



Pemodelan Sistem Akses Masuk Ruangan Pribadi Berdasarkan Inputan *Password* Dengan Notifikasi *E-Mail* Berbasis IoT

Johan Makal¹, Ronny Katuuk², Johan Pongoh³, Ali Ramschie⁴

Sarjana Terapan Teknik Listrik, Teknik Elektro, Politeknik Negeri Manado, Manado ¹

D3 Teknik Listrik, Teknik Elektro, Politeknik Negeri Manadoi, Manado ^{3,4}

D3 Teknik Komputer, Teknik Elektro, Politeknik Negeri Manadoi, Manado ²

E-mail: ali.a.s.ramschie@elektro.polimdo.ac.id

Abstrak

Sistem keamanan akses masuk ruangan memegang peranan penting dalam melindungi aset dan informasi yang berharga. Namun, penggunaan kunci fisik atau kartu akses konvensional telah menunjukkan beberapa keterbatasan, terutama dalam hal keamanan dan manajemen akses. Oleh karena itu, pengembangan sistem akses masuk yang lebih canggih dan terhubung dengan internet (IoT) menjadi penting untuk memastikan keamanan yang lebih baik serta manajemen akses yang lebih efisien.

Penelitian ini bertujuan untuk memodelkan sistem akses masuk ruangan pribadi berbasis IoT yang menggunakan inputan password melalui keypad untuk autentikasi pengguna, serta dapat memberikan notifikasi melalui e-mail saat akses dicoba untuk masuk secara ilegal.

Penelitian ini akan menggunakan pendekatan pengembangan sistem berbasis IoT. Pengembangan sistem melibatkan pemrograman mikrokontroler yang terhubung dengan sensor dan modul WiFi untuk mengelola inputan password, memvalidasi pengguna, dan mengirimkan notifikasi melalui e-mail.

Hasil pengujian menunjukkan bahwa model sistem akses masuk ruangan pribadi berbasis IoT dapat memvalidasi orang yang mempunyai akses masuk ruangan melalui penginputan password yang sesuai untuk membuka kunci pintu, dan jika passwordnya tidak sesuai, maka secara otomatis alarm akan berbunyi dan pemilik ruangan akan menerima notifikasi melalui e-mail bahwa ada orang yang tidak memiliki akses mencoba untuk masuk, sehingga pemilik ruangan dapat menonaktifkan sistem jarak jauh.

Kata kunci—Keypad, Akses masuk, Notifikasi e-mail, IoT

1. PENDAHULUAN

Maraknya teknologi Internet of Things (IoT) telah memberikan dampak signifikan pada berbagai aspek kehidupan, termasuk sistem keamanan (Truyadi, et al., 2021), (Putra et al., 2023) dan akses terhadap ruangan (Affandi et al., 2023), (Kristomson et al., 2018). IoT memungkinkan perangkat yang terhubung untuk berkomunikasi dan bertukar data secara real time, memberikan kemudahan dan efisiensi dalam mengelola sistem keamanan (Wilianto et al., 2018). Sistem akses ruangan berbasis IoT menggunakan entri kata sandi dan notifikasi e-mail merupakan implementasi dari teknologi ini yang memberikan solusi modern untuk keamanan pribadi.

Saat ini, kebutuhan akan sistem keamanan yang andal dan dapat diakses semakin meningkat. seiring dengan meningkatnya ancaman keamanan (Anggono et al., 2023). Banyak sistem konvensional yang masih menggunakan kunci fisik atau kartu akses

yang mudah dicuri atau disalin. Oleh karena itu, memerlukan sistem yang tidak hanya aman tetapi juga mampu memberikan notifikasi real-time kepada pengguna jika ada akses yang mencurigakan atau tidak sah (Qureshi et al., 2023).

Tujuan dari penelitian ini adalah untuk memodelkan sistem akses masuk ruangan pribadi yang berbasis pada dengan notifikasi e-mail menggunakan teknologi IoT. Penelitian ini diharapkan dapat: Menghasilkan sistem yang mampu memberikan keamanan lebih tinggi dibandingkan sistem konvensional; Meningkatkan efisiensi dalam pengelolaan akses masuk ruangan; Memberikan notifikasi real-time kepada pengguna mengenai status akses ruangan.

Penelitian ini memiliki beberapa manfaat, antara lain:

1. Keamanan yang Lebih Baik: Sistem ini dirancang untuk meningkatkan keamanan ruangan dengan menggunakan teknologi IoT yang lebih canggih .
2. Pemberitahuan Real-time: Dengan adanya notifikasi e-mail, pengguna dapat segera mengetahui jika ada percobaan akses yang tidak sah, sehingga dapat mengambil tindakan yang diperlukan dengan cepat .

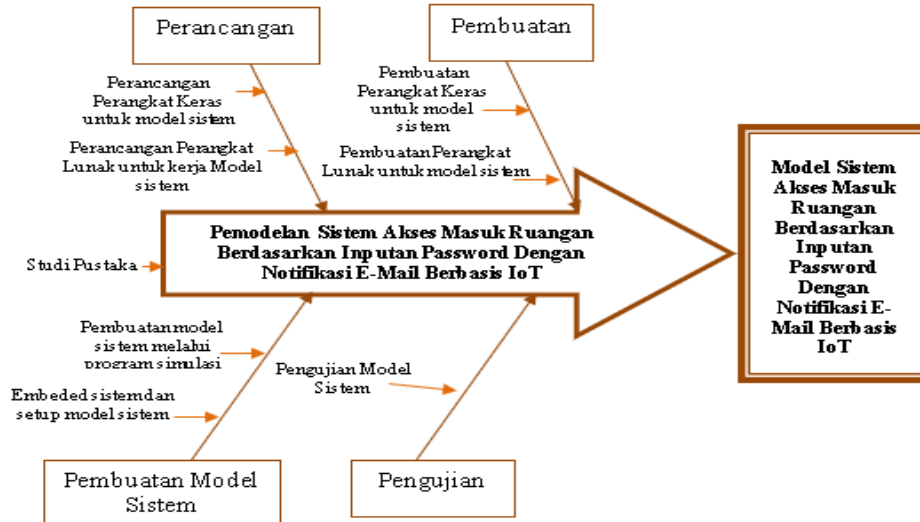
Adapun isu-isu terkait dengan topik Penelitian, seperti penelitian yang telah dilakukan sebelumnya meliputi:

