

Rancang Bangun Sistem Keamanan Akses Terbatas dengan Teknologi RFID pada PJB Muara Tawar

¹*Karno Diantoro, ²Faraz Rohmatullahama,
Sekolah Tinggi Manajemen Informatika dan Komputer (STMIK) Mercusuar,
Bekasi, Indonesia

¹karnodiantoro@gmail.com, ²rohfaraz@gmail.com

*Penulis Korespondensi

Diajukan : 17/11/2022

Diterima : 09/01/2023

Dipublikasi : 09/01/2023

ABSTRAK

Menjaga keamanan objek vital nasional tidak cukup hanya dengan adanya SATPAM dan perangkat CCTV. Sehingga keamanan itu tidak hanya sebatas pintu masuk yang dijaga oleh satpam, tapi keamanan yang lebih terstruktur dan canggih agar lebih menjamin keamanan. Untuk menjaga objek vital nasional, dan menghindari setiap orang bisa masuk ke area terbatas tanpa adanya akses tertentu dan juga untuk melacak pengunjung yang datang.

Untuk mengatasi permasalahan tersebut diperlukan sebuah sistem keamanan akses terbatas menggunakan sistem realtime monitoring *web base* untuk melacak pengunjung. Dalam proses pembuatan sistem ini, penulis menggunakan metode RFID (*Radio Frequency Identification*) berbasis *Internet Of Thing* (IoT) sebagai alat Sistem Keamanan, *visual studio code*, Arduino IDE, HTML dan Bootstrap merupakan sebagai aplikasi pendukung yang digunakan dalam pembuatan sistem aplikasi. *Database* menggunakan My SQL, dan untuk komponen elektronika menggunakan *keypad*, *solenoid*, *Node MCU* dan *RFID Reader* yang dimanfaatkan sebagai alat identifikasi personal untuk melakukan akses ke dalam suatu ruangan.

Sistem keamanan akses terbatas yang telah dirancang dapat menghasilkan protokol keamanan dan keselamatan yang baik untuk membuat karyawan dan fasilitas yang lebih aman, sehingga keamanan dan objek vital nasional PJB Muara Tawar lebih maksimal, Profesional dan juga dapat termonitoring secara aktual melalui *web base*.

Kata Kunci: Sistem Akses Terbatas, RFID, IoT, PJB Muara Tawar

I. PENDAHULUAN

PT Pembangkitan Jawa-Bali atau biasa disingkat menjadi PJB, adalah anak usaha PLN yang bergerak di bidang pembangkitan listrik. Hingga tahun 2020, perusahaan ini memiliki delapan pembangkit listrik dengan total kapasitas terpasang sebesar 7.054 MW. Melalui anak usahanya, PJB juga menyediakan jasa EPC, investasi pembangkit listrik, operasi dan pemeliharaan pembangkit listrik, serta penyediaan suku cadang pembangkit listrik. Untuk mendukung kegiatan bisnisnya, perusahaan ini pun perlu adanya akses untuk masuk ke zona terbatas yang bisa memonitoring pengunjung secara *real time*, saat ini PT PJB sudah menggunakan akses kontrol yang masih menggunakan metode "*stand alone*" atau belum terkoneksi ke jaringan LAN sehingga hal tersebut menyulitkan pihak IT dalam mendaftarkan kartu dan membackup data kartu karena alat *existing* saat ini belum tersentralisasi. Menjaga keamanan objek vital nasional tidak cukup hanya dengan adanya SATPAM dan perangkat CCTV. Sistem keamanan itu tidak hanya sebatas pintu masuk yang dijaga oleh satpam, tapi sistem keamanan yang lebih terstruktur dan canggih agar lebih menjamin keamanan.

