Rancang Bangun Sistem Keamanan Pintu Menggunakan Metode *Two-Factor Authentication*

Ahmad Ilham Ali Mashudi[1], Agus Prihanto[2]

[1,2] Teknik Informatika, Fakultas Teknik, Universitas Negeri Surabaya
[1]ahmad.18075@mhs.unesa.ac.id
[2]agusprihanto@unesa.ac.id

***Abstrak*— Pentingnya keamanan informasi dan fisik telah meningkat tidak hanya dalam dunia digital tetapi juga dalam kehidupan sehari-hari. Pintu, sebagai komponen penting dari arsitektur bangunan, berfungsi sebagai titik masuk dan keluar utama. Sistem keamanan pintu tradisional yang sering bergantung pada kunci dan rantai telah terbukti tidak memadai dan tidak efisien dalam menangani tantangan keamanan kontemporer. Dengan kondisi tersebut peneliti menemukan rumusan masalah yaitu bagaimana cara membangun sistem keamanan pintu dengan teknologi 2FA dan bagaimana cara mengetahui log history pengunjung yang keluar masuk pada pintu tersebut. Penelitian ini juga bertujuan untuk mengeksplorasi penerapan Otentikasi Dua Faktor (2FA) sebagai metode canggih untuk meningkatkan sistem keamanan pintu, menggabungkan teknologi RFID dan One-Time Password (OTP) untuk mengatasi kerentanan yang terkait dengan metode otentikasi satu faktor. Pendekatan berlapis ganda ini berfungsi untuk memperkuat kontrol akses dan mengurangi risiko masuk yang tidak sah. Integrasi 2FA dalam sistem keamanan pintu secara signifikan meningkatkan keamanan dengan mengatasi keterbatasan metode otentikasi satu faktor. Dari pengujiaan penggunaan RFID dan OTP menunjukkan bahawa metode tersebut sangat efektif untuk mengamankan area dengan tingkat keamanan tinggi seperti pusat data. Temuan penelitian ini menunjukkan bahwa 2FA dapat berhasil diterapkan dalam skenario dunia nyata, menyediakan langkah proaktif untuk melindungi aset berharga dari potensi ancaman keamanan. Selain itu hasil dari pengujian log history keluar masuk juga bisa berjalan dengan baik dan menunjukkan data yang sangat rinci. Mengingat keberhasilan penerapan dan hasil pengujian 2FA dan log history, disarankan untuk menerapkan sistem keamanan canggih ini di area yang sangat sensitif yang memerlukan kontrol akses ketat.**

Kata Kunci*— *Otentikasi Dua Faktor (2FA), RFID, One-Time Password (OTP), Sistem Keamanan Pintu.

I. PENDAHULUAN

Keamanan informasi dan akses, tidak hanya dalam dunia maya tetapi juga diperlukan dalam kehidupan sehari-hari dan menjadi prioritas utama, terutama terkait dengan keamanan fisik ruangan atau bangunan. Sebagai bagian penting dari arsitektur rumah, pintu berfungsi sebagai tempat masuk dan keluar pada sebuah bangunan. Pada umumnya sistem keamanan pintu hanya dirancang menggunakan gembok dan rantai yang dinilai kurang tepat dan tidak efisien [4]. Apalagi pada zaman yang sekarang banyak didapati kasus keamanan rumah yang semakin kompleks [8]. Penggunaan kunci yang konvensional juga mudah dibuka oleh pencuri, karena semakin berkembang cara pencuri untuk membuka pintu rumah [12]. Oleh karena itu, sistem keamanan pintu harus dirancang dengan baik untuk mencegah akses yang tidak sah atau kemungkinan pelanggaran keamanan.

Menghadapi ancaman keamanan yang semakin kompleks, metode otentifikasi satu faktor seperti penggunaan kunci fisik atau password saja dianggap tidak aman dan rentan terhadap serangan atau pencurian identitas. Selain rentan terhadap serangan dan pencurian identitas penggunan otentikasi satu faktor juga sangat rentan akan kebocoran sistem. Satu jenis otentifikasi cukup untuk memungkinkan pihak yang tidak memiliki wewenang untuk mendapatkan akses. Akibatnya terjadi hal hal yang tidak diinginkan yang dilakukan oleh pihak tertentu. Oleh karenanya sistem keamanan yang lebih kuat diperlukan untuk mengamankan akses ke area atau bangunan. Untuk melindungi sebuah bangunan atau ruangan, pengamanan sistem keamanan pintu sangat penting. Salah satu cara yang dapat dilakukan untuk meningkatkan keamanan akses adalah menggunakan metode Otentikasi dua faktor. Otentikasi dua faktor, juga dikenal sebagai Two-factor authentication (2FA), menjadi metode yang semakin populer dan digunakan secara luas. Metode ini menambahkan lapisan keamanan tambahan dengan meminta dua jenis identifikasi berbeda untuk memberikan akses seperti kombinasi kode on-time password yang dikirimkan melalui perangkat mobile, penggunaan kombinasi on-time password dan RFID juga termasuk ke dalam metode sebagai Two-factor authentication (2FA).

Dua-Faktor Verifikasi menawarkan keamanan tambahan, tetapi implementasinya tidak selalu lancar. Tidak mudah untuk berintegrasi dengan sistem yang sudah ada, melakukan manajemen identitas yang efektif, dan mendorong pengguna untuk menggunakan metode keamanan yang lebih kompleks. Untuk memastikan sistem keamanan pintu dapat berjalan dan berfungsi dengan baik, maka perlu dipastikan bahwa masalah keamanan seperti kebocoran data atau kehilangan faktor otentikasi dapat ditangan dan diatasi secara baik dan benar. Dengan menerapkan metode Two-factor authentication (2FA) keamanan pada suatu sistem keamanan pintu diharapkan dapat meningkatkan sistem kemanan pintu secara signifikan.

