Perancangan Sistem Keamanan Ruang Server Akses Doorlock Dengan Teknologi RFID (*Radio Frequency Identification*) Berbasis IoT Pada Ruang Server FISIP UNJANI

Ade Sena Permana [1*)], Jumagar Arthady Sormin [2)], Ni Ketut H.D [3)]

[1,2,3)]Program Studi Teknik Elektro
Universitas Jenderal Achmad Yani
Jalan Terusan Jend. Sudirman PO.BOX 148 Cimahi 40531

[*)]Korespondensi : adesena@unjani.ac.id

Abstrak
Keamanan pada server data diperlukan untuk mengamankan semua data yang dimiliki oleh suatu instansi. Pengembangan akses keamanan ke ruang server juga perlu ditingkatkan untuk melindungi semua data yang dimiliki oleh instansi tersebut. Pada penelitian ini, peneliti merancang suatu alat keamanan dimana pengguna yang mengakses ke ruang server harus melewati sistem keamanan *doorlock* yang berbasis IoT (*Internet of Things*). Sistem keamanan *doorlock* ini menggunakan teknologi RFID yang selanjutnya data yang diakses diproses oleh raspberry untuk mengirimkan data pengakses ke web server. Hasil perancangan sistem keamanan server akses *doorlock* ke ruang server dengan teknologi RFID berbasis IoT pada proyek NEW UNJANI pada jarak maksimal 2 cm antara RFID *tag* dengan RFID dengan tingkat keberhasilan pembacaan RFID *reader* ke RFID *tag* 100%. Pengujian selanjutnya RFID *tag* diberikan media lain, yaitu dompet dan *cover card* yang pengujiannya mendapatkan persentasi keberhasilan 100%. Dengan hasil tersebut, peneliti kembali menguji 3 buah RFID *tag* yang memiliki jenis berbeda. Setiap RFID *tag* dilakukan pengujian 50 kali, sehingga total dilakukan pengujian sebanyak 150 kali. Untuk pengujian RFID *tag* pertama mendapatkan persentasi kegagalan sebesar 26%. Untuk pengujian RFID *tag* kedua mendapatkan persentasi kegagalan sebesar 20%. Untuk pengujian RFID *tag* ketiga mendapatkan persentasi keberhasilan sebesar 100%. Pengujian alat termasuk efektif dikarenakan pada pengujian pertama dan kedua memiliki persentasi keberhasilan tinggi, yang dimana kegagalan dari alat mendapatkan kesalahan dikarenakan jaringan hotspot yang di terima perangkat tidak stabil, dan alasan lainnya pada pengujian ketiga RFID *tag* yang tidak terdaftar dan tidak memiliki akses mendapatkan persentasi keberhasilan 100% yang mengartikan tidak akan ada akses pada orang yang tidak mendaftarkan RFID *tag* tersebut.

Kata kunci : *Doorlock,* IoT (*Internet of Things*), RFID, web server, API

Abstract
Security on the data server is needed to secure all data owned by an agency. The development of security access to the server room also needs to be improved to protect all data owned by the agency. This makes user-owned data sets very secure. In this study, researchers designed a security tool where users who access the server room must pass a doorlock based on IoT (Internet of Things). Security system doorlock uses RFID technology which is then processed by the raspberry accessed data to send the accessing data to the web server. The results of the design of a doorlock access server security system to the server room with IoT-based RFID technology in the NEW UNJANI project at a maximum distance of 2 cm between RFID tags and RFID with a 100% success rate of reading RFID reader to RFID tag. Further testing of RFID tags is given other media, namely wallets and cover cards whose tests get a 100% success percentage. With these results, the researcher again tested 3 RFID tags that have different types. Each RFID tag was tested 50 times, so that a total of 150 tests were carried out. For the first RFID tag , the failure percentage was 26%. For the second RFID tag , the failure percentage is 20%. For the third RFID tag , the success percentage is 100%. Tool testing is effective because the first and second tests have a high percentage of success, where the failure of the tool gets an error because the hotspot network received by the device is unstable, and other reasons in the third test are RFID tags that are not registered and don't have access to get a success percentage 100% which means there will be no access to people who do not register the tag.

***Keywords** : Doorlock, IoT (Internet of Things), RFID, web server, API*

I. PENDAHULUAN

Info Makalah:
Dikirim : 11-07-2022;
Revisi 1 : 12-25-2022;
Diterima : 01-03-2022.