Untuk mengatasi permasalahan di atas, maka diperlukan sebuah manajemen pengunjung

menggunakan sistem *realtime monitoring web base* untuk melacak pengunjung. RFID dimanfaatkan sebagai alat identifikasi personal untuk melakukan akses ke dalam suatu ruangan. Dalam proses pembuatan sistem ini, penulis menggunakan *HTML Bootstrap*, *Arduino IDE*, dan *visual studio code* sebagai aplikasi pendukung yang digunakan dalam pembuatan aplikasi ini serta *Database* yang digunakan *MySQL* sebagai basis data, dan untuk komponen elektronika menggunakan *keypad*, *solenoid*, *Node MCU* dan *RFID Reader* yang dimanfaatkan sebagai alat identifikasi personal untuk melakukan akses ke dalam suatu ruangan atau dengan kata lain sebagai kunci elektronik. Sistem keamanan akses terbatas yang telah dirancang dapat menghasilkan protokol keamanan dan keselamatan yang baik untuk membuat karyawan dan fasilitas yang lebih aman, sehingga keamanan dan objek vital nasional PJB Muara Tawar lebih maksimal, profesional dan juga dapat termonitoring secara aktual melalui *web base*.

Label RFID berfungsi untuk menyimpan dan mengambil data jarak jauh. Label RFID pada prakteknya dapat disematkan dalam suatu produk, hewan bahkan manusia (Anggara & Fitriani, 2021). Proses identifikasi pada RFID dapat terjadi dengan menggunakan gelombang elektromagnetik, oleh sebab itu proses identifikasi RFID membutuhkan dua perangkat yaitu *tag* dan *Reader* agar dapat berfungsi dengan baik. Identifikasi data pada RFID *tag* dilakukan melalui frekuensi radio yang merambat melalui media udara pada jangkauan tertentu sesuai dengan fitur yang dimiliki oleh setiap modul RFID (terdiri dari *RFID Reader* dan *RFID tag*) yang digunakan (Rachmat & Hutabarat, 2014). Pada umumnya, data RFID *tag* yang bersifat unik tersimpan atau tertanam dalam sebuah kartu *Chip* sehingga pengaruh kondisi alam seperti debu, kotoran ataupun temperatur udara tidak akan mengurangi kualitas komunikasi data yang terjadi (Ekayana, 2018).

RFID terdiri dari dua komponen utama utama, yaitu *tag* yang digunakan untuk menyimpan data yang dikenal dengan *UID* dan *Reader* untuk membaca *UID* yang ada didalam *tag* dengan cara memanfaatkan gelombang radio pada frekuensi tertentu. RFID memiliki dua jenis yaitu RFID Pasif dan RFID Aktif (Rahardja et al., 2015). Shandy, Y. D (2015) menyatakan sistem kunci otomatis ini adalah salah satu bentuk keamanan smart home yang bisa dipasang dirumah karena campur tangan manusia untuk mengaksesnya sudah diminimalisir. Selanjutnya penelitian Septryanti & Fitriyanti (2017) menyatakan bahwa komunikasi antara *smartphone android* dengan mikrokontroler dapat dilakukan secara *wireless* atau *bluetooth*, yang mana *smartphone android* dan *bluetooth module* pada sistem mikrokontroler dapat berkomunikasi menggunakan data serial.

II. STUDI LITERATUR

A. Definisi RFID

RFID adalah singkatan dari (*Radio Frequency Identification*). RFID adalah suatu teknologi yang digunakan untuk melakukan identifikasi dan pengambilan data dengan menggunakan *barcode* atau *magnetic card* (Alghifary et al., 2021; Kusumah et al., 2017).

B. Definisi Access Control Security

Access control didefinisikan atau diimplementasikan sebagai pemberi ijin terhadap sebuah objek tertentu secara spesifik. Akses kontrol sendiri membatasi orang-orang yang akan mengakses objek tersebut. Tanpa adanya akses kontrol, kemungkinan sesuatu (termasuk data) dapat di curi lebih meningkat (Nusantara, 2019).

Ada dua macam tipe komponen *access control*, yaitu :

1. Authentication

Autentikasi yang dimaksud adalah berupa keaslian suatu dokumen tertentu, dan mengaju kepada verifikasi suatu subjek yang di klaim, benar atau tidaknya subjek tersebut.

2. Authorization

Autorisasi ini berarti izin yang diberikan sebuah sistem. Hak seseorang dalam memasuki sistem ini sangat dibatasi. Biasanya otorisasi muncul setelah autentikasi.