1. Implementasi Teknologi NFC Untuk Akses Pintu Masuk dan Keluar, dimana Penelitian ini menghasilkan aplikasi sistem akses pintu masuk dan keluar menggunakan NFC yang bisa mengetahui waktu *user* masuk dan keluar ruangan, dan siapa saja yang memiliki hak untuk masuk dalam sebuah ruangan (Djamar et al., 2017).
2. Sistem Keamanan Ruangan Berbasis Arduino Uno R3 Dengan Sensor PIR dan *Fingerprint*, Dimana penelitian ini menghasilkan sistem keamanan dengan memanfaatkan teknologi mikrokontroler berupa Arduino Uno R3 sebagai pusat pengendali keamanan , selain itu teknologi keamanan ini dilengkapi dengan sensor *Passive Infra Red* (PIR) yang diletakkan dalam ruangan serta *fingerprint* sebagai akses masuk yang telah dirancang untuk mengamankan barang yang ada dalam ruangan, teknologi ini dirancang untuk mengamankan objek dalam ruangan dengan membatasi akses masuk ruangan tersebut melalui teknologi *fingerprint* sebagai pembuka utama pintu masuk (Mahfudh et al., 2021).
3. Perancangan Sistem Pengenalan Wajah untuk Keamanan Ruangan Menggunakan Metode *Local Binary Pattern Histogram*, dimana penelitian ini berhubungan dengan rancang bangun sistem keamanan akses ruangan menggunakan teknologi pengenalan wajah (*face recognition*) dengan metode LBPH yang berbasis Raspberry Pi. Sistem yang dikembangkan terdiri dari dua bagian, yaitu perangkat yang terpasang pada Raspberry Pi sebagai otak kamera, dan aplikasi Telegram pada *smartphone*. Kamera ini dapat mengenali wajah pengguna yang telah terdaftar serta beberapa orang lain yang diizinkan untuk mengakses ruangan. Jika kamera tidak mengenali wajah yang terdeteksi, maka akan mengambil gambar dan mengirimkannya ke pemilik rumah melalui aplikasi Telegram sebagai notifikasi untuk mengambil tindakan lebih lanjut terhadap kedatangan orang yang tidak dikenal (Sunardi et al., 2022).
4. Sistem Keamanan Ruangan Berbasis Internet Of Things Dengan Menggunakan Aplikasi Android, dimana penelitian yang dilakukan untuk pengamanan ruangan dengan menggunakan sensor inframerah dan kamera untuk mendeteksi orang masuk dan mengambil gambar, selanjutnya gambar tersebut akan dikirimkan ke *smartphone android*, selanjutnya petugas atau admin akan memverifikasi apakah orang tersebut dapat diberikan akses masuk atau tidak (Kristomson et al., 2018).
5. Rancang Bangun Sistem Keamanan Rumah Berbasis *Internet Of Things* dengan Platform Android, dimana penelitian yang dilakukan berhubungan dengan pengamanan rumah yang dapat dilakukan melalui *smartphone* sehubungan dengan pengontrolan kerja pintu, lampu dan kebocoran gas untuk menghindari terjadinya kebakaran (Khana et al., 2018).

Pada penelitian ini mengusulkan model yang mengintegrasikan teknologi IoT dengan sistem keamanan berbasis *web server* serta fitur notifikasi e-mail. Segi originalitas penelitian ini terletak pada kombinasi fitur-fitur tersebut yang belum banyak diterapkan secara bersamaan dalam sistem akses ruangan pribadi .

2. METODE PENELITIAN

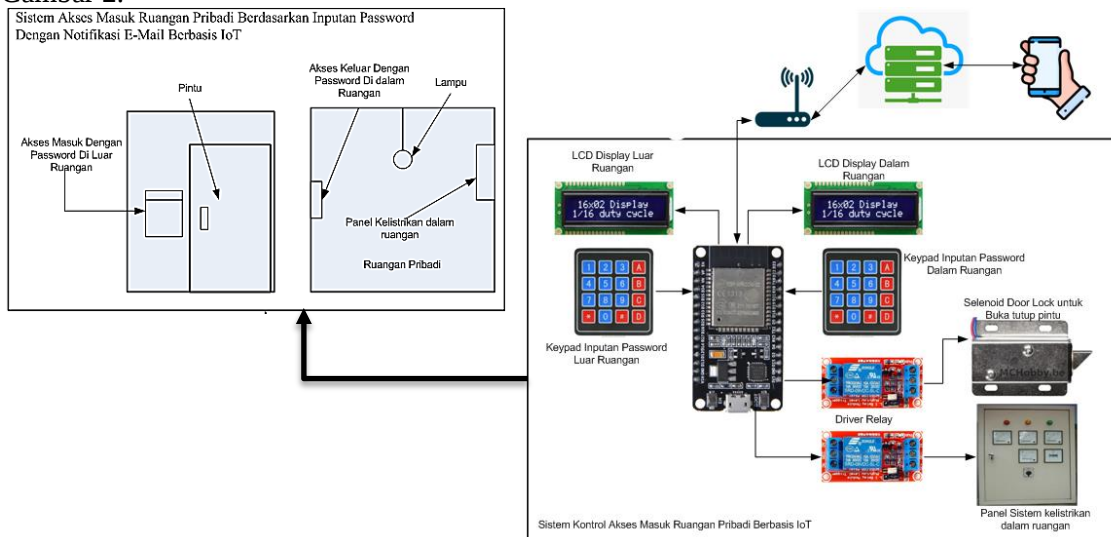
Dalam menghasilkan model Sistem Akses Masuk Ruangan Pribadi Berdasarkan Inputan *password* Dengan Notifikasi E-Mail Berbasis IoT, metode yang digunakan adalah metode *prototyping*, dimana tahapannya seperti diperlihatkan pada Gambar 1.