Studi ini akan membahas penelitian terbaru tentang keamanan informasi, keamanan fisik, dan implementasi otentikasi dua faktor yang akan diimplementasikan dengan penggunaan RFID dan On-Time Password yang dikombinasikan dengan aplikasi mobile untuk memudahkan penerapannya. Referensi relevan mencakup buku teks, jurnal ilmiah, dan dokumentasi teknis tentang penerapan metode 2FA untuk sistem keamanan pintu. Pemasangan otentikasi dua faktor pada sistem keamanan pintu dianggap sebagai tindakan

proaktif untuk meningkatkan tingkat keamanan dan melindungi aset berharga dari bahaya keamanan yang mungkin terjadi. Oleh karena itu, penelitian ini mempengaruhi pemahaman kita tentang keamanan informasi dalam konteks keamanan fisik pintu, yang berkaitan dengan berbagai sektor industri. Dikarenakan penelitian ini menggunakan sistem keamanan tingkat tinggi. Maka peneliti menyarankan untuk implementasi penggunaan pada ruang yang sangat rahasia seperti data center, dll. Berdasarkan latar belakang tersebut, peneliti berkeinginan untuk melakukan penelitian tentang bagaimana cara membangun sistem keamanan pintu dengan teknologi *Two-Factor Authentication* yang dilengkapi dengan *log history* keluar mask pengungjungnya.

II. METODOLOGI PENELITIAN

A. Jenis Penelitian

Penelitian ini merupakan jenis penelitian pengembangan (*development research*). Menurut definisi, penelitian pengembangan adalah studi sistematis tentang perancangan, pengembangan, dan evaluasi program, proses, dan produk instruksional yang harus memenuhi kriteria konsistensi internal dan efektivitas (Richey, 1994). Dalam konteks penelitian ini, penelitian pengembangan melibatkan perancangan dan pembangunan sistem keamanan pintu menggunakan metode two-factor authen-tication. Tujuan utama dari penelitian ini adalah untuk menghasilkan sistem keamanan pintu yang lebih baik dan lebih aman. Dalam penelitian ini, proses perancangan dan pembangunan sistem menjadi bagian penting dari penelitian. Selain itu, penelitian ini juga melibatkan pengujian dan evaluasi sistem yang telah dibangun untuk memastikan bahwa sistem tersebut berfungsi dengan baik dan dapat meningkatkan keamanan pintu.

B. Variabel Penelitian

Variabel penelitian adalah segala sesuatu yang akan menjadi obyek penelitian. Sering pula variabel penelitian dinyatakan sebagai faktor-faktor yang berperan dalam peristiwa yang akan diteliti. Melakukan klasifikasi variabel sangat perlu untuk menentukan alat pengambilan data yang akan digunakan dan metode analisis mana yang sesuai untuk diterapkan pada sebuah penelitian. Penelitian ini memiliki dua variabel yaitu variabel bebas (*Independent* Variabel) dan variabel dependen. Variabel variabel tersebut adalah sebagai berikut:

1. Variabel Bebas (*Independent Variabel*)
   Variabel bebas dalam penelitian ini adalah variabel dari sistem keamanan pintu yang menggunakan RFID dan *One-Time Password*.
2. Variabel Dependen
   Variable dependen pada penelitian ini adalah metrik-metrik yang digunakan untuk analisis yang terdiri dari tingkat keamanan, kenyamanan, dan ontetikasi dari sistem keamanan pintu tersebut.

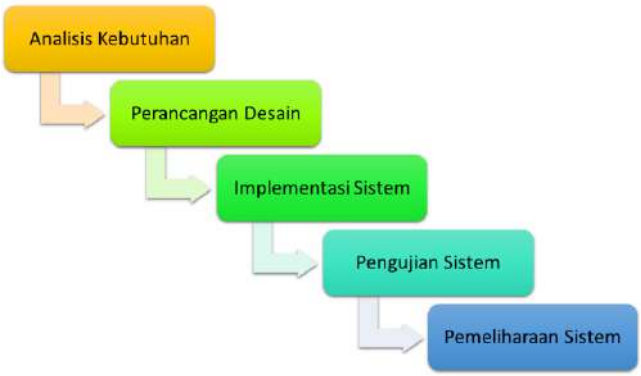
C. Sumber Data dan Data Penelitian

1. Sumber Data Primer
   Sumber data primer adalah sumber pertama dimana sebuah data dapat dihasilkan. Dalam penelitian ini yang menjadi sumber data primer adalah observasi yang dilakukan oleh peneliti untuk mengetahui sejauh mana teknologi *two-factor authentification* efektif dalam meningkatkan keamanan pada pintu.
2. Sumber Data Sekunder
   Sumber data sekunder adalah sumber data yang tidak langsung memberikan data kepada pengumpul data, misalnya melalui orang lain atau dokumen. Dalam penelitian ini yang menjadi sumber data sekunder adalah jurnal-jurnal dan *e-book* yang akan digunakan sebagai referensi serta untuk melengkapi hasil penelitian.

D. Pengembangan Sistem

Pada tahap pengembangan sistem keamanan pintu dengan *two-factor authentication* ini akan menggunakan sistem *waterfall*. *Waterfall* disini menggunakan pendekatan SDLC (*System Development Life Cycle*) pertama yang biasa digunakan untuk pengembangan sebuah sistem.

1. *Waterfall*
   Metode pengembangan waterfall merupakan salah satu pendekatan dalam pengembangan yang mengikuti rangkaian fase secara terencana dan linear. Metode ini dicetuskan oleh Royce pada tahun 1987 dipublikasinya yang berjudul "*Managing the development of large software systems: concepts and techniques*" (Royce, 1987) dan sudah diadaptasi oleh banyak peneliti di seluruh dunia. Fase-fase dalam metode waterfall harus dilaksanakan secara berurutan, di mana setiap fase harus diselesaikan sepenuhnya sebelum memasuki fase berikutnya. Analogi dengan air terjun digunakan karena proses pengembangan ini mengikuti pola langkah yang berurutan, seperti aliran air yang mengalir melalui tingkatan air terjun.