Tiga metode akses yang ada :

1. *Network Access* yaitu akses yang didapatkan dalam sebuah jaringan *website*.
2. *System Access* yaitu akses yang diberikan pada sebuah sistem.

3. *Data Access* yaitu akses yang diberikan saat ingin mengakses data.

Empat macam strategy access control :

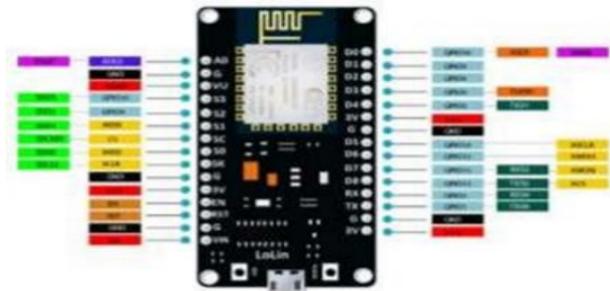
1. *Discretionary Access Control (DAC)*
 Pemilik utama akses dapat menentukan siapa yang dapat mengakses miliknya dan dapat menentukan ijin akses.
2. *Mandatory Access Control (MAC)*
 Sebuah grup/ organisasi yang memberikan ijin akses berdasarkan spesifik level yang ada untuk klasifikasi informasi/data.
3. *Role Based Access Control (RBAC)*
 Ijin akses yang diberikan tergantung dari role/ peran dia dalam suatu perusahaan atau organisasi tertentu, contoh : Data gaji karyawan hanya dapat di akses oleh *owner, manager*, dan bagian *finance*.
4. *Attribute Based Access Control*
 Akses yang diberikan menggunakan sebuah atribut atau subjek atau identitas atau peran atau nama atau file atau record tertentu.

C. Komponen-Komponen Elektronika

Berikut komponen-komponen elektronika yang digunakan dalam membuat sistem keamanan.

1. Node MCU

Node MCU adalah pengendali mikro *Single-board* yang bersifat *opensource*, diturunkan dari *Wiring platform*, dirancang untuk memudahkan penggunaan elektronik dalam berbagai bidang hardware. *Node MCU* terdiri dari perangkat keras berupa *System OnChip ESP8266* dari *ESP8266* buatan *Espressif System*, juga *firmware* yang digunakan, yang menggunakan bahasa pemrograman *scripting Lua*. *Node MCU* menyederhanakan proses bekerja dengan mikrokontroler



Gambar 1. Node MCU

Spesifikasi *Node MCU*

Tabel 1. Spesifikasi NodeMCU

SPESIFIKASI	NODE MCU V3
Mikrokontroler	ESP8266
Ukuran Board	57 mmx 30 mm
Tegangan Input	3.3 ~ 5V
GPIO	13 PIN
Kanal PWM	10 Kanal
10 bit ADCPin	1 Pin
Flash Memory	4 MB
Clock Speed	40/26/24 Mhz
WiFi	IEEE 802.11 b/g/n
Frekuensi	2.4 GHz – 22.5 Ghz

<i>USB Port</i>	<i>Micro USB</i>
-----------------	------------------

Sumber: Datasheet *NodeMCU ESP8266*, 2020

2. Catu Daya

Catu daya atau yang dalam bahasa Inggrisnya adalah *power supply* adalah suatu peralatan listrik yang berperan menyediakan energi listrik dan mengolahnya pada perangkat elektronika. Secara sederhana, peran sebuah catu daya yaitu mengolah sumber listrik dari stop kont



Gambar 2. Jenis Adaptor

3. Module RFID RC522

Modul ini berfungsi sebagai *Reader* maupun *writer* RFID. Sangat praktis diaplikasikan pada perangkat elektronik Anda. Dengan frekuensi 13.56MHz, modul mampu membaca maupun menulis *Chip* RFID dari jarak dekat.