Gambar 1. Metode Penelitian (*Prototyping*)

2.1 Perancangan dan Pembuatan Model Sistem Sistem Akses Masuk Ruangan Pribadi Berdasarkan Inputan *password* Dengan Notifikasi E-Mail Berbasis IoT

Dalam menghasilkan Model Sistem Akses Masuk Ruangan Pribadi Berdasarkan Inputan *password* Dengan Notifikasi E-Mail Berbasis IoT, maka tahapan awalnya adalah membuatnya dalam bentuk blok diagram sistem. Blok diagram Model Sistem Akses Masuk Ruangan Pribadi Berdasarkan Inputan *password* Dengan Notifikasi E-Mail Berbasis IoT diperlihatkan pada Gambar 2.



Gambar 2. Blok diagram Model Sistem Akses Masuk Ruangan Pribadi Berdasarkan Inputan *password* Dengan Notifikasi E-Mail Berbasis IoT

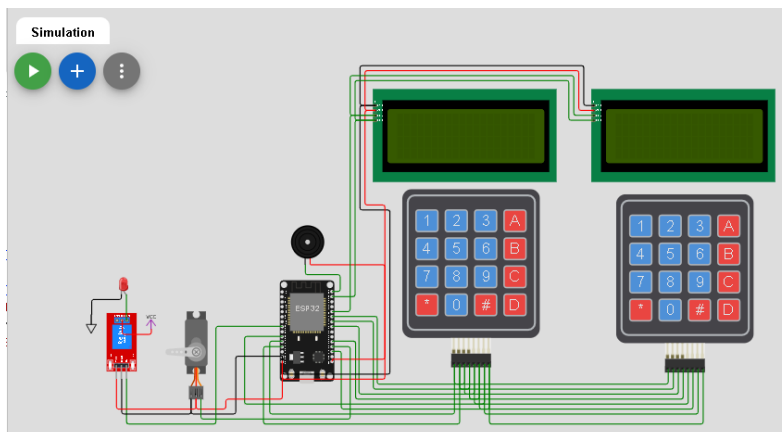
Keterangan Gambar 2:

1. Kontroler difungsikan sebagai pusat pengolahan data untuk proses verifikasi inputan *password* untuk akses masuk ruang pribadi dan proses pengontrolan sistem kelistrikan dalam ruangan saat akses masuk sesuai. Disamping itu juga kontroler difungsikan sebagai media

komunikasi dengan *web server* untuk monitoring kondisi sistem akses masuk ruangan, dimana saat terindikasi akses masuk ruangan tidak sesuai, maka secara otomatis kontroler akan mengirimkan informasi ke e-mail dari pemilik ruangan sebagai notifikasi kesalahan akses masuk melalui *web server*, sehingga pemilik ruangan dapat menonaktifkan sistem akses masuk ruangan melalui perangkat *smartphone*-nya yang telah tertanam dengan aplikasi sesuai dengan *platform* dari penyedia jasa layanan IoT.

2. *Keypad* difungsikan sebagai media penginputan *password*, baik untuk masuk ke dalam ruangan, menutup pintu dan saat akan keluar ruangan.
3. LCD display, difungsikan sebagai media penampil informasi sehubungan dengan prosedur penginputan *password*, kondisi akses masuk diterima atau ditolak, kondisi ada tidaknya orang dalam ruangan serta kondisi sistem akses masuk ruangan apakah dalam kondisi aktif atau dikunci oleh pemilik ruangan.
4. *Driver relay*, difungsikan sebagai *On/Off* sistem kelistrikan yang ada dalam ruangan, serta *On/Off solenoid doorlock* untuk buka tutup pintu.
5. Akses Point (*wifi*), berfungsi sebagai media komunikasi internet antara kontroler dengan *web server* untuk proses monitoring dan pengontrolan sistem akses masuk ruangan.
6. *Web server*, berfungsi sebagai media untuk pengguna dalam proses memonitoring dan mengontrol sistem sekuritas jarak jauh, melalui perangkat *smart phone*.

Setelah proses pembuatan model sistem selesai dilakukan, tahapan selanjutnya adalah proses pembuatan model sistem (perangkat keras) melalui aplikasi simulasi sistem, dimana proses pembuatan simulasi model sistem akses masuk ruangan berbasis IoT seperti yang diperlihatkan pada Gambar 3.



Gambar 3. Pembuatan simulasi model sistem akses masuk ruangan berbasis IoT

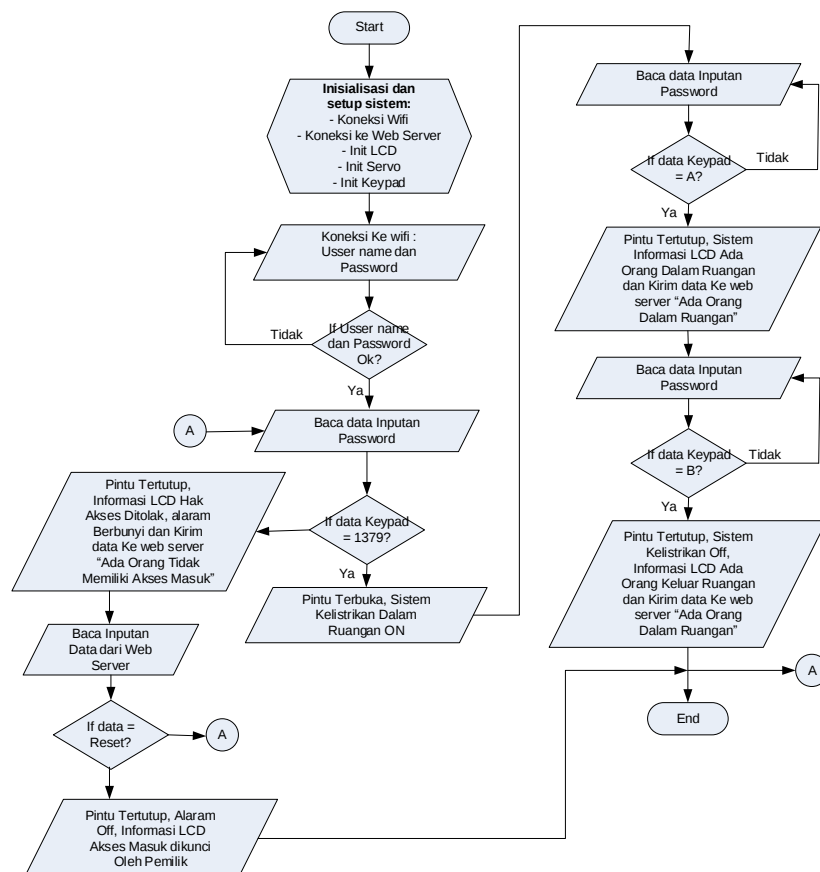
2.2 Perancangan dan Pembuatan Perangkat Lunak