Gbr 1 Tahapan Metode Waterfall

2. Analisis Kebutuhan
   Pada tahapan ini ditujukan agar penelitian ini berjalan sesuai dengan perencanaan, maka dibutuhkan sebuah perangkat yang dapat mendukung penelitian. Adapun

kebutuhan perangkat dalam sistem yang akan dibangun sebagai berikut:

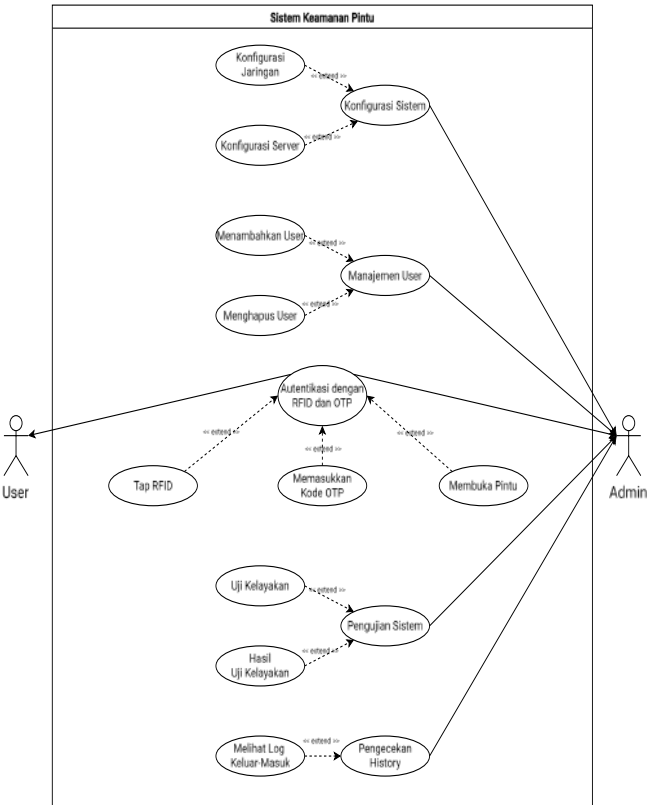
a. Perangkat Keras (*Hardware*)
   1) Mikrokontroller (NodeMCU ESP32)
   2) Keypad
   3) LCD
   4) Solenoid (Sebagai Pengunci Pintu
b. Perangkat Lunak (*Software*)
   1) Android SDK
   2) Android Studio
   3) Visual Studio Code IDE

3. Perencanaan Desain

Pada tahapan perencanaan ini, data yang telah dianalisis sebelumnya akan diterjemahkan dalam bentuk yang lebih mudah dimengerti oleh pengguna. Untuk mempermudah pemahaman sistem, beberapa sistematika perencanaan yang digunakan melibatkan penggunaan beberapa diagram, antara lain, *Activity Diagram* digunakan untuk menggambarkan alur kerja sistem secara visual. *Usecase Diagram* digunakan untuk mengidentifikasi fungsionalitas utama sistem dan keterlibatan pengguna dalam interaksi dengan sistem. Selanjutnya, *Sequence Diagram* digunakan untuk menggambarkan urutan langkah-langkah yang terjadi dalam proses tertentu.

a. *Usecase Diagram* Sistem Keamanan Pintu

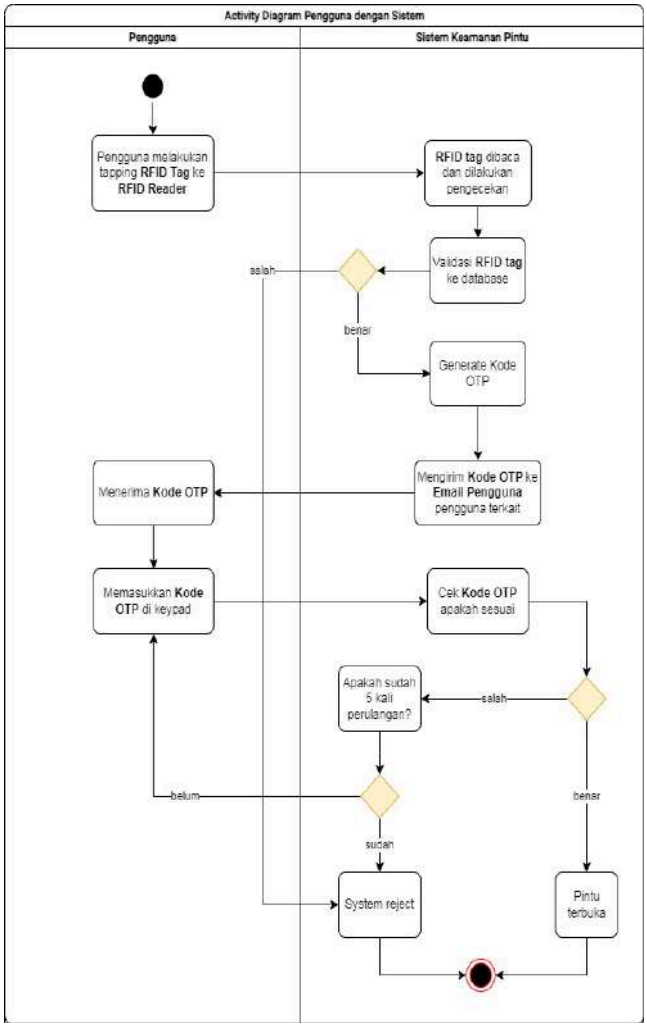
Desain diagram yang dihasilkan pada tahap ini akan menjadi panduan utama dalam proses pengimplementasian sistem. Berikut adalah gambar *usecase diagram* sisten keamanan pintu.



Gbr 2 Usecase Diagram

b. *Activity Diagram* Sistem Keamanan Pintu

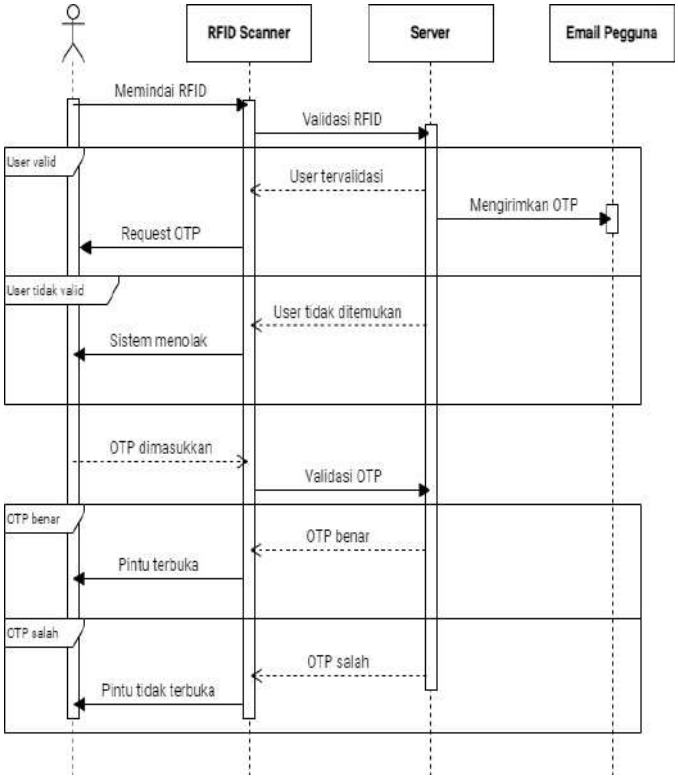
Activity diagram adalah jenis diagram UML yang digunakan untuk menunjukkan model alur kerja atau aktivitas dari suatu proses atau sistem memodelkan aktivitas dalam suatu sistem. Untuk sistem keamanan pintu dengan autentikasi dua faktor (2FA) menggunakan *One-Time Password* (OTP) yang dikirim ke email pengguna, kita dapat membuat activity diagram sebagai berikut.