Penulis Korespondensi:
Telp : +62-81223-15056
e-mail : adesena@unjani.ac.id

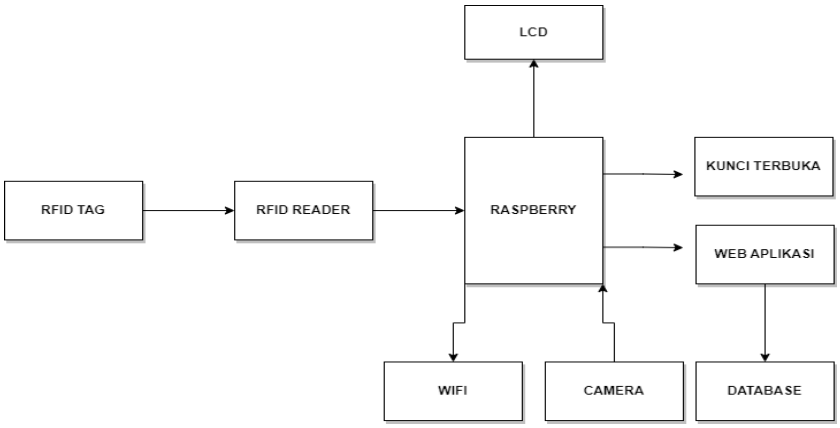
Ketika penggunaan perangkat berbasis sistem jaringan meningkat, penjahat di dunia maya akan menargetkan suatu instansi atau sistem [1]. Banyak organisasi menghadapi tantangan terbesar dalam memantau ancaman berbasis jaringan, terutama di sektor-sektor yaitu pemerintahan, energi [2], kesehatan, bank, pusat penilitian. Selain itu, sektor-sektor ini berinvestasi dalam alat pemantauan keamanan untuk melindungi dan melindungi infrastruktur [3].

Tujuan dari penelitian ini adalah untuk membuat dan menganalisis pengamanan akses untuk memasuki server, dimana pengamanan yang digunakan adalah *Radio Frequency Identification* (RFID) dengan mikrokontroller yang digunakan adalah Raspberry 3B+ yang kemudian akan disambungkan dengan perangkat IoT. Peneliti akan mendapatkan informasi yaitu siapa saja yang mengakes server lalu berapa lama subjek berada di server sehingga akses ke server diharapkan lebih terpantau dan aman.

II. METODE

A. Diagram Blok Sistem

Dalam perancangan sistem jaringan ini memiliki beberapa blok sistem yang dimana setiap blok terkait satu sama lain. Bagian pertama di Gambar 1 adalah pembacaan *tag* oleh RFID Reader. Tahap selanjutnya RFID akan memberikan sinyal keluaran ke Raspberry Pi dan akan mengaktifkan indikator. Setelah data yang sesuai dengan *database* didapatkan oleh Raspberry Pi, maka kunci pintu akan terbuka, kamera akan aktif memotret dan data subjek yang mengakses akan ditampilkan di perangkat yang sudah disiapkan.



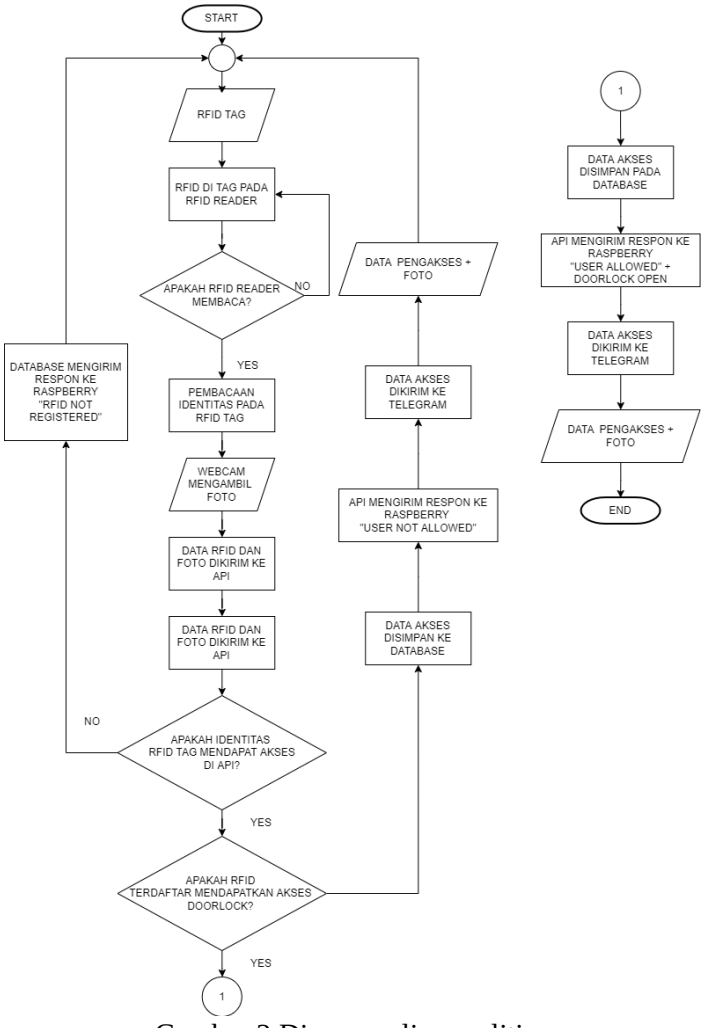
Gambar 1 Diagram blok sistem

B. Diagram Alir Penelitian

Perancangan dan perbandingan sistem jaringan ini dilakukan dengan beberapa tahapan seperti Gambar 2 yang terorganisir dan melalui beberapa proses yang memerlukan waktu lebih. Mulai dari mempersiapkan bahan dan peralatan yang digunakan, pembuatan koding lalu *trial and error*. Hal-hal tersebut sangat penting untuk membuat sebuah sistem keamanan secara langsung yang dimana hal ini akan menjadi pertimbangan bagi pegiat usaha ataupun sebagai bahan *study*. Berikut merupakan diagram alir pembuatan sistem keamanan server dengan teknologi IoT [4].