Gambar 3. Module RFID RC522

4. Adapter Board Inter Integrated Circuit (I2C)

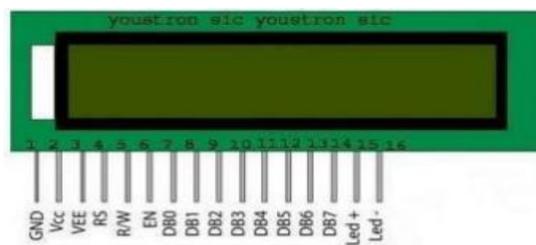
Inter Integrated Circuit atau sering disebut I2C adalah standar komunikasi serial dua arah menggunakan dua saluran yang didisain khusus untuk mengirim maupun menerima data. Sistem I2C terdiri dari saluran SCL (*Serial Clock*) dan SDA (*Serial Data*) yang membawa informasi data antara I2C dengan pengontrolnya.



Gambar 4. Adapter Board I2C

5. LCD (Liquid Crystal Display)

LCD (*liquid crystal display*) adalah suatu jenis media tampilan yang menggunakan kristal cair sebagai penampil utama. LCD sudah digunakan di berbagai bidang misalnya dalam alat-alat elektronik seperti televisi, kalkulator ataupun layar komputer. Pada aplikasi LCD yang di gunakan ialah LCD dot matrik dengan jumlah karakter 16 x 2.



Gambar 5. Konfigurasi Pin LCD

6. Selenoid

Bagian ini berfungsi sebagai aktuator. Prinsip dari solenoid sendiri akan bekerja sebagai pengunci dan akan aktif ketika diberikan tegangan sebesar 12V. Didalam solenoid terdapat kawat yang melingkar pada inti besi. Ketika arus listrik mengalir melalui kawat ini, maka terjadi medan magnet untuk menghasilkan energi yang akan menarik inti besi ke dalam (Shandy, Y. D, 2015).



Gambar 6. Selenoid

7. Relay

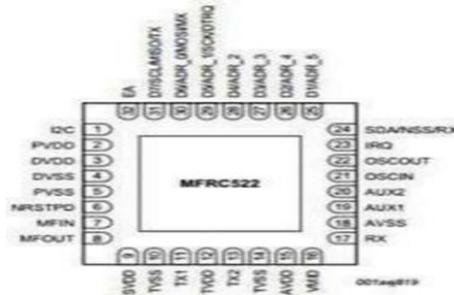
Relay adalah *output* yang dapat digunakan sebagai *switch* atau saklar untuk perangkat lain. Relay dikontrol dengan tegangan dari pin Arduino sehingga dapat melakukan *switch*. Terdapat 3 koneksi utama yaitu COM untuk input dari perangkat lain. NC (Normaly Close) pada keadaan biasa com akan terhubung ke pin NC.



Gambar 7. Relay

8. Keypad 4x4

Keypad Matriks adalah tombol-tombol yang disusun secara maktriks (baris x kolom) sehingga dapat mengurangi penggunaan pin *input*. Sebagai contoh, *Keypad* Matriks 4x4 cukup menggunakan 8 pin untuk 16 tombol. Hal tersebut dimungkinkan karena rangkaian tombol disusun secara horizontal membentuk baris dan secara vertikal membentuk kolom (www.immersa-lab.com, 2015).



Gambar 8. Keypad 4x4

III. METODE

Selama ini sistem otomatis yang dikenal adalah sistem *barcode*. Sistem *barcode* mempunyai keterbatasan dalam penyimpanan data serta tidak dapat dilakukan program ulang atas data yang tersimpan di dalamnya. Namun pada teknologi RFID, proses mengambil atau mengidentifikasi obyek atau data dilakukan secara *contactless* (tanpa kontak langsung) (Hamdani, 2014; Tarigan, 2004). RFID adalah teknologi penangkapan data yang dapat digunakan secara elektronik untuk mengidentifikasi, melacak dan menyimpan informasi yang tersimpan dalam *tag* RFID (Hidayat, 2016). Proses identifikasi pada RFID dapat terjadi dengan menggunakan gelombang elektromagnetik.