Gbr 3 Activity Diagram

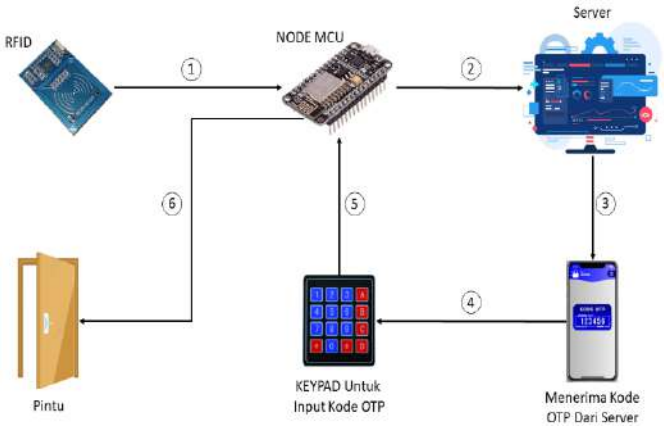
c. *Sequence Diagram* Sistem Keamanan Pintu

Sequence diagram juga salah satu jenis diagram dalam UML yang digunakan untuk menggambarkan urutan interaksi antara objek-objek dalam sebuah sistem. *Sequence diagram* menjelaskan bagaimana pesan atau panggilan metode dikirim antara objek-objek selama proses tertentu. Dalam kasus sistem keamanan pintu dengan 2FA ini, *sequence diagram* dapat digunakan untuk menggambarkan alur interaksi antara komponen-komponen utama.



Gbr 4 Sequence Diagram

d. Desain Arsitektur Sistem



Gbr 5 Rancangan Arsitektur Sistem

Arsitektur sistem merupakan gambaran umum dari sebuah sistem keamanan pintu. Dalam arsitektur sistem keamanan pintu ini memerlukan RFID dan email pengguna yang digunakan sebagai penerima OTP untuk mengintegrasikan *Two-factor authentication* nya seperti pada Gbr 5. Dengan penjelasanya sebagai berikut:

1) RFID berperan sebagai perangkat yang mendeteksi dan membaca data dari tag RFID. RFID berkerja menggunakan gelombang radio untuk mentransfer data dari tag RFID. RFID yang digunakan adalah bertipe RC522 yang merupakan sebuah modul RFID

yang popular digunakan pada proyek proyek elektronika dan keamanan.

2) Nodemcu berperan sebagai mikrokontroler yang digunakan untuk mengontrol pembaca RFID dan memproses kode OTP yang diinputkan melalui keypad. Nodemcu memiliki chip WI-FI yang terintegrasi dengan jaringan internet lokal sehingga mikrokontroler dapat terhubung ke internet guna merequest kode OTP ke server lokal yang sudah dibuat tanpa memerlukan komponen tambahan lagi.
3) Server berperan untuk mengkonfirmasi, menerima mengenerate dan mengirimkan kode OTP ke email pengguna yang sudah di daftar dalam database lokal. Server disini memiliki database yang berisi user id, generate OTP, dan username pengguna/user. Server disini berjalan dalam localhost saja guna menjaga keamanan dari kebocoran data melalui internet.
4) Email pengguna berperan untuk menerima kode OTP yang dikirimkan dari Server. Kode OTP tersebut harus diinputkan kedalam keypad agar bisa diproses lagi oleh Nodemcu.
5) Keypad berperan sebagai media untuk menginputkan OTP yang sudah diterima oleh user dari email pengguna. Setelah OTP diinputkan maka akan diproses kevalidannya oleh Nodemcu yang nantinya akan menghasilkan pintu yang bisa dibuka oleh user.
6) Pintu berperan sebagai penghalang fisik yang dapat mencegah orang atau benda masuk ke area yang tidak diinginkan. Pintu akan bisa dibuka jika sudah mendapatkan sinyal dari Nodemcu setelah diinputkan OTP yang dikirim ke Email pengguna user.

4. Implementasi Sistem

Pada tahap implementasi, rancangan sistem yang telah dibuat pada tahap perancangan akan diwujudkan menjadi perangkat lunak atau sistem yang berjalan sesuai dengan spesifikasi yang telah ditetapkan. Implementasi sistem mencakup mengintegrasikan perangkat keras, seperti pembaca RFID dan keypad, dengan perangkat lunak yang telah dibuat. Juga diperlukan pengujian keterhubungan untuk memastikan bahwa perangkat keras dapat berkomunikasi secara efektif dengan perangkat lunak.

5. Pengujian Sistem

Pada tahapan ini hasil dari rancangan yang sudah dibuat oleh peneliti akan diimplementasikan dan diuji sesuai alur kerja yang telah direncanakan. Dalam sistem ini, pertama user akan menempelkan kartu RFID pada RFID reader. Kemudian data dari RFID tersebut akan di cek apakah data tersebut terdaftar pada sistem keamanan atau tidak, jika data tidak terdaftar maka akses akan ditolak. Apabila data terdaftar maka berikutnya adalah memasukkan kode OTP yang dikirimkan dari database sistem ke aplikasi mobile yang telah dibuat sebagai pengaman kedua. Apabila kode OTP tidak terverifikasi oleh database sistem maka akses akan ditolak. Sedangkan apabila kode OTP yang dimasukkan terverfikasi oleh sistem maka akses akan diterima dan user bisa membuka pintu serta menerima notifikasi mengenai siapa yang telah melakukan akses terhadap pintu tersebut. Selain itu pengujian akan dilakukan dengan menggunakan berbagai metrik untuk mengukur efektivitas sistem keamanan pintu. Berikut adalah skema pengujian yang diterapkan.

a. Keberhasilan Otentikasi (*Accuracy*)