RFID *tag* yang akan digunakan disiapkan untuk dilakukan pengujian. RFID *tag* di tap pada RFID *reader*. Perangkat akan memberikan pilihan apakah RFID *tag* terbaca atau tidak, ketika tidak membaca maka proses akan kembali di ulang ke tahap RFID *tag* di tap pada RFID *reader*, tetapi jika berhasil maka proses selanjutnya berjalan. Pembacaan identitas pada RFID dilakukan raspberry. Perangkat akan mengambil gambar pada subjek yang mengakses pintu dengan RFID *tag* yang dimiliki. Selanjutnya data yang telah dikumpulkan dikirimkan ke API yang selanjutnya akan di proses ke bagian web server. Pada tahapan selanjutnya API akan memastikan apakah RFID *tag* yang terbaca sudah diberikan akses pada API atau belum. Jika belum mendapatkan akses maka API akan mengirim sinyal ke raspberry dan LCD

akan menampilkan "*RFID not registered*", lalu akan dikembalikan ke proses awal, tetapi jika sudah didaftarkan pada API maka akan lanjut ke tahap selanjutnya [5]. Pada tahap ini, API akan memastikan kembali pada RFID *tag* yang terbaca apakah memiliki akses untuk *doorlock* atau tidak. Ketika RFID *tag* tidak memiliki akses maka akan berlanjut ke tahap selanjutnya penyimpanan data. Pada tahap ini ketika RFID *tag* tidak memiliki akses untuk membuka *doorlock* maka *database* akan menyimpan data subjek yang melakukan tap akses yang dimana API akan melakukan tugasnya selanjutnya. API akan mengirimkan sinyal pada raspberry dimana raspberry akan mengirim sinyal pada LCD yang menampilkan "*User not allowed*". Pada tahap ini juga data subjek akan dikirim ke telegram yang dimana semua informasi akan ditampilkan. Informasi yang dikirimkan berupa foto dan data pengakses, lalu proses dikembalikan ke proses awal kembali. Pada tahapan lain, dimana RFID *tag* yang digunakan memiliki akses *doorlock.* Maka tahapan ini selanjutnya data subjek yang mengakses *doorlock* akan di simpan di *database*. Tahapan selanjutnya API akan mengirimkan sinyal pada raspberry dimana raspberry akan menampilkan pada LCD "*User Allowed*" dan pada tahap ini juga *doorlock* akan terbuka. Tahap selanjutnya data subjek akan akan dikirimkan ke telegram dimana semua informasi akan di tampilkan. Informasi yang dikirimkan berupa foto dan data pengakses.



Gambar 2 Diagram alir penelitian

C. Perangkat Keras

Perangkat keras yang digunakan dalam perancangan sistem keamanan ruang server dengan akses *doorlock*. Dalam sistem ni, yang menjadi perhatian khusus sebagai perangkat keras diantaranya raspberry 3B+, *webcam*, RFID *reader*, RFID *tag*, LCD dan motor *servo* sebagai indikator *lock system.*

1. RFID RC522

Modul RFID RC522 pada Gambar 3 berdasarkan IC MFRC522 dari NXP adalah salah satu opsi RFID paling murah. Biasanya dilengkapi dengan *tag* kartu RFID dan *tag* fob kunci yang memiliki memori 1KB [6]. *Tag* dapat diisi, sehingga dapat menyimpan semacam pesan di dalamnya. Modul Pembaca RFID RC522 dirancang untuk menciptakan medan elektromagnetik 13,56MHz yang digunakan untuk berkomunikasi dengan *tag* RFID (*tag* standar ISO 14443A) [7]. Pembaca dapat berkomunikasi dengan mikrokontroler melalui 4-pin *Serial Peripheral Interface* (SPI) dengan kecepatan data maksimum 10Mbps. Ini juga mendukung komunikasi melalui protokol I2C dan UART [8]. Modul dilengkapi dengan pin interupsi. Ini berguna karena alih-alih terus-menerus menanyakan modul RFID, modul akan mengingatkan ketika sebuah *tag* datang ke sekitarnya. Tegangan operasi modul adalah dari 2,5 hingga 3,3V, tetapi kabar baiknya adalah bahwa pin logika toleran 5 volt, sehingga dapat dengan mudah menghubungkannya ke Arduino atau mikrokontroler logika 5V tanpa menggunakan konverter level logika lainnya [9].

Gambar 3 RFID RC522

2. *Webcam Logitech C270*

Webcam atau kamera web pada Gambar 4 pada dasarnya adalah kamera digital yang terhubung dengan komputer yang mengambil gambar yang akan diproses oleh komputer. Awalnya, *webcam* digunakan sebagai alat komunikasi yang menampilkan serangkaian gambar dan dapat diakses melalui *world wide web*. Namun, saat mengembangkan webcam juga digunakan untuk tujuan lain. Jenis webcam yang digunakan adalah Logitech C270 dengan beberapa fitur utama sebagai berikut :

a. Panggilan video (1280 x 720 pixels).
b. Perekaman video hingga 1280 x 720 pixels.
c. Foto hingga 3.0 megapixels.
d. Mikrofon dengan teknologi Logitech Right Sound.
e. USB 2.0 tersertifikasi berkecepatan tinggi.

Dengan spesifikasi sebagai berikut :

a. *High Definition (HD) video calling* (1280 x 720 pixels).
b. *Video capture* : sampai 1280 x 720 pixels.
c. Foto : sampai 3.0 megapixels.
d. Mikrofon internal dengan teknologi teknologi Logitech Right SoundTM.
e. *Hi-speed* USB 2.0 bersertifikat.
f. Klip universal untuk laptop, monitor LCD atau CRT [10].