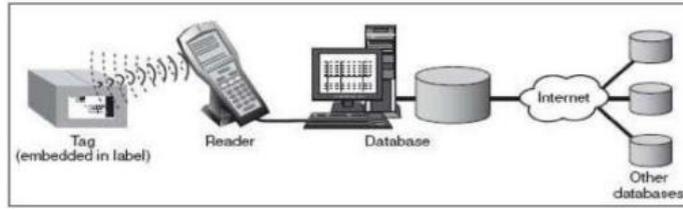
Proses identifikasi RFID membutuhkan dua perangkat yaitu *tag* dan *Reader* agar dapat berfungsi dengan baik. Identifikasi data pada RFID *tag* dilakukan melalui frekuensi radio yang merambat melalui media udara pada jangkauan tertentu sesuai dengan fitur yang dimiliki oleh setiap modul RFID (terdiri dari RFID *Reader* dan RFID *tag*) yang digunakan. Pada umumnya, data RFID *tag* yang bersifat unik tersimpan atau tertanam dalam sebuah kartu *Chip* sehingga pengaruh kondisi alam seperti debu, kotoran ataupun temperatur udara tidak akan mengurangi kualitas komunikasi data yang terjadi. modul RFID *Reader* yang digunakan adalah modul RFID RC522 yang berbasis IC MFRC522. IC MFRC522 yang berada pada modul RFID *Reader* sebetulnya dapat menggunakan 3 interface komunikasi yaitu *Serial Peripheral Interface* (SPI), I2C dan UART. Namun pada modul RFID *Reader* yang digunakan, komponen yang terpasang hanya mendukung antarmuka komunikasi SPI saja. Modul MFRC522 menggunakan komunikasi SPI karena transfer data dapat terjadi dengan cepat. Modul MFRC522 ini nantinya akan bekerja pada *Node* MCU yang bertindak sebagai *slave*. Informasi identitas yang dimiliki RFID *tag* kemudian akan dikirim menggunakan interface komunikasi serial UART oleh *slave* ke *master* yaitu *Node* MCU. Berikut penjelasan *Chip* MFRC522 pada Gambar 9 berikut :



Gambar 9. Konfigurasi Chip MFRC522

RFID dapat melakukan kontrol otomatis untuk banyak hal. Sistem-sistem RFID menawarkan peningkatan efisiensi dalam pengendalian inventaris, logistik dan manajemen

rantai supply (Hidayat, 2016).

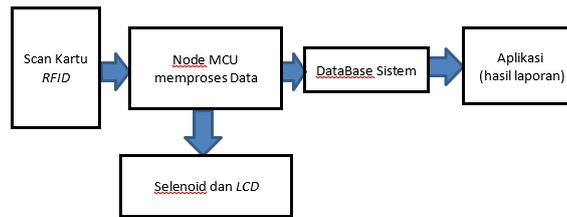


Gambar 10. Komponen Utama Sistem RFID

IV. HASIL DAN PEMBAHASAN

A. Analisa Sistem Rancangan Alat

Rancangan alat disusun dan dianalisa dengan *software* atau program sebagai pengatur dari *port-port* serta I/O yang digunakan serta algoritma sebagai proses pengaktifan rangkaian alat sistem keamanan akses terbatas dengan menggunakan RFID *Reader*, dan LCD diperlukan sebuah program yang ditanamkan ke dalam IC CHG340 atau *Node MCU* dengan menggunakan bahasa pemrograman C. Sistem kerja dari Alat Sistem Keamanan Akses Terbatas menggunakan RFID *Reader*, dan LCD. Berikut penjelasan mengenai blok cara kerja dari rangkaian Sistem Keamanan Akses Terbatas Dengan Menggunakan RFID Berbasis *Internet Of Thing* (IoT)



Gambar 11. Blok Sistem Akses Terbatas

Cara kerja pada alat RFID *Reader* yang digunakan sebagai pembaca antara RFID *Tag* dan mikrokontroller *Node MCU* digunakan untuk mengatur atau mengontrol kerja dari alat ini. Dan untuk output atau keluaran dari alat ini adalah LCD yang berguna sebagai 37 indikator bacaan saat proses tapping kartu RFID dan solenoid berguna sebagai indikator saat proses masuk. Jika sudah berhasil melakukan *tapping*, maka data kartu RFID akan tersimpan dalam *database* sistem dan ini hanya bisa diakses oleh admin.