Pengukuran keberhasilan otentikasi dilakukan dengan menjalankan serangkaian percobaan di mana pengguna melakukan autentikasi menggunakan RFID dan OTP. Percobaan ini dilakukan sebanyak 5 kali pada 5 tag RFID yang berbeda. Tingkat keberhasilan dihitung sebagai persentase dari percobaan yang berhasil.

$$\text{Akurasi} = \frac{\text{Jumlah Percobaan Berhasil}}{\text{Total Percobaan}}$$

Tabel 1 Skema Percobaan Keberhasilan Otentikasi

No	No Tag RFID	Percobaan				
		1	2	3	4	5
1	001	(Y/N)	(Y/N)	(Y/N)	(Y/N)	(Y/N)
2	002	(Y/N)	(Y/N)	(Y/N)	(Y/N)	(Y/N)
3	003	(Y/N)	(Y/N)	(Y/N)	(Y/N)	(Y/N)
4	004	(Y/N)	(Y/N)	(Y/N)	(Y/N)	(Y/N)
5	005	(Y/N)	(Y/N)	(Y/N)	(Y/N)	(Y/N)

b. Mengetahui Log History Keluar Masuk

Untuk memastikan sistem keamanan pintu yang menggunakan metode *Two-factor Authentication* dapat berfungsi dengan baik dalam mencatat dan melacak log aktivitas keluar masuk, pengujian log history dapat dilakukan dengan membuat skema basis data yang dapat menyimpan informasi log, termasuk waktu, tanggal, identitas pengguna, nomor kartu RFID dan status (keluar/masuk) serta memastikan bahwa setiap percobaan akses tercatat dengan benar dan mencakup informasi yang akurat. Log history yang digunakan oleh peneliti sendiri menggunakan database lokal server yang diintegrasikan dengan alat NodeMCU ESP 32. Dengan melaksanakan pengujian ini, sistem diharapkan dapat mencatat dan menyediakan log history yang akurat dan dapat diandalkan, memberikan wawasan yang berharga mengenai aktivitas keluar masuk yang terjadi. Log

history yang baik tidak hanya membantu dalam audit keamanan tetapi juga dalam analisis kebiasaan penggunaan dan identifikasi potensi ancaman.

6. Pemeliharaan Sistem

Pada tahapan akhir, peneliti memasukan tahap pemeliharaan sistem yang dimana pada tahapan ini peneliti akan berfokus pada penjagaan dan peningkatan sistem secara berkala yang telah ada untuk melakukan update sistem kemanan agar lebih baik untuk kedepannya. Tahap pemeliharaan sistem ini merupakan tahap yang sangat penting untuk dilakukan secara berkala dalam sebuah siklus pengembangan perangkat yang ada karena tujuan dari pemeliharaan sistem ini adalah untuk memastikan bahwa sistem yang sudah ada bisa tetap beroperasi dan berjalan dengan baik, bebas dari bug, dan siap menerima perubahan jika diperlukan. Selain itu pemeliharaan sistem sendiri juga bertujuan untuk meningkatkan sistem kemanaan yang sudah ada menjadi lebih baik lagi dengan penambahan enkripsi atau dan lain-lain.

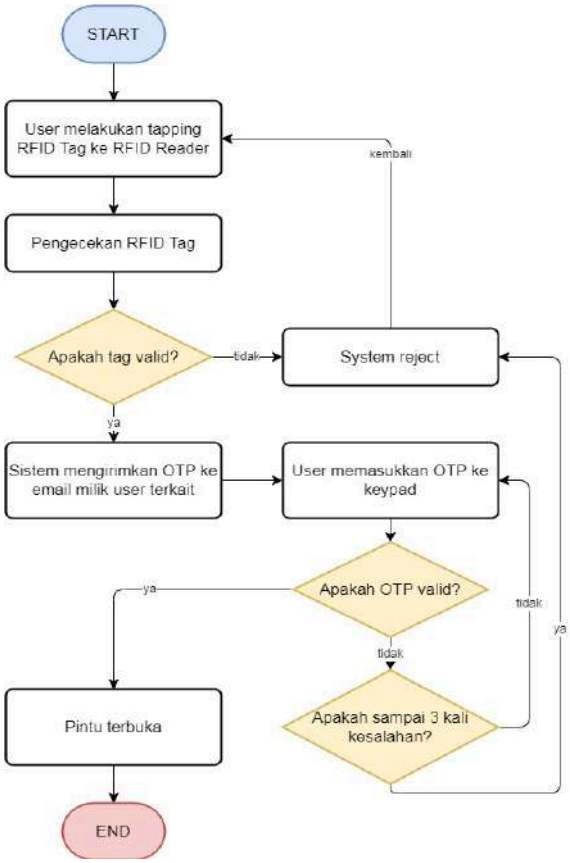
III. HASIL DAN PEMBAHASAN

Pada bab ini, akan dipaparkan hasil dari perancangan alat dan pengujian yang telah dilakukan terkait rancang bangun sistem keamanan pintu menggunakan metode *Two-factor Authentication*. Pengujian pada penelitian ini dilakukan sebanyak 5 kali pengujian, yang pertama dilakukan pengujian keberhasilan otentikasi dan kemudian dilakukan pengujian log history keluar masuk. Pengujian ini dilakukan untuk mengetahui seberapa efesien dan efektif alat yang sudah peneliti buat dengan menggunakan *two-factor authentication* dimana peneliti mengkombinasikan antara otentikasi fisik dengan tag RFID dan otentikasi kode OTP yang akan dikirim melalu email kepada pengguna tag RFID.

