetahui alat dapat bekerja sesuai dengan perancangan atau tidak. Hasil pengujian data tersebut akan disajikan pada Tabel 4.

**Tabel 4. Pengujian Deteksi Pembobolan Pintu**

No	Kondisi pintu	Sensor MC-38	Buzzer	Notifikasi Telegram	Respon uji		
					Uji 1	Uji 2	Uji 3
1	Terbuka	High	On	Akses abnormal	√	√	√
2	Tertutup	Low	Off	-	×	×	×

Tabel 4. merupakan hasil pengujian pengujian deteksi pembobolan pintu dalam kondisi tanpa menggunakan akses. Dari hasil pengujian didapatkan hasil jika pintu terbuka maka sistem berhasil menyalakan buzzer dan mengirim notifikasi Telegram. Maka deteksi pembobolan pintu sesuai dengan perancangan sistem.

#### 4. KESIMPULAN

Berdasarkan hasil perancangan sistem keamanan pada brankas yang telah dilakukan sebelumnya untuk mengetahui kondisi yang mungkin terjadi pada sistem, maka dapat disimpulkan sebagai berikut:

1. Telah berhasil dibuat sistem keamanan ruang server yang hanya bisa diakses oleh orang yang sudah terdaftar pada sistem. Jumlah slot pada sistem hanya 5 pengguna dikarenakan penyimpanan pada ESP32-Cam hanya sebesar 4mb. Pengguna yang tidak terdaftar maka tidak akan bisa membuka pintu tersebut.
2. Sistem pengenalan wajah (*face recognition*) bekerja sesuai rencana yang dibuat. Sensor kamera mampu mendeteksi wajah mulai jarak 20cm sampai 80cm dapat menangkap citra wajah dengan baik.
3. Pada hasil pengujian fingerprint hasil yang didapatkan sensor sidik jari bekerja dengan baik dengan tingkat keberhasilan 100%. Pengujian dilakukan dengan menggunakan jari tangan jempol dan telunjuk guna memudahkan fleksibilitas tangan untuk menjangkau sensor.
4. Deteksi pembobolan pintu menggunakan sensor pintu MC38 berfungsi sesuai prinsip kerja, jika terjadi pembukaan pintu tanpa melalui sistem akses mampu menyalakan *buzzer* dan mengirim pesan ke Telegram.
5. Hasil pengujian sistem keamanan ruang server menunjukkan secara keseluruhan sistem alat keamanan ini sudah bekerja dengan baik sesuai dengan perancangan dan prinsip kerjanya.

**DAFTAR PUSTAKA**

- [1]. Bahri, S., & Suhardiyanto. (2018). Sistem Keamanan Ruang Server Menggunakan Teknologi RFID Dan Password. *Jurnal Elektum*, 15(1), 12–18.
- [2]. Nurwijaksana, T., & Candra, R. (2021). Access Server Room Using RFID Implemented for Security. *Agustus*, 20(3), 411–419.