RFID *Reader* atau transponder, terdiri atas sebuah *microChip* dan sebuah antena. *Chip* tersebut menyimpan nomor seri yang unik/ID dan informasi lainnya tergantung kepada tipe memorinya. Tipe memori itu sendiri dapat *readonly*, *read-write*, atau *write-onceread-many*. Antena yang terpasang pada *mikroChip* mengirimkan informasi ke RFID *Reader*.

RFID *Reader* mempunyai nomor yang dibagi menjadi 64 block (block 0- 63) yang dialokasikan pada memori menjadi 16 baris (no baris 0-15). Setiap *Tag* atau RFID *card* mempunyai salah satu nomor unik yang tercantum pada RFID *Reader*.



Gambar 12 Alat Akses Terbatas

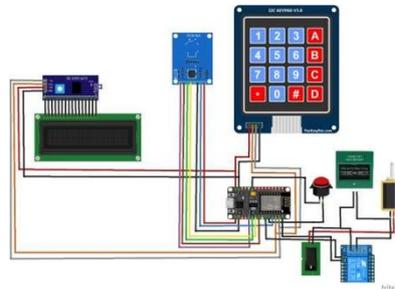
Rangkaian komponen yang digunakan pada alat Sistem Keamanan Akses Terbatas Dengan Menggunakan RFID Berbasis *Internet Of Thing* (IoT) secara detail. Pada bagian sumber tegangan

menggunakan tegangan 12v untuk mengaktifkan seluruh rangkaian yang terhubung pada mikrokontroller *Node MCU*. Blok input disini menggunakan 2 komponen inputan yaitu RFID.



Gambar 12 Alat Akses Terbatas

Reader dan *RFID Reader* berfungsi sebagai komponen untuk menscan kartu. Untuk output pada alat ini yaitu tampilan kalimat pada LCD yang digunakan sebagai indikator saat akses diterima, Selenoid berfungsi sebagai alat pengunci dan juga *database* yang digunakan untuk menyimpan data Log, dapat dilihat pada gambar 13.



Gambar 13. Desain RFID Reader

B. Analisa Pengujian Sistem

Pada penelitian ini pengujian yang digunakan untuk sistem ini adalah *Black Box Testing* adalah *software testing* untuk mengamati hasil input dan output dari perangkat lunak. Pengujian yang dilakukan hanya dengan mengamati hasil eksekusi melalui data uji dan memeriksa otimisasi pengujian dari Sistem Rancang Bangun Sistem Keamanan Akses Terbatas Dengan Teknologi RFID Pada PJB Muara Tawar. Perancangan pengujian sistem selengkapannya dapat dilihat pada tabel-tabel berikut ini.

1. Pengujian *Form Login*

Pada halaman *login* terdapat 2 kolom yang perlu diisi yaitu kolom *user* dan kolom *password*. *Login* pada web ini hanya dapat dilakukan oleh IT yang disebut operator. Pada tahap ini sistem dapat mengerjakan proses tersebut. Berikut adalah pengujian *Form Login* pada *website* yang tersaji pada tabel 2 dibawah ini.

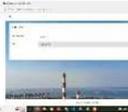
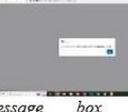
Tabel 2. Hasil Pengujian Black box pada *Form Login*

Kriteria dan Hasil Uji (Data Normal)			
Skema Pengujian	Uji Coba	Hasil Yang Di Harapkan	Hasil Uji
Memasukan <i>username</i> dan <i>password</i> yang benar		 Masuk ke halaman <i>dashboard</i>	Valid
Kriteria dan Hasil Uji (Data Tidak Normal)			
Memasukan <i>username</i> dan <i>password</i> yang salah		 Pemberitahuan <i>Email</i> dan <i>password</i>	Invalid

2. Pengujian Form Add User

Pada halaman ini, terdapat tombol “Register” yang digunakan operator untuk membuka pendaftaran Kartu RFID. Pada tahap ini sistem dapat mengerjakan proses tersebut. Berikut adalah tampilan form add user sebelum dibuka oleh operator. Berikut adalah pengujian form Add User pada website yang tersaji pada tabel dibawah ini.