Untuk menjalankan model sistem akses masuk ruangan pribadi dengan notifikasi *e-mail* berbasis IoT, maka dibutuhkan perangkat lunak yang akan di-*embedded*-kan ke kontroler, dimana langkah awal dalam menghasilkan perangkat lunak ini adalah perancangan perangkat lunak dalam bentuk diagram alir (*Flowchart*). Adapun *Flowchart*-nya diperlihatkan pada Gambar 4, dimana prosedur kerjanya sebagai berikut:

1. Saat sistem dijalankan, maka yang dijalankan pertama kali adalah bagian inisialisasi dan *setup* sistem, yang mencakup: inisialisasi *library* yang akan digunakan, mengkoneksikan kontroler ke *web server* melalui akses point (*Router*) berdasarkan (Nama akses point, *Web server* dan Token dari *dashboard web server*). Prosedur pengkoneksian ini akan berlangsung, sampai proses pengkoneksiannya berhasil. Setelah proses koneksi berhasil, maka prosedur selanjutnya akan dijalankan.
2. Membaca inputan data *password* akses masuk ruangan melalui inputan dari *Keypad*, dimana *password*-nya adalah 1379. Jika inputan *password* sesuai, maka sistem akan membuka pintu

dengan mengaktifkan servo motor yang difungsikan sebagai anak kunci dari pintu. Saat pintu terbuka, maka bersamaan dengan itu juga sistem kelistrikan dalam ruangan akan diaktifkan, ditandai dengan menyalanya lampu (indikator Led), serta informasi yang ditampilkan pada layar LCD berupa "Pintu Terbuka, Sistem kelistrikan Aktif". Jika inputan *password* tidak sesuai, maka secara otomatis sistem akan mengaktifkan alarm dan mengirimkan notifikasi ke *e-mail* bahwa ada orang yang mencoba masuk ruangan yang tidak memiliki hak akses. Berdasarkan notifikasi tersebut, pemilik ruangan dapat mengunci sistem akses masuk ruangan jarak jauh melalui perangkat *smartphone* yang terkoneksi dengan *web server*. Saat kontroler membaca data dari *web server* bahwa sistem akses masuk ruangan telah dikunci, maka secara otomatis alarm akan dinonaktifkan dan sistem akses masuk ruangan tidak dapat digunakan.

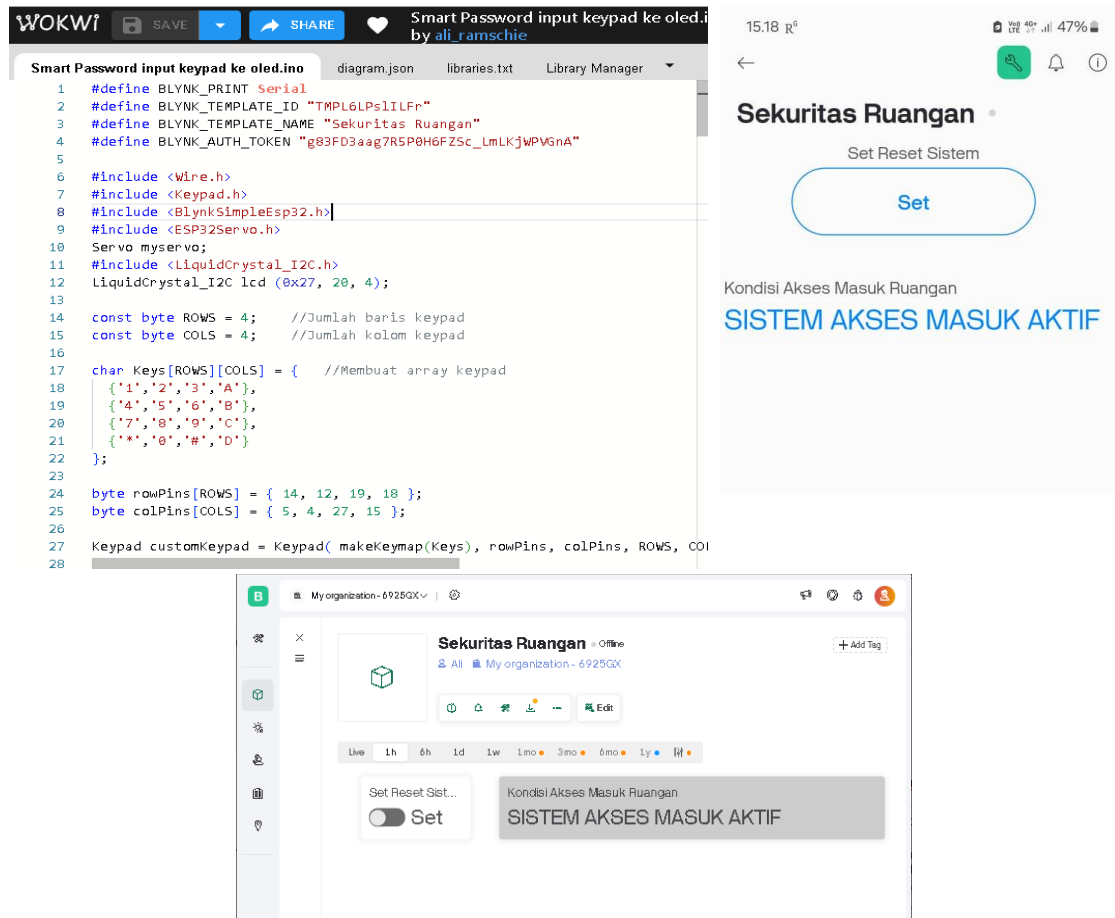
3. Jika pintu telah terbuka, dan orang telah berada di dalam ruangan, prosedur selanjutnya adalah menutup pintu dengan cara menekan huruf A pada *Keypad*. Saat huruf A pada *keypad* ditekan, maka pintu akan tertutup melalui aktifnya servo motor ke posisi 0° dan informasi pada tampilan LCD bahwa ada orang dalam ruangan, serta informasi serupa dikirimkan juga ke *web server*.
4. Untuk keluar ruangan, maka yang dilakukan adalah menginputkan *web server* dengan prosedur seperti pada point 2. dan jika telah berada di luar ruangan dan akan menutup pintu, maka hal yang dilakukan adalah menekan tombol B pada *keypad*, dimana saat tombol ini ditekan, maka secara otomatis pintu akan tertutup dan sistem kembali ke prosedur semula membaca data inputan *password* untuk masuk ke dalam ruangan pribadi.