A. Perancangan Alat

1. Alur Kerja Sistem Keamanan Pintu

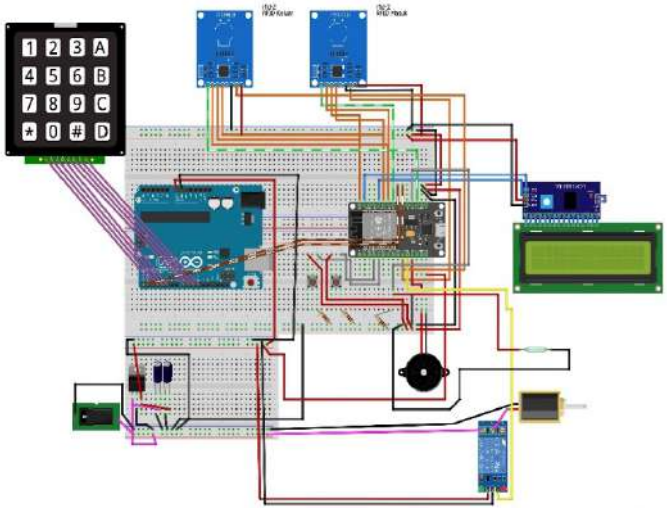
Pada sub bab ini, akan dijelaskan secara rinci mengenai alur kerja sistem keamanan pintu yang dirancang menggunakan metode *Two-factor Authentication*. Penjelasan pada gambar ini mencakup langkah-langkah proses otentikasi mulai dari pengguna melakukan tap dengan tag RFID hingga verifikasi dengan kode OTP yang sudah dikirim ke email pengguna. Alur kerja ini diilustrasikan melalui diagram alur (*flowchart*) untuk mempermudah pemahaman mengenai tahapan-tahapan yang terjadi dalam sistem, serta bagaimana setiap komponen sistem berinteraksi untuk memastikan keamanan akses pintu yang optimal. Berikut adalah diagram alur (*flowchart*) dari alur kerja sistem keamanan pintu.



Gbr 6 Diagram Alur Kerja Sistem Kemanan Pintu

2. Desain *Wiring* Diagram

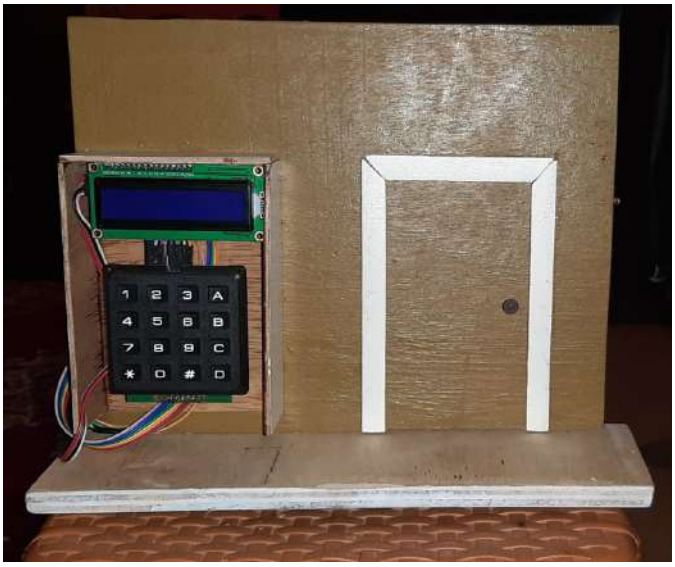
Sub bab ini akan membahas mengenai desain wiring diagram dari sistem keamanan pintu yang menggunakan metode *Two-factor Authentication*. Wiring diagram ini menggambarkan bagaimana setiap komponen elektronik dihubungkan satu sama lain, termasuk sensor rfid, mikrokontroler esp32 dan arduino uno, lcd untuk menampilkan proses yang sedang berlangsung, keypad untuk memasukkan kode OTP yang dikirim ke email, selenoid untuk mengunci pintu, relay modul untuk membantu mereaksi selenoid, sensor magnetic untuk mengetahui pintu sedang terbuka atau tertutup, buzzer untuk menandakan setiap proses berhasil dijalankan dan perangkat tambahan lain sebagai penunjang. Penjelasan pada gambar ini akan mencakup detail koneksi serta bagaimana aliran sinyal berjalan dalam sistem untuk memastikan proses otentikasi dan akses pintu berjalan dengan lancar dan aman. Berikut adalah gambar desain wiring diagram.



Gbr 7 Desain *Wiring* Diagram

3. Hasil *Hardware* Tampak Depan

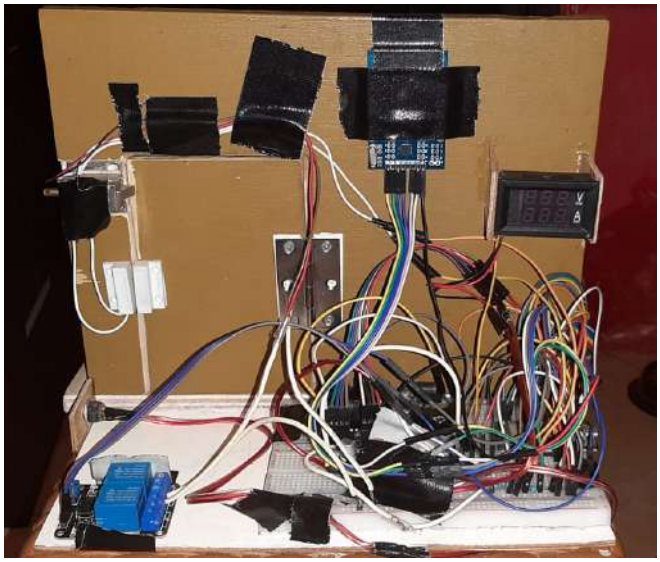
Pada bagian depan pada hardware sistem keamanan pintu terdapat LCD 16x2 Bluelight untuk menampilkan setiap proses yang terjadi pada saat melakukan aktivitas membuka pintu. Selain itu juga terdapat keypad untuk menginputkan kode OTP yang dikirimkan ke email pengguna. Dibelakang keypad juga terdapat satu RFID Reader untuk menangkap sinyal dari tag RFID sebagai proses awal untuk mengirimkan sinyal ke server untuk meregenerate OTP yang akan dikirimkan ke email pengguna.



Gbr 8 Gambar *Hardware* Tampak Depan

4. Hasil *Hardware* Tampak Belakang

Pada bagian belakang hardware terdapat banyak komponen diantaranya ada node mcu esp32 sebagai mikrokontroler utama yang akan menyimpan semua proses yang ada pada sistem kemanan pintu, terdapat arduino uno yang berfungsi untuk mentransfer banyaknya pin pada keypad menjadi beberapa pin saja karena keterbatasan pin yang ada pada node mcu, terdapat RFID Reader untuk scan tag RFID ketika akan keluar pintu, terdapat selenoid sebagai pengunci pintu, terdapat sensor magnetik sebagai sensor utama untuk mengetahui keadaan pintu sedang terbuka atau tertutup, terdapat relay sebagai modul utama untuk selenoid ketika sedang terkunci, serta terdapat voltmeter untuk mengetahui berapa arus listrik yang masuk ke node mcu.