Gambar 4 Kamera Logitech C270

3. Raspberry Pi 3B+

Raspberry Pi adalah papan komputer dengan biaya rendah, ukuran kecil dan portabel. Hal ini dapat digunakan untuk plug-in ke monitor komputer atau televisi, *keyboard*, *mouse*, *pen-drive* dan lainnya [11]. Raspberry Pi telah dibangun di *software* seperti *Scratch* yang memungkinkan pengguna untuk program dan desain animasi, permainan atau video yang menarik. Selain itu, programmer juga dapat mengembangkan script atau program dengan menggunakan bahasa *Python*; itu adalah bahasa inti utama dalam sistem operasi Raspbian. Raspberry Pi B+ adalah evolusi dari Model B. Bahasa *Python* telah digunakan dalam pekerjaan ini untuk menulis skrip untuk komunikasi klien/server [12]. Selain itu, ada peningkatan seperti menambahkan lebih banyak PIN header GPIO, lebih banyak port USB, konsumsi daya yang lebih rendah, dll. Disarankan untuk menggunakan model B+ untuk pembelajaran di sekolah karena menawarkan lebih banyak fleksibilitas daripada model A terutama untuk proyek yang disematkan dan juga membutuhkan daya yang rendah. Sebagai menyediakan lebih banyak port USB dibandingkan dengan Model B [13].

Raspberry Pi 3 model B+ merupakan versi terbaru dari minicomputer yang dirilis oleh Raspberry Pi sebagai evolusi dari Raspberry Pi versi sebelumnya dan merupakan penerus dari Raspberry Pi B yang telah dirilis sebelumnya. Desain fisik model B Raspberry Pi B dan Raspberry Pi B+ di Gambar 5 adalah sama [14].

Gambar 5 Raspberry pi 3B+

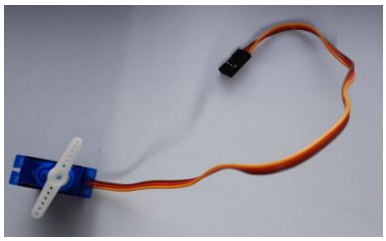
Perangkat lunak sistem yang mengatur sumber daya dari perangkat keras dan perangkat lunak, serta sebagai *daemon* untuk program komputer. Sistem operasi sangat menentukan seperti apa sistem akan diolah. Pada perancangan sistem keamanan ruang server akses *doorlock* menggunakan *Raspbian* dengan *Linux raspberrypi*. Adapun spesifikasi *raspberry pi* 3B+ yang ditunjukan pada Tabel 1. berikut :

Tabel 1. Spesifikasi raspberry pi 3B+ [15]

Spesifikasi	***Raspberry Pi 3B+***
CPU	BCM2837B0 64-bit Quad-Core Cortex-A53 @ 1.4 GHz
RAM	1 GB LPDDR2
GPU	Broadcom VideoCore IV @ 400 MHz
Output Video	1x HDMI
Resolusi	2560 x 1600
Output Audio	Audio Jack 3.5 mm
Wifi	802.11b/g/n/ac Dual Band @ 2.4 GHz & 5 GHz
Bluetooth	Bluetooth 4.2
Ethernet	Gigabit Ethernet Via USB 2.0 @ 300 Mbps
USB	4x USB 2.0
Catu Daya	5V @ 2.5A
Port Catu Daya	Micro USB
GPIO	40 in

4. *Locked Door* (Motor Servo)

Motor servo seperti Gambar 6 adalah aktuator putar atau motor yang memungkinkan kontrol presisi dalam hal posisi sudut, akselerasi, dan kecepatan. Itu membuat penggunaan motor biasa lebih baik dan melakukan operasi tipe khusus daripada motor biasa. Motor Servo SG90 digunakan untuk prototipe sistem [16].



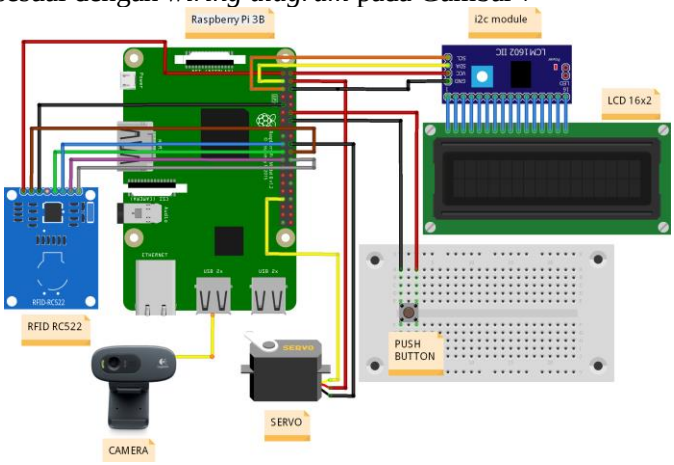
Gambar 6 Motor servo indikator *doorlock*

D. Prosedur Pengujian

Untuk melakukan perancangan dan penelitian, terdapat beberapa tahapan untuk merancang perangkat tersebut, langkah-langkahnya sebagai berikut:

a. Perancangan perangkat keras.