Gambar 4. Diagram alir untuk kerja sistem akses masuk ruangan pribadi dengan notifikasi *e-mail* berbasis IoT.

Setelah proses perancangan perangkat lunak dibuat, selanjutnya proses pembuatan program dan pembuatan *dashboard* pada *web server*, sebagai *user interface* antara pemilik ruangan dengan

sistem akses masuk ruangan, yang diperlihatkan pada Gambar 5.



Gambar 5. Pembuatan program dan tahapan pembuatan *dashboard* pada *web server* serta pada perangkat *Smart Phone*.

3. HASIL DAN PEMBAHASAN

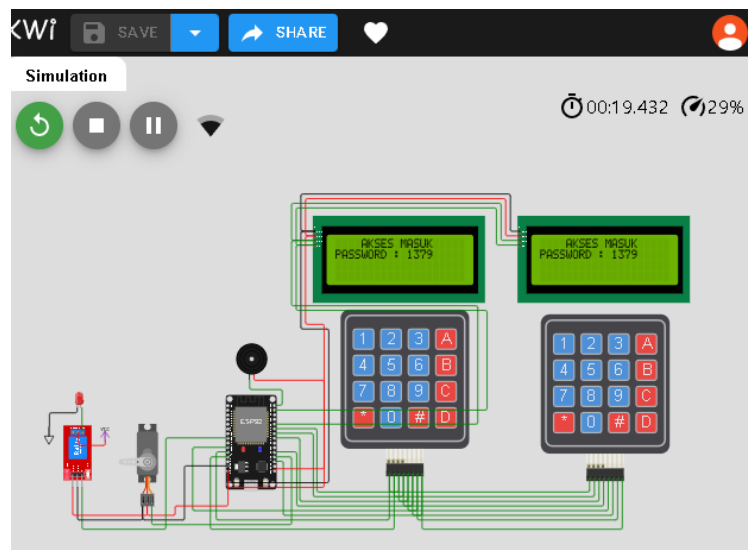
Pengujian model sistema akses masuk ruangan pribadi melalui penginputan *password* dengan notifikasi *e-mail* berbasis IoT, menggunakan metode pengujian secara prosedural guna mengevaluasi unjuk kerja model sistem dalam mengamankan ruangan pribadi terhadap pihak-pihak yang tidak memiliki akses yang mencoba untuk masuk..

3.1. Pengujian Model Sistem Proses Penginputan Password Yang Benar

Pengujian model sistem saat pertama kali diaktifkan, bertujuan untuk menguji kerja sistem apakah dapat terkoneksi dengan *web server* atau tidak, dimana hal yang dilakukan sistem adalah menjalankan sistem hak akses masuk ruangan pribadi yang telah dihasilkan melalui program simulasi, adapun program yang dijalankan pertama kali adalah bagian program untuk melakukan koneksi ke akses point berdasarkan nama dari akses point dan *web server*-nya serta kode token dari *dashboard* dari *web server*. Adapun bagian programnya adalah **Blynk.begin(auth, ssid, pass);**, dimana prosedur ini kan dilakukan secara terus menerus sampai terkoneksi antara perangkat kontroler dengan *web server*.

Jika proses koneksi berhasil, maka sistem akses masuk ruangan pribadi dapat dilakukan, dimana pada bagian penampil LCD yang ada di bagian simulasi sistem (bagian perangkat keras) akan menampilkan informasi akses masuk dan masukan *web server*, sehingga pengguna ruangan dapat melakukan proses penginputan *password* melalui *keypad* yang berada di luar ruangan. Untuk proses masuk ruangan, hal yang dilakukan adalah menginputkan *password*, dimana *password* -

nya berupa kombinasi angka “1379” dan selanjutnya menekan Tombol # untuk melakukan proses validasi *password*. Gambar 6 memperlihatkan proses penginputan *password* melalui *keypad* untuk akses masuk ruangan.



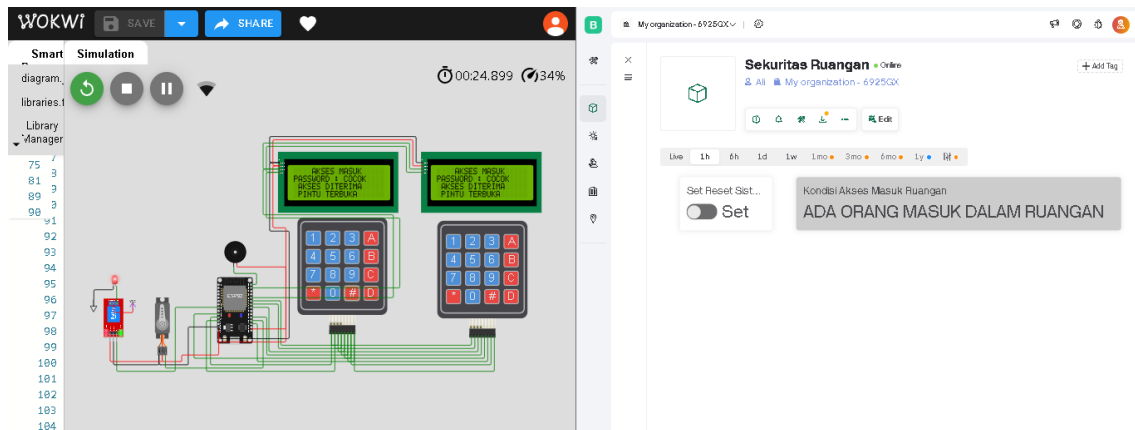
Gambar 6. Proses penginputan *password* melalui *keypad* untuk akses masuk ruangan