Tabel 3 Black box pada form Add User

Kriteria dan Hasil Uji (Data Normal)			
Skema Pengujian	Uji Coba	Hasil Yang Di Harapkan	Hasil Uji
Menambahkan <i>user</i> baru pada <i>kontroller</i>		 Masuk ke halaman <i>Usr Accepted</i>	Valid
Kriteria dan Hasil Uji (Data Tidak Normal)			
Menambahkan <i>user</i> baru pada <i>kontroller</i>		 <i>Message box</i> tampil Pemberitahuan <i>invalid Uid</i>	Invalid

3. Pengujian Form Add Controller

Pada halaman ini digunakan operator untuk melakukan pendaftaran *Controller Node MCU* dan juga dapat mengelola data kontroler. Berikut adalah pengujian form Add User pada website yang tersaji pada tabel dibawah ini.

Tabel 4. Black box pada form Add Controller

Kriteria dan Hasil Uji (Data Normal)			
Skenario Pengujian	Uji Coba	Hasil Yang Di Harapkan	Hasil Uji
Menambahkan <i>user</i> baru pada <i>controller</i>		 Masuk ke halaman <i>list user</i>	Valid
Kriteria dan Hasil Uji (Data Tidak Normal)			
Menambahkan <i>user</i> baru pada <i>controller</i>		 <i>Message box</i> tampil pemberitahuan “data tidak boleh kosong”	Invalid

C. Hasil Analisa

Dari hasil pengujian rancangan alat dan sistem maka perancangan ini menggunakan metode RFID Berbasis IoT, berupa pengambilan foto dan fisik dari alatnya yaitu pada jarak 0,5 cm sampai 3 cm, kartu tag dapat teridentifikasi dengan baik oleh RFID Reader, sedangkan pada jarak 3,5 cm, kartu tag mulai tidak dapat teridentifikasi oleh RFID Reader. Hal ini disebabkan karena jarak pancar gelombang elektromagnetik RFID Reader yang mampu diterima kartu tag sangat terbatas. Dan juga untuk waktu responsivitas terhadap RFID Reader adalah kurang dari 0,2 detik. Untuk lebih jelaskan akan di ditampilkan dalam bentuk Tabel 5 adalah :

Tabel 5. Hasil Pengujian Jarak Pembacaan Tag RFID

Jarak	Pengujian ke-					Keterangan
	1	2	3	4	5	
0.5 cm	1	1	1	1	1	<u>Tag</u> Terbaca
1 cm	1	1	1	1	1	<u>Tag</u> Terbaca
1.5 cm	1	1	1	1	1	<u>Tag</u> Terbaca
2 cm	1	1	1	1	1	<u>Tag</u> Terbaca
2.5 cm	1	1	1	1	1	<u>Tag</u> Terbaca
3 cm	1	1	1	1	1	<u>Tag</u> Terbaca
3.5 cm	0	0	0	0	0	<u>Tag</u> Tidak Terbaca
4 cm	0	0	0	0	0	<u>Tag</u> Tidak Terbaca
4.5 cm	0	0	0	0	0	<u>Tag</u> Tidak Terbaca
5 cm	0	0	0	0	0	<u>Tag</u> Tidak Terbaca

V. KESIMPULAN

Pada tahap perancangan sistem keamanan akses terbatas dan tahap implementasi serta pengujian alat maka dapat diambil kesimpulan sebagai berikut:

1. Alat ini bekerja untuk memberikan akses terkendali pada objek vital nasional sehingga orang yang tidak berkepentingan tidak sembarang masuk, dan juga memungkinkan akses hanya untuk personil yang berwenang.
2. Dalam alat ini juga sudah dilengkapi dengan *database* dan secara automatic akan membackup *database* serta dapat memonitoring pengunjung secara aktual melalui web base, sehingga memudahkan dalam membuat data laporan.
3. Pada rancangan aplikasi ini masih terdapat kekurangan dan keterbatasan yang di miliki yang dapat diperbaiki dengan mengembangkan alat tersebut di masa yang akan mendatang.
4. Pengembangan alat tersebut dapat di rancang dan di bentuk supaya lebih interaktif serta disesuaikan dengan kondisi dan situasi dalam penempatan perangkatnya. Sehingga pembuatan alat ini lebih efektif. Untuk mengembangkan alat ini kedepannya di sarankan dapat menggunakan *metal sensor detector* agar terhindar dari visitor yang membawa senjata tajam yang berbahaya.