Komponen dirancang sesuai dengan *wiring diagram* pada Gambar 7



Gambar 7 Wiring diagram sistem keamanan

b. Pembuatan *bootable*

Persiapkan satu komputer atau laptop untuk melakukan konfigurasi. Monitor dapat dipersiapkan untuk melakukan konfigurasi awal pada raspberry. Keyboard dan mouse dengan USB untuk melakukan konfigurasi. SD Card dipersiapkan dengan ukuran penyimpanan minimal 32GB. *Card Reader* dipersiapkan untuk membuat *bootable*. SD Card dimasukan ke *card reader*, dan selanjutnya di sambungkan ke komputer atau laptop. Download Raspberry PI Imaginer menggunakan link https://downloads.raspberrypi.org/imager/imager_latest.exe_ *File installer* dengan "*Install*" di klik, dan hasil ditunggu hingga proses selesai. Tombol *finish* diklik ketika proses instalasi sudah selesai, dan klik "*Run Raspberry Pi Imager*". Dipilih Raspberry PI OS (32-bit). Selanjutnya *choose storage* dipilih sesuai dengan sd card yang sebelumnya sudah disiapkan. Logo "*Setting*" diklik yang ada di kanan bawah untuk konfigurasi *username*, *password*, *enable* SSH dan WiFi. Opsi pengaturan disesuaikan dan kemudian selanjutnya di *save*. Selanjutnya tombol *write* diklik untuk masuk ke langkah selanjutnya. Selanjutnya proses instalasi dimulai, dan ditunggu sampai proses selesai. Dengan selesainya *bootable*, maka akan muncul *pop up* yang selanjutnya di klik "*Continue*". Setelah di klik "*Continue*", card reader dilepaskan dari komputer atau laptop, dan selanjutnya SD Card dimasukkan ke slot SD Card di Raspberry. Raspberry kemudian dikoneksikan dengan monitor menggunakan *port* HDMI yang ada pada kedua perangkat (Raspberry dan Monitor). Raspberry Pi dihidupkan dengan kabel *micro* USB *charger* HP ke *port* USB di Raspberry. 8. Dengan konfigurasi awal tadi, raspberry sudah secara otomatis terkoneksi dengan wifi. Koneksi wifi dipastikan terhubung dengan internet dengan memastikan masuk ke *browser* pada tahap.

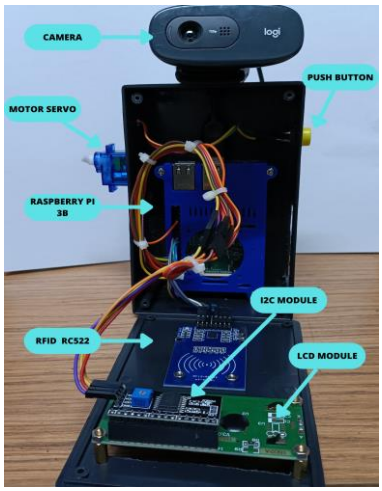
c. Menyiapkan *environtment* agar program yang dibuat dapat berjalan.

Terminal dibuka dengan cara mengklik shortcut yang berada pada barisan ke 4 pada bagian taskbar. Selanjutnya, pada program terminal yang dijalankan, ketik "sudo su" dan tekan enter. Modul modul python diinstal dengan mengetik baris berikut: **"pip install RPi.GPIO mfrc522 rpi_lcd dotenv"**. Raspberry sudah siap, dan dilanjutkan untuk ke tahap pemrograman.

d. Pemrograman Raspberry Pi dilakukan sesuai dengan koding dan instuksi-instruksi khusus.

III. HASIL DAN DISKUSI

Hasil dari perancangan di Gambar 8, alat sistem keamanan ruang server akses *doorlock* menggunakan teknologi RFID berbasis IoT. Pengujian dan analisis bertujuan untuk memastikan apakah perangkat bekerja dengan baik. Analisis dilakukan terdapat hasil yang ditujukan selama pengujian.



Gambar 8 Hasil perancangan perangkat keras

A. Hasil Pengukuran Kepekaan RFID Tag Dan RFID Reader

Tahap awal melakukan pengujian jarak pada RFID *tag* dan RFID *reader* yang didapat hasil pada Tabel 2.

Tabel 2 Hasil pengukuran jarak ukur pada RFID *tag* dan RFID *reader*

Distansce	Frequency									
	1st	2nd	3rd	4st	5st	6st	7st	8st	9st	10st
1 cm	√	√	√	√	√	√	√	√	√	√
1.5 cm	√	√	√	√	√	√	√	√	√	√
2 cm	√	√	√	√	√	√	√	√	√	√
2.5 cm	χ	χ	χ	χ	χ	χ	χ	χ	χ	χ
3 cm	χ	χ	χ	χ	χ	χ	χ	χ	χ	χ
Dengan dompet	√	√	√	√	√	√	√	√	√	√
Dengan IDCard	√	√	√	√	√	√	√	√	√	√

$$Persentasi\ keberhasilan = \frac{Jumlah\ keberhasilan\ pengujian\ jarak}{Total\ pengujian} \times 100\% \quad (1)$$
$$= \frac{30}{50} \times 100\%$$
$$= 60\%$$