Dari hasil pengujian yang dilakukan terhadap model sistem akses masuk ruangan pribadi seperti yang diperlihatkan pada Gambar 6, terlihat bahwa proses penginputan data *password* dapat dilakukan melalui *keypad* yang datanya diolah melalui kontroler dan selanjutnya di tampilkan ke penampil LCD. Adapun bagian program yang dijalankan untuk prosedur ini adalah sebagai berikut:

```
customKey = customKeypad.getKey(); //Baca input keypad

//-----Prosedur jika input berupa angka-----//
switch(customKey){
  case '0' ... '9':
    number = number * 10 + (customKey - '0');
    lcd.setCursor (11, 1);
    lcd.print (number); // menampilkan informasi web server yang di tekan ke LCD
    break;
```

Setelah proses penginputan *password* selesai dilakukan, maka selanjutnya adalah memvalidasi data *web server* dengan cara menekan tombol “#” pada *keypad*. Jika data *password* -nya sesuai, maka pintu akan terbuka. Adapun hasil pengujian proses buka pintu dengan *password* yang benar diperlihatkan pada Gambar 7.



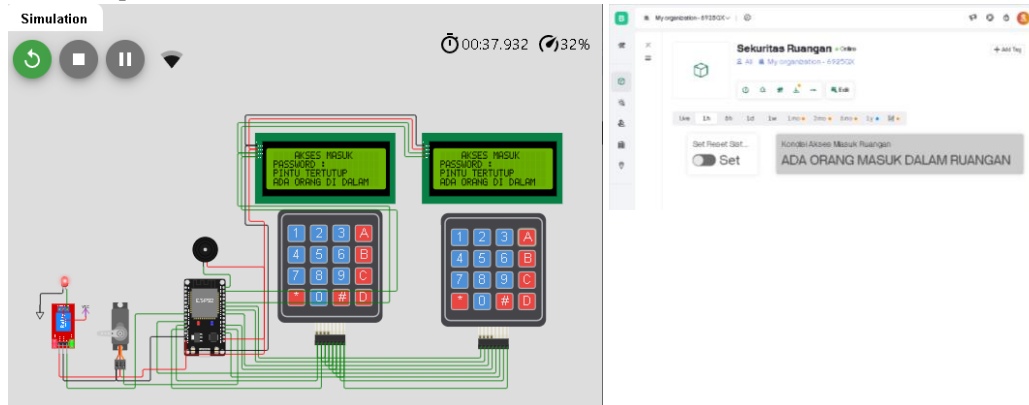
Gambar 7. Pengujian proses buka pintu dengan *password* yang benar

Dari hasil pengujian yang dilakukan seperti yang diperlihatkan pada Gambar 7 terlihat bahwa saat sistem mengidentifikasi bahwa data *password* yang diinputkan sesuai, maka secara otomatis sistem akan membuka pintu melalui aktifnya motor servo yang bergerak pada sudut 90°, disamping itu juga sistem akan mengaktifkan sistem kelistrikan dalam ruangan yang ditandai dengan nyalanya indikator LED, serta informasi yang ditampilkan pada LCD *display* bahwa *password* yang diinputkan cocok, akses masuk diterima dan pintu terbuka. Adapun bagian program yang dijalankan untuk proses ini adalah sebagai berikut:

```
case '#':
    if(number == password){          //Jika web server benar, maka
        myservo.write(90);
        delay(15);
        lcd.setCursor (0, 2);
        lcd.print ("      ");
        lcd.setCursor (0, 2);
        lcd.print (" AKSES DITERIMA");
        lcd.setCursor (0, 3);
        lcd.print ("      ");
        lcd.setCursor (0, 3);
        lcd.print (" PINTU TERBUKA");
        digitalWrite(lampu, HIGH);
        noTone(buzzer);
        lcd.setCursor (11, 1);
        lcd.print ("      ");
        lcd.setCursor (11, 1);
        lcd.print ("COCOK");
        number = 0;
    }
```

Saat pengguna telah berada dalam ruangan, maka hal yang dilakukan adalah mengunci pintu melalui proses penekanan huruf A yang berada di *Keypad* di dalam ruangan, di mana saat huruf A ditekan, maka secara otomatis pintu akan terkunci dengan aktifnya motor servo yang bergerak di posisi 0° dan sistem akan menginformasikan melalui tampilan LCD bahwa pintu telah terkunci dan ada orang dalam ruangan. Informasi ini juga akan dikirimkan ke *web server* sehingga pemilik ruangan mengetahui ada orang yang masuk ke dalam ruangan pribadinya, dan orang tersebut

memiliki hak akses kedalam ruangan. Hasil pengujian proses tutup pintu dari dalam ruangan diperlihatkan pada Gambar 8.