Gbr 9 Gambar *Hardware* Tampak Belakang

B. Hasil Pengujian

1. Pengertian *Two-Factor Authentication*

Pengujian *Two-Factor Authentication* pada sistem keamanan pintu ini dilalukan untuk menguji penggunaan RFID dan OTP dimana meliputi berbagai skenario untuk mengevaluasi keefektifan dan kehandalan sistem dalam memverifikasi identitas pengguna. Data hasil pengujian akan dipresentasikan dan dianalisis, termasuk tingkat keberhasilan otentikasi sistem terhadap berbagai kondisi atau tantangan yang mungkin dihadapi. Analisis ini akan memberikan gambaran mengenai performa sistem dalam situasi nyata dan potensi perbaikan yang dapat dilakukan. Berikut adalah tabel hasil dari pengujian yang sudah dilakukan untuk mengetahui tingkat keberhasilan otentikasi dari sistem keamanan pintu yang sudah dibuat.

Tabel 2 Tabel Hasil Pengujian Keberhasilan Otentikasi

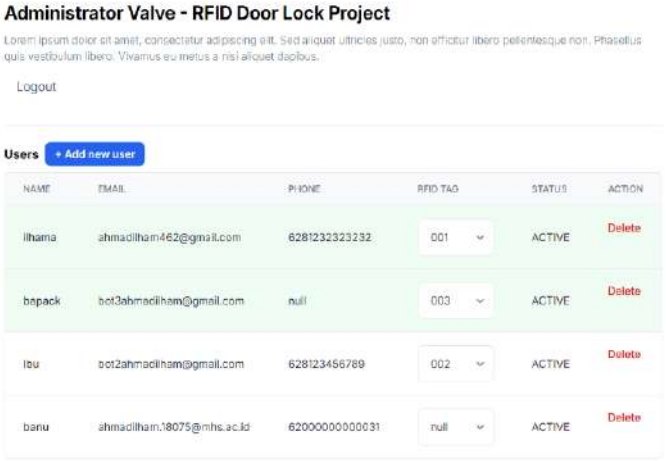
No	No Tag RFID	Percobaan				
		1	2	3	4	5
1	001	Y	Y	Y	Y	Y
2	002	Y	Y	Y	Y	Y
3	003	Y	Y	Y	Y	Y
4	004	Y	Y	Y	Y	Y
5	005	Y	Y	Y	Y	Y

Berdasarkan tabel 2 diatas dapat diperoleh informasi bahwa hasil dari lima kali percobaan pada lima tag RFID setelah dilakukan pengujian keberhasilan sistem keamanan pintu dapat berjalan dengan sangat baik dan tidak mengalamai kendala sama sekali. Sistem kemanan pintu yang sudah dibuat dapat sangat efektif dan handal untuk diterapkan pada kehidupan nyata seperti pada pintu rumah, pintu kamar, dan atau pintu rahasia yang hanya bisa diakses oleh beberapa orang saja. Berikut adalah contoh hasil OTP yang dikirimkan ke email yang sudah terdaftar.

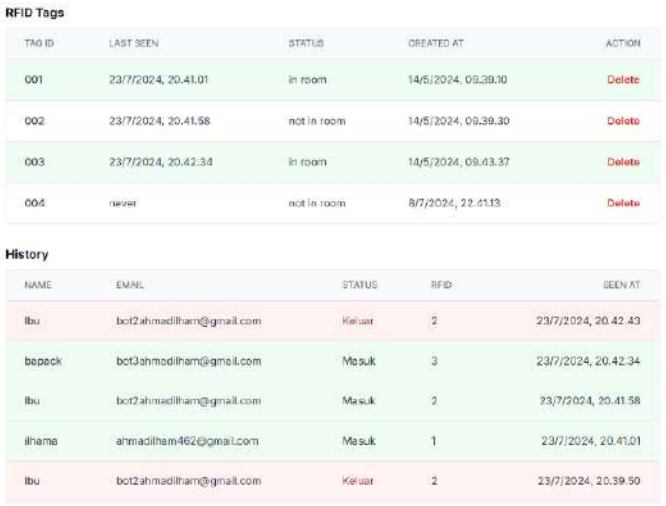
Gbr 10 Hasil OTP yang terkirim ke email

2. Pengujian *Log History* Keluar Masuk

Pengujian log history ini bertujuan untuk memastikan bahwa sistem keamanan pintu yang menggunakan metode *Two-factor Authentication* dapat berfungsi dengan baik, maka perlu dilakukan pencatatan dan pelacakan log aktivitas keluar masuk. Pengujian log history dilakukan dengan skenario yang menyesuaikan dengan skema basis data yang sudah dibuat dimana log history dapat menyimpan informasi waktu, tanggal, identitas pengguna, nomor kartu RFID dan status (keluar/masuk) serta memastikan bahwa setiap percobaan akses tercatat dengan benar dan mencakup informasi yang akurat. Log history dapat dilihat dan diakses melalui web admin yang sudah peneliti sediakan dimana dalam web admin tersebut peneliti dapat mengetahui dan menambahkan user dari alat sistem keamanan pintu, peneliti dapat mengetahui kartu RFID mana saja yang sudah terdaftar dan peneliti juga dapat mengetahui log keluar masuk dari setiap user. Log tersebut berfungsi untuk mencari dan mengetahui siapa saja yang mengakses dan keluar masuk pintu yang sudah terpasang alat tersebut. Berikut adalah hasil dari pengujian log history.



Gbr 11 User yang sedang aktif



Gbr 12 RFID Tags dan Log History Keluar Masuk

Berdasarkan Gbr 11 dan Gbr 12 dapat diketahui bahwa log history yang dibuat oleh peneliti sudah berjalan dengan baik dan benar. Dengan melaksanakan pengujian tersebut, diharapkan sistem dapat mencatat dan menyediakan log history yang akurat dan dapat diandalkan, memberikan wawasan yang berharga mengenai aktivitas keluar masuk yang terjadi. Log history yang baik tidak hanya membantu dalam audit keamanan tetapi juga dalam analisis kebiasaan penggunaan dan identifikasi potensi ancaman.