B. Hasil Pengujian RFID Tag Yang Terdaftar

Tabel 3 Hasil pengujian RFID *tag* yang terdaftar

Frek	*Berhasil/Gagal*	*Mulai Tap Kartu*	*Mulai Ambil Gambar*	*Menyimpan Gambar*	*Mengirim Data ke Server*	*Respon dari Server*	*Waktu Total*
1	√	16:03:50	16:03:52	16:03:55	16:03:55	16:03:58	0:00:08
2	√	16:04:04	16:04:06	16:04:10	16:04:10	16:04:13	0:00:09
3	√	16:04:18	16:04:21	16:04:24	16:04:24	16:04:28	0:00:10
4	√	16:04:33	16:04:35	16:04:39	16:04:39	16:04:43	0:00:10
5	√	16:04:49	16:04:51	16:04:54	16:04:55	16:04:58	0:00:09
6	√	16:05:03	16:05:05	16:05:09	16:05:09	16:05:13	0:00:10
7	√	16:05:18	16:05:21	16:05:24	16:05:24	16:05:28	0:00:10
8	√	16:05:34	16:05:36	16:05:39	16:05:39	16:05:43	0:00:09
9	√	16:05:48	16:05:50	16:05:54	16:05:54	16:05:57	0:00:09
10	χ	16:06:03	16:06:05	16:06:05			0:00:02
…							
50	√	16:13:53	16:13:55	16:13:59	16:13:59	16:14:02	0:00:09
Rata - rata waktu delay							0:00:07

$$Persentasi\ kegagalan = \frac{Jumlah\ kegagalan\ pengujian}{Total\ pengujian} \times 100\% \qquad (2)$$
$$= \frac{13}{50} \times 100\%$$
$$= 26\%$$

Dari 50x pengujian yang diatas terdapat kesalahan sebesar 26 % itu dikarenakan oleh pembacaan dari mikrokontroler yang dimana proses berhenti sampai penyimpanan gambar. Ketika mikrokontroler mendapatkan sinyal hotspot yang kurang stabil sehingga perangkat tidak dapat mengirimkan sinyal pada web server dimana *database* tersimpan. Hal ini sangat berpengaruh ke perangkat dikarenakan perangkat data yang bisa mengakses diambil di web server yang dimana *database* tersebut tersimpan dan pada percobaan ini RFID *tag* yang memiliki akses akan melanjutkan proses sampai mengirimkan data.

C. Hasil Pengujian RFID Tag Yang Tidak Terdaftar

Dari 50x pengujian yang tabel 4 terdapat kesalahan sebesar 20 % itu dikarenakan oleh pembacaan dari mikrokontroler yang dimana proses berhenti sampai penyimpanan gambar. Sama dengan percobaan RFID *tag* yang memiliki akses ketika mikrokontroler mendapatkan sinyal hotspot yang kurang stabil sehingga perangkat tidak dapat mengirimkan sinyal pada web server dimana *database* tersimpan. Hal ini sangat berpengaruh ke perangkat dikarenakan perangkat harus mendapatkan data yang bisa mengakses diambil di web server yang dimana *database* tersebut tersimpan dan pada percobaan ini RFID *tag* yang terdaftar tetapi tidak memiliki akses akan melanjutkan proses sampai mengirimkan data.

Tabel 4 Hasil pengujian RFID *tag* yang tidak terdaftar

Frek	*Berhasil/Gagal*	*Mulai Tap Kartu*	*Mulai Ambil Gambar*	*Menyimpan Gambar*	*Mengirim Data ke Server*	*Respon dari Server*	*Waktu Total*
1	χ	16:15:00	16:15:02	16:15:03			0:00:03
2	χ	16:15:06	16:15:09	16:15:09			0:00:03
3	√	16:15:12	16:15:15	16:15:18	16:15:18	16:15:21	0:00:09
4	√	16:15:27	16:15:29	16:15:32	16:15:32	16:15:36	0:00:09
5	√	16:15:41	16:15:44	16:15:47	16:15:47	16:15:50	0:00:09
6	√	16:15:56	16:15:58	16:16:02	16:16:02	16:16:05	0:00:09
7	√	16:16:10	16:16:13	16:16:16	16:16:16	16:16:20	0:00:10
8	√	16:16:25	16:16:27	16:16:31	16:16:31	16:16:34	0:00:09
9	√	16:16:39	16:16:42	16:16:45	16:16:45	16:16:49	0:00:10
10	√	16:16:54	16:16:56	16:17:00	16:17:00	16:17:03	0:00:09
…							
50	√	16:25:26	16:25:28	16:25:32	16:25:32	16:25:35	0:00:09
Rata - rata waktu delay							0:00:08

$$Persentasi\ kegagalan = \frac{10}{50} \times 100\% = 20\%$$

D. Hasil Pengujian RFID Tag Yang Tidak Terdaftar Dan Tidak Memiliki Akses

Tabel 5 Hasil pengujian RFID *tag* yang tidak terdaftar dan tidak memiliki akses

Frek	***Berhasil/Gagal***	***Mulai Tap Kartu***	***Mulai Ambil Gambar***	***Menyimpan Gambar***	***Mengirim Data ke Server***	***Respon dari Server***	***Waktu Total***
1	χ	16:26:27	16:26:30	16:26:33			0:00:06
2	χ	16:26:41	16:26:43	16:26:47			0:00:06
3	χ	16:26:55	16:26:57	16:27:01			0:00:06
4	χ	16:27:08	16:27:11	16:27:11			0:00:03
5	χ	16:27:14	16:27:17	16:27:20			0:00:06
6	χ	16:27:27	16:27:30	16:27:33			0:00:06
7	χ	16:27:41	16:27:43	16:27:47			0:00:06
8	χ	16:27:54	16:27:57	16:27:57			0:00:03
9	χ	16:28:00	16:28:03	16:28:03			0:00:03
10	χ	16:28:06	16:28:09	16:28:12			0:00:06
…							
50	χ	16:35:57	16:35:59	16:36:02			0:00:05
Rata - rata waktu delay							0:00:05