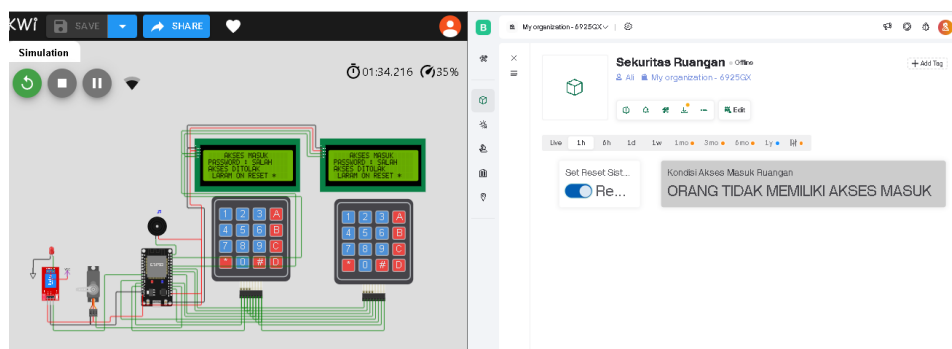


Gambar 8. Hasil pengujian proses tutup pintu dari dalam ruangan

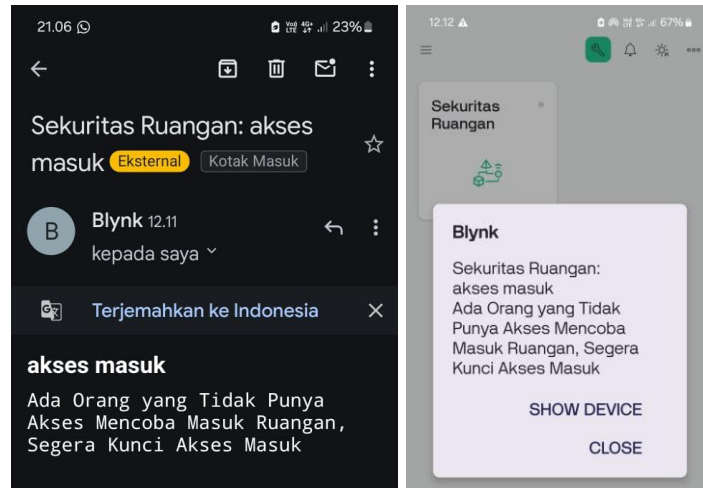
Saat orang dalam ruangan akan keluar, maka hal yang dilakukan adalah menginputkan *password* yang sesuai seperti prosedur pada proses buka pintu. Saat pintu telah terbuka dan orang telah berada di luar ruangan, maka untuk menutup pintu maka hal yang dilakukan adalah menekan huruf B pada *keypad*. Saat sistem mendeteksi data huruf B, maka secara otomatis sistem akan mengunci pintu melalui aktifnya motor servo ke posisi 0° dan sistem kembali ke proses awal untuk akses masuk ruangan.

3.2. Pengujian Model Sistem Akses masuk Ruangan Pribadi Saat Password Salah

Pengujian dilakukan pada sistem dengan menginputkan *password* yang salah, di mana saat hal ini dilakukan, maka sistem akan memferifikasi data *password* tersebut dan jika datanya tidak sesuai dengan data referensi (tidak diberi akses), maka secara otomatis sistem akan mengaktifkan alarm melalui aktifnya buzzer dan kontroler akan mengirimkan notifikasi ke *e-mail* dan notifikasi pada aplikasi *web server* yang berada di perangkat *smart phone* dari si pemilik ruangan bahwa ada orang yang mencoba masuk ke dalam ruangan, di mana orang tersebut tidak diberi hak akses. Seiring dengan itu juga, sistem akan menginformasikan melalui tampilan LCD bahwa *web server* yang diinputkan tidak sesuai dan segera mereset sistem dengan menekan tombol * pada *keypad*. Walaupun sistem telah direset, tetapi informasi penolakan sistem terhadap *web server* yang salah telah diterima oleh pemilik ruangan, sehingga pemilik ruangan dapat mengunci sistem akses masuk ruang pribadinya secara jarak jauh melalui perangkat *smartphone* yang terkoneksi dengan *web server*. Gambar 9 memperlihatkan hasil pengujian saat penginputan *password* salah. Dan Gambar 10 memperlihatkan notifikasi yang terkirim ke *e-mail* dan notifikasi dari aplikasi *web server*.

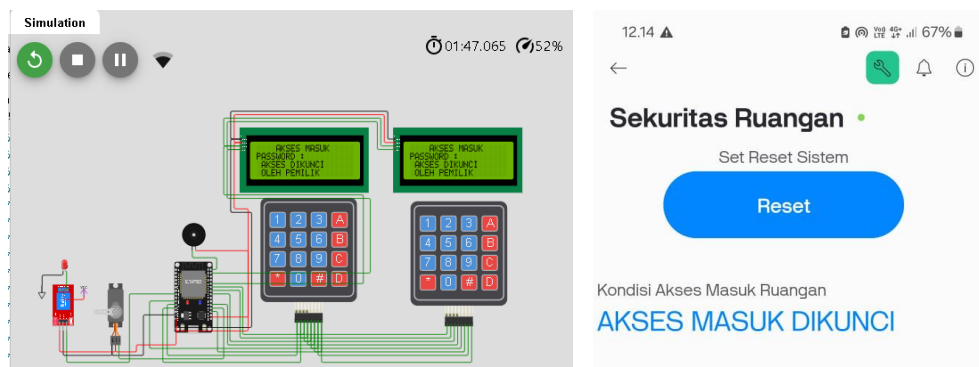


Gambar 9. Hasil pengujian saat penginputan *password* salah



Gambar 10 Hasil pengujian pengiriman notifikasi ke *e-mail* dan notifikasi dari aplikasi *web server*.

Dari hasil pengujian yang dilakukan terhadap model sistem akses masuk ruangan pribadi, seperti yang diperlihatkan pada Gambar baik pada Gambar 9 dan Gambar 10, terlihat bahwa saat sistem mendeteksi bahwa *password* yang diinputkan tidak sesuai, maka pemilik ruangan dapat mengetahuinya melalui penerimaan notifikasi, di mana penerimaan notifikasi melalui *e-mail* si pemilik ruangan dan notifikasi dari *web server* ke perangkat *smart phone* dari si pemilik ruangan. Saat kondisi ini terjadi, pemilik ruangan dapat melakukan penguncian terhadap sistem akses masuk ruangan pribadinya secara jarak jauh, tanpa harus ke lokasi/ke ruang pribadinya melalui perangkat *smart phone* yang terkoneksi dengan aplikasi *web server*. Adapun hal yang dapat dilakukan pemilik ruangan adalah mengaktifkan tombol reset yang berada pada bagian *dashboard* dari aplikasi *web server*. Saat tombol reset diaktifkan, maka *web server* akan mengirimkan data ke kontroler melalui jaringan internet dan kontroler akan merespon data tersebut dengan cara mengunci sistem akses masuk ruangan pribadi, sehingga tidak dapat dioperasikan, menunggu pemilik ruangan mengaktifkannya kembali. Gambar 11 memperlihatkan proses penguncian sistem akses masuk ruangan pribadi jarak jauh, melalui aplikasi *web server* yang terinstal di perangkat *smart phone* dari pemilik ruangan.