IV. KESIMPULAN

Dari hasil pengujian dan dan pembahasan di bab sebelumnya, dapat disimpulkan bahwa:

1. Hasil pengujian *Two-factor Authentication* pada sistem keamanan pintu yang sudah dibuat dapat berjalan dengan sangat baik dan tidak mengalamai kendala sama sekali pada

lima kali percobaan dengan lima tag RFID yang sudah didaftarkan. Sistem kemanan pintu yang sudah dibuat sangat memungkinkan untuk diterapkan pada kehidupan nyata seperti pada pintu-pintu rahasia yang hanya bisa diakses oleh beberapa orang saja.
2. Dari hasil pengujian log history pada sistem keamanan pintu menggunakan metode *Two-factor Authentication* yang sudah dibuat, dapat diketahui bahwa fitur tersebut sudah bisa berfungsi dengan baik dan benar. Hal tersebut dibuktikan dengan pencatatan log history yang sangat lengkap dan rinci.

V. SARAN

Dari hasil pengujian, terdapat beberapa saran yang dapat dilakukan untuk mengembangkan sistem agar mencapai hasil yang lebih optimal, yaitu sebagai berikut:

1. Melakukan penelitian lebih lanjut untuk mengoptimalkan algoritma otentikasi sehingga proses verifikasi dapat dilakukan dengan lebih cepat tanpa mengurangi tingkat keamanan.
2. Pertimbangkan untuk mengintegrasikan teknologi biometrik, seperti sidik jari atau pengenalan wajah, sebagai salah satu faktor otentikasi untuk meningkatkan keamanan dan kenyamanan pengguna.
3. Mengembangkan aplikasi mobile yang dapat digunakan sebagai inovasi sistem untuk otentikasi, memungkinkan pengguna untuk menerima kode OTP (*One-Time Password*) atau notifikasi otentikasi melalui smartphone mereka dengan lebih cepat lagi.

REFERENSI

[1] G. C. Mahardhika and F. David, "Implementasi Two Factor Authentication (2FA) pada Sistem Keamanan Otentikasi User di Aplikasi Kasir Legends Barbershop," Jurnal Sistem dan Teknologi Informasi (Justin), vol. 8, no. 4, p. 357, 2020, doi: 10.26418/justin.v8i4.42247.

[2] S. Sinurat, "RANCANG BANGUN SISTEM AKSES DAN SECURITY BRANKAS MENGGUNAKAN METODE OTP BERBASIS IoT," Teknik Elektro Universitas Medan Area, 2022.

[3] Y. Ariyanto, "Algoritma Rc4 Dalam Proteksi Transmisi Dan Hasil Query Untuk Ordbms Postgresql," Jurnal Informatika, vol. 10, no. 1, pp. 127–136, 2010, doi: 10.9744/informatika.10.1.53-59.

[4] D. Dwi Septian and dan Tatyantoro Andrasto, "Pengaman Pintu Rumah Menggunakan Otentifikasi Dua Faktor Berbasis Arduino Uno," Edu Elektrika Journal, vol. 9, no. 2, pp. 24–30, 2020.

[5] A. Fauji, A. Goeritno, L. Hardian, and B. A. Prakoso, "Embedded Device pada Smarthome System Berbasis IoT untuk Pengoperasian Pintu Gerbang Terkendali melalui Smartphone," Jurnal Rekayasa Elektrika, vol. 18, no. 1, 2022, doi: 10.17529/jre.v18i1.22224.

[6] D. Kalingga, Perancangan Algoritma Two Factor Authentication Untuk Keamanan Jaringan Internet of Things. 2023.

[7] M. Cs. Bronto Kuncoro, Prof.Dr.Ir. Eko Sediyono, M.Kom., Winarso Martyas Edi, S.Kom., "Penerapan Sistem One Time Password Dengan Motor Servo Untuk Pengaman Rumah," Teknik Informatika Fakultas Teknologi Informasi Universitas Kristen SatyaWacana, no. July, 2016.

[8] Mundhir, RANCANG BANGUN APLIKASI SISTEM KEAMANAN WEBSITE DENGANMENERAPKAN AUTENTIFIKASI 2 FAKTOR MENGGUNAKAN SMS GATEAWAY. 2016.

[9] E. M. J. Hatami Ra'is Bukhari, Vera Suryani, "Two Step Authentication Dengan Rfid Dan Algortima Time-based One Time Password Pada Smart Lock," Jurnal Tugas Akhir Fakultas Informatika e-Proceeding of Engineering : Vol.8, No.2 April 2021 | Page 3577, vol. 8, no. 2, pp. 3577–3596, 2021, [Online]. Available: https://openlibrarypublications.telkomuniversity.ac.id/index.php/engineering/article/viewFile/14739/14516

[10] R. Pasmah, A. J. Lubis, and A. Usman, "Prototipe Sistem Keamanan Ruangan Menggunakan Finger Print dan Keypad Matrix dengan One Time Pad," Journal of Computer Science and Information Technology E-ISSN 2774-4647, vol. 1, no. 2, pp. 53–62, 2021, doi: 10.47065/explorer.v1i2.89.

[11] T. Handayani, A. Basuki, S. Sudiana, and I. Dirgantara, "Rancang Bangun Sistem Keamanan Pintu menggunakan Metode Pengenalan Wajah berbasis Internet of Things," Aviation Electronics, Information Technology, Telecommunications, Electricals, Controls (AVITEC), vol. 5, no. 1, p. 1, 2022, doi: 10.28989/avitecv5i1.1393.

[12] N. Sarah Hapsari, Y. Fatman, and E. Penulis Korespondensi, "JURNAL MEDIA INFORMATIKA BUDIDARMA Implementasi Metode One Time Password pada Sistem Pemesanan Online," Jurnal Media Informatika Budidarma, vol. 4, pp. 930–939, 2020, doi: 10.30865/mib.v4i4.2195.

[13] H. Raka Herdiantoro and M. Reza Redo Islami, "Implementasi Two-Factor Authentication (2Fa) Dan Firewall Policies Dalam Mengamankan Website," Jmik (Jurnal Mahasiswa Ilmu Komputer), vol. 4, no. 1, pp. 1–9, 2023, [Online]. Available: https://scholar.ummetro.ac.id/index.php/IlmuKomputer/article/download/3300/1620/

[14] I. Permana, M. Hardjianto, and K. Ahmad Baihaqi, "Securing the Website Login System with the SHA256 Generating Method and Time-based One-time Password (TOTP)," Systematics, vol. 2, no. 2, pp. 65–71, 2020, doi: 10.35706/sysv2i2.3756.