$$Persentasi\ Keberhasilan = \frac{50}{50} \times 100\% = 100\%$$

Dari 50x pengujian yang diatas terdapat keberhasilan sebesar 100 % dimana RFID *tag* tidak dilanjutkan proses setelah pembacaan RFID *reader* di raspberry. Hal itu dikarenakan oleh data pada RFID *tag* yang ketiga ini tidak terdaftar sama sekali pada *database* sehingga perangkat hanya bisa melakukan proses sampai penyimpanan gambar sehingga proses pengiriman informasi yang dilakukan oleh API tidak terkirim ke telegram admin dan *doorlock* tidak akan terbuka.

E. Analisis

Pengujian pertama pada Tabel 2 dengan mengukur jarak dari antara tag dengan *reader* dilakukan dengan berbagai jarak. Pengujian yang dilakukan sebanyak 10 kali setiap jarak nya membuat pengujian mendapatkan beberapa hasil yang didapat penguji. Pengujian pertama pada jarak 1 cm, RFID *reader* dapat membaca RFID tag dengan baik dimana dari 10 kali pengujian semua dapat terbaca dengan baik. Dengan ditambah jarak pengujian sejauh 1,5 cm, kembali RFID *reader* dapat membaca kembali dengan baik RFID tag sebanyak 10 kali pengujian. Pengujian selanjutnya menambahkan kembali jarak dari RFID tag ke RFID *reader* sejauh 2 cm dan dengan ditambahnya jarak pembaca masih sangat baik dan RFID reader membaca RFID tag sebanyak 10 kali pengujian. Pada pengujian selanjutnya dengan menambahkan jarak sejauh 2,5 cm dan 3 cm antara RFID tag dan RFID *reader* didapatkan hasil dimana RFID *reader* sudah tidak dapat membaca RFID tag. Maka pada jarak tempuh yang dapat dipindai oleh RFID *reader* adalah sejauh 2 cm. Pada pengujian jarak maka didapat persentasi keberhasilan pembacaan perangkat sebesar 60%.

Pada pengujian selanjutnya masih pada Tabel 2, dilakukan pengujian dengan menempatkan RFID tag pada dompet dan pada *cover card*. Pada pengujian pertama dengan menggunakan dompet, RFID *reader* dapat membaca dengan baik RFID tag yang telah diuji sebanyak 10 kali. Yang selanjutnya, pengujian dengan menggunakan *cover card* pada RFID tag, RFID *reader* dapat membaca dengan baik ketika dilakukan pengujian sebanyak 10 kali. Semua hasil dari pengujian dibaca dengan baik oleh *database* yang ada pada *web server*, dan hasil pengujian dikirim dengan baik pada telegram yang dimana semua data dikirimkan dengan baik. Dengan berhasilnya pengujian ini maka persentasi keberhasilan pembacaan perangkat yaitu 100%.

Pengujian ketiga pada Tabel 3 dimana dilakukan pengujian dengan menggunakan RFID tag yang sudah terdaftar dan memiliki akses pada *database*. Pengujian ini melakukan percobaan sebanyak 50 kali dimana persentasi kegagalan pada percobaan ini sebesar 26% dan pada percobaan keempat yang datanya

ada pada tabel 3 dilakukan pengujian sebanyak 50 kali dimana persentasi kegagalan pada percobaan ini 20%. Dari kedua pengujian ini kegagalan disebabkan oleh mikrokontroler atau raspberry mendapatkan jaringan *hotspot* dari *access point* yang tidak stabil sehingga data tidak dapat dilanjutkan sehingga proses berhenti di penyimpanan gambar. Kedua pengujian ini data yang terbaca dengan baik akan terkirim ke web server untuk dilakukan pengecekan kesesuaian data. Pada Tabel 3 semua data yang berhasil terbaca mengirim respon pada perangkat sehingga *doorlock* terbuka atau motor servo akan berputar sebanyak 180º selama 2 detik. Pada pengujian Tabel 4 semua data yang berhasil terbaca mengirim respon pada perangkat akan tetapi *doorlock* tidak terbuka dikarenakan *user* tidak memiliki akses untuk membuka *doorlock*.

Pada Tabel 5 pengujian dilakukan sebanyak 50 kali dimana persentasi keberhasilan percobaan sebesar 100%. Hal ini disebabkan tidak terdaftarnya RFID tag data pada *database* sehingga semua yang terbaca terhenti di penyimpanan gambar dan membuat alat ini bekerja dengan baik.