VI. REFERENSI

- Alghifary, I., Nurfadhila, A., Handini, J., Nurhakim, T. F., Rohmaniar, R. A., & Wirasta, W. (2021). STUDI LITERATUR IMPLEMENTASI IOT PADA ANDAKARA CARD DENGAN MEMANFAATKAN TEKNOLOGI RFID DAN NFC. *Prosiding SNAPP*, 283–292.
- Anggara, R., & Fitriani, E. (2021). PROTOTYPE PENGAMAN KOMPLEK PERUMAHAN MENGGUNAKAN RFID DAN SENSOR ULTRASONIK BERBASIS SMARTPHONE ANDROID. *Bina Darma Conference on Engineering Science (BDCES)*, 3(2), 307–318.
- Ekayana, A. A. G. (2018). Implementasi Sistem Penguncian Pintu Menggunakan RFID Mifare Frekuensi 13.56 Mhz dengan Multi Access. *Jurnal Pendidikan Teknologi Dan Kejuruan*, 15(2).
- Hamdani, F. (2014). Penerapan RFID (Radio Frequency Identification) di perpustakaan: kelebihan dan kekurangannya. *Khazanah Al-Hikmah: Jurnal Ilmu Perpustakaan, Informasi, Dan Kearsipan*, 2(1), 71–79.
- Hidayat, R. (2016). Teknologi wireless RFID untuk perpustakaan polnes: suatu peluang. *Informatika Mulawarman: Jurnal Ilmiah Ilmu Komputer*, 5(1), 42–49.

- Kusumah, I. M. Y., Apriyadi, D., & Ramadhan, A. R. (2017). PENERAPAN ALAT PEMBACA KARTU IDENTITAS MENGGUNAKAN RADIO FREKUENSI IDENTIFICATION (RFID) PADA APLIKASI ABSENSI MAHASISWA: DI LINGKUNGAN STMIK BANDUNG. *Jurnal Teknologi Informasi Dan Komunikasi*, 6(1), 11–14.
- Nusantara, B. (2019). *Access Control Security*. <https://sis.binus.ac.id/2019/02/18/access-control-security/>
- PintarElektro. (2020). *CATU DAYA: Pengertian, Fungsi, Cara Kerja hingga Jenisnya*. PintarElektro.Com. <https://pintarelektro.com/catu-daya/>
- Rachmat, H. H., & Hutabarat, G. A. (2014). Pemanfaatan Sistem RFID sebagai Pembatas Akses Ruangan. *ELKOMIKA: Jurnal Teknik Energi Elektrik, Teknik Telekomunikasi, & Teknik Elektronika*, 2(1), 27.
- Rahardja, U., Frecilia, Y., & Komaeni, N. (2015). Analisa Peminjaman Buku Perpustakaan Dengan Menggunakan Sistem Rfid Pada Perguruan Tinggi Raharja. *Creative Communication and Innovative Technology Journal*, 9(1), 1–12.
- Septryanti, A., & Fitriyanti, F. (2017). Rancang Bangun Aplikasi Kunci Pintu Otomatis Berbasis Mikrokontroler Arduino Menggunakan Smartphone Android. *CESS (Journal of Computer Engineering, System and Science)*, 2(2), 59–63.
- Tarigan, Z. J. H. (2004). Integrasi Teknologi RFID dengan Teknologi Erp Untuk Otomatisasi Data (Studi Kasus Pada Gudang Barang Jadi Perusahaan Furniture). *Jurnal Teknik Industri*, 6(2), 134–141.
- YDSVD, A. R., & Suwastika, A. (2015). Implementasi Sistem Kunci Pintu Otomatis Untuk Smart Home Menggunakan SMS Gateway. *E-Proceeding of Engineering*, 2, 6395–6407.