Gambar 11 Pengujian proses penguncian sistem akses masuk ruangan pribadi jarak jauh, melalui perangkat *smart phone* dari pemilik ruangan.

5. KESIMPULAN

Berdasarkan hasil pengujian yang dilakukan terhadap model sistem akses masuk ruang pribadi melalui inputan *password* dari *keypad* dengan notifikasi *e-mail* berbasis IoT, dapat beroperasi sesuai dengan fungsinya dan dapat diimplementasikan pada sistem yang sebenarnya, guna mengamankan ruang pribadi terhadap orang-orang yang tidak diberikan hak akses masuk. Adapun hasil yang didapat melalui pengujian model sistem ini adalah jika orang yang menginputkan *password* sesuai, maka pintu akan terbuka dan sistem kelistrikan dalam ruangan akan aktif dan jika orang yang menginputkan *password* salah karena tidak diberikan hak akses, maka secara otomatis alarm akan berbunyi dan sistem akan mengirimkan notifikasi ke pemilik ruangan melalui *e-mail* bahwa ada orang yang tidak memiliki akses masuk ruangan mencoba untuk masuk kedalam ruangan, sehingga pemilik ruangan dapat mengetahuinya dan dapat mengunci sistem akses masuk ruangnya dimanapun dia berada melalui perangkat *smartphone* yang tertanam aplikasi *web server*, sehingga ruangnya terhindar dari gangguan orang-orang yang tidak berkepentingan.

UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih kepada Politeknik Negeri Manado yang telah mendanai penelitian ini, dan kepada rekan-rekan baik peneliti dan rekan-rekan dosen yang telah berkontribusi dalam penulisan artikel ini.

DAFTAR PUSTAKA

- Ahmad Sadik Djamar, Sherwin R.U.A Sompie, M. Dwisnanto Putro, (2017), Implementasi Teknologi NFC Untuk Akses Pintu Masuk dan Keluar, E-Journal Teknik Informatika Vol. 11, No. 1, ISSN : 2301-8364
- Adzhal Arwani Mahfudh, Mochammad Ali, Ridho Fathoni, Sahrul Ramadhani, (2021), Sistem Keamanan Ruangan Berbasis Arduino Uno R3 Dengan Sensor PIR dan Fingerprint, Walisongo Journal of Information Technology, Vol. 3, No. 2, DOI: 10.21580/wjit.2021.3.2.9616 .
- H, Kristomson, Rosalia, H, Gozali, Ferrianto. (2019). Sistem Keamanan Ruangan Berbasis Internet Of Things Dengan Menggunakan Aplikasi Android. TESLA: Jurnal Teknik Elektro. 20. 127. 10.24912/tesla.v20i2.2989.
- Rajes Khana, Uus Usnul, 2018, Rancang Bangun Sistem Keamanan Rumah Berbasis Internet Of Things dengan Platform Android, Jurnal Kajian Teknik Elektro, Vol. 3, No. 1.
- Sunardi, Anton Yudhana, Muhamad Alwi Talib, (2022), Perancangan Sistem Pengenalan Wajah untuk Keamanan Ruangan Menggunakan Metode Local Binary Pattern Histogram, Jurnal Teknologi Elektro, Vol. 13. No. 02, e-ISSN: 2621-8534
- Fauzan Prasetyo Eka Putra, Selly Mellyana Dewi, Maugfiroh , Amir Hamzah, (2023), Privasi dan Keamanan Penerapan IoT Dalam Kehidupan Sehari-Hari : Tantangan dan Implikasi, Jurnal Sistem Informasi dan Teknologi, Vo. 5, No. 2, hal: 26-32, doi: 10.37034/jsisfotek.v5i1.232
- Iswahyudhi Utari Turyadi , Firman Johan, Dadang Widyanto, (2021), Analisa Dukungan Internet of Things (IoT) terhadap Peran Intelegen dalam Pengamanan Daerah Maritim Indonesia Wilayah Timur, Jurnal Teknologi dan Management Informatika, Vol. 7, No.1, Hal: 29-39.
- Moh.Misbakhul Affandi , Zaenal Abidin, (2023), Rancang Bangun Kotak Penyimpanan Dengan Akses Masuk Menggunakan Rfid Berbasis Internet Of Things (IOT), Journal of Electrical Engineering and Computer, Vol. 10, No. 10, DOI: 10.33650/jeecom.v4i2

- Kristomson H, Rosalia H Subrata, Ferrianto Gozali, (2018), Sistem Keamanan Ruang Berbasis Internet Of Things Dengan Menggunakan Aplikasi Android, T E S L A, Vol. 20, No. 2
- Wilianto, Ade Kurniawan, (2018), Sejarah, Cara Kerja Dan Manfaat Internet Of Things, Jurnal Matrix, Vol. 8, No. 2.
- Sigit Umar Anggono , Edy Siswanto, Laksamana Rajendra Haidar Azani Fajri, Munifah, (2023), User Interface Berbasis Web Pada Perangkat Internet Of Things, Jurnal Ilmu Teknik Dan Informatika, Vol. 3, No. 1.
- Abir Iftikhar Kashif Qureshi, Muhammad Shiraz , Saleh Albali, (2023), Security, trust and privacy risks, responses, and solutions for high-speed smart cities networks: A systematic literature review, Journal Computer and Information Science, Vol. 35, No. 9, <https://doi.org/10.1016/j.jksuci.2023.101788>