IV. KESIMPULAN

Dari hasil pengujian perancangan sistem keamanan ruang server akses doorlock dengan teknologi rfid berbasis iot pada ruang server FISIP UNJANI, maka dapat disimpulkan Pada pengujian jarak, didapatkan persentasi keberhasilan pada jarak didapatkan 60%. Hal ini terjadi dikarenakan jarak pemindaian antara RFID *reader* ke RFID *tag* memiliki jarak makasimal sejauh 2 cm, dan ketika mengukur diatas 2 cm RFID *reader* tidak dapat mendektsi RFID *tag*. Pada pengujian menggunakan media yang telah dilakukan didapatkan hasil dengan persentasi keberhasilan 100%. Media yang digunakan adalah dompet dan *cover card*. Pengujian alat termasuk efektif dikarenakan pada pengujian pertama dan kedua memiliki persentasi keberhasilan tinggi, yang dimana kegagalan dari alat mendapatkan kesalahan dikarenakan jaringan hotspot yang di terima perangkat tidak stabil, dan alasan lainnya pada pengujian ketiga RFID *tag* yang tidak terdaftar dan tidak memiliki akses mendapatkan persentasi keberhasilan 100% yang mengartikan tidak akan ada akses pada orang yang tidak mendaftarkan RFID *tag* tersebut.

DAFTAR PUSTAKA

[1] I. Purnamasari dan M. A. Mustofa, "Optimasi Pemanfaatan Local Area Network dengan 7 Layer Protokol," *Journal of Information System, Informatics and Computing,* vol. 3, no. 2, pp. 9-15, 2019.

[2] N. H. Motlagh, M. Mohammadrezaei dan J. Hunt, "Internet of Things (IoT) and the Energy Sector," *Energies,* vol. 13, no. 494, pp. 1-27, 2020.

[3] Z. Munawar dan N. I. Putri, "Keamanan IoT dengan Deep Learning dan Teknologi Big Data," *TEMATIK - Jurnal Teknologi Informasi dan Komunikasi,* vol. 7, no. 1, p. 161, 2 Desember 2020.

[4] J. D. Irawan, S. Prasetio dan S. Adi, "Pengembangan Kunci Elektronik Menggunakan RFID Dengan Sistem IoT," *Industri Inovatif,* vol. 6, no. 2, pp. 28-32, 2016.

[5] U. Rahardja, Q. Aini dan N. P. L. Santoso, "Pengintegrasian YII Framework Berbasis API pada Sistem Penilaian Absensi," *Jurnal Ilmiah Sisfotenika,* vol. 8, no. 2, pp. 140-152, 2018.

[6] P. Tan, H. Wu, P. Li dan H. Xu , "Teaching Management System with Applications of RFID and IoT Technology," *Education Sciences,* vol. 26, no. 1, p. 8, 2018.

[7] A. Rohmanu dan I. Setiyadi, "Arduino Door Security System Menggunakan Rfid Rc522 Terintegrasi Arduino Data Logger Berbasis Mikrokontroller Atmega328 Pada PT. Indocipta Hasta Perkasa Cikarang," *Jurnal Informatika SIMANTIK,* vol. 2, no. 1, pp. 10-17, 2017.

[8] K. Wirawibawa, R. Susana dan H. H. Rachmat, "Evaluasi Keandalan Identifikasi RFID MFRC522 dengan Barrier Berbahan Dasar Plastik Berbasis Sistem Mikrokontroler," *JEECOM,* vol. 4, no. 1, pp. 1-6, 2022.

[9] K. S. Ravi, G. H. Harun, T. Vamsi dan P. Pratiyusha, "RFID Based Security System," *International Journal of Innovative Technology and Exploring Engineering (IJITEE),* vol. 2, no. 5, pp. 132-134, 2013.

[10] Logitech, "Logitech C270HD Webcam," Logitech, [Online]. Available: www.logitech.com/id-id/product/hd-webcam-c270. [Diakses 25 April 2022].

[11] M. Saluch, D. Tokarski, T. Grudniewski, M. Chodyka, J. A. Nitychoruk, P. Wolinski, B. Jaworska dan G. Adamczewski, "Raspberry PI 3B + Microcomputer as a Central Control Unit in Intelligent Building Automation Management System," *MATEC Web of Conference,* vol. 1, no. 1, p. 196, 2018.

[12] V. S. G. Reddy, N. Rathour, G. S. Ganesh, Yaswanth dan S. Kumar, "Real Time Face Detection Using Raspberry Pi 3B+," *Futuristic Sustainable Energy and Technology,* vol. 1, no. 1, pp. 187-198, 2017.

[13] V. Simadiputra dan N. Surantha, "Rasefiberry: Secure and Efficient Raspberry-Pi Based Gateway for Smarthome IoT Architecture," *Bulletin of Electrical Engineering and Informatics,* vol. 10, no. 2, pp. 1035-1045, 2021.

[14] C. W. Zhao, J. Jegatheesan dan S. C. Loon, "Exploring IOT Application Using Raspberry Pi," *International Journal of COmputer Networks and and Applications,* vol. 2, no. 1, pp. 27-34, 2015.

[15] Singgeta, R. Laksamana, Y.-H. Chang dan H.-W. Lin, "Raspberry Pi based pH Control for Nutrient Film Hydroponic System," *OSF Preprints,* vol. 1, no. 1, pp. 1-6, 2018.

[16] M. Murshed dan S. Chowdhury, "An IoT Based Car Accident Prevention and Detection System with Smart Brake Control," *Procs. of International Conference on Applications and Techniques in Information Science* , vol. 6, no. 1, pp. 1-4, 2019.