KUNCI PINTU PINTAR DENGAN AUTENTIKASI DUA FAKTOR

SMART DOOR LOCK WITH TWO FACTOR AUTHENTICATION

Inez Wahyu Widhianingrum[1], Achmad Ali Muayyadi[2], Nyoman Bogi Aditya Karna[3]
[1,2,3]Program Studi Teknik Telekomunikasi, Fakultas Teknik Elektro, Universitas Telkom
[1]inezwidhia@student.telkomuniversity.ac.id, [2]alimuayyadi@telkomuniversity.ac.id, [3]aditya@telkomuniversity.ac.id

Abstrak

Maka dari itu penelitian ini bertujuan untuk membuat purwarupa kunci pintar digital yang berhubungan dengan *Two Factor Authentication* (2FA) yang bertujuan menambah keamanan dan kemudahan dalam mengendalikan kontrol pintu. Purwarupa yang dilakukan merupakan implementasi dari IoT. Pada purwarupa, keamanan pintu menggunakan *microcontroller* Arduino UNO sebagai pengendali utama yang memiliki sistem autentikasi token yang disinkronisasikan dengan Google Authenticator. Kode *One Time Password* (OTP) yang didapatkan kemudian dimasukkan ke *Keypad Matrix* 4x4. Ketika kode yang diinputkan benar, *microcontroller* akan memasukkan perintah pada *Metal Oxide Field Effect Transistor* (MOSFET) untuk menyalakan solenoid. Purwarupa yang dirancang dikategorikan sebagai implementasi IoT dengan tujuan penggunaan pada pintu rumah tanpa menggunakan kunci untuk membuka maupun menutup pintu.

Kata Kunci: *2FA (Two Factor Authentication), Google Authenticator, Arduino UNO, One Time Password (OTP), Keypad Matrix 4x4, Internet of Things (IoT).*

Abstract

Therefore, this research aims to create a prototype of a digital smart lock associated with Two Factor Authentication (2FA) which aims to increase security and convenience in controlling door control. The prototype is an implementation of IoT. In the prototype, the door lock uses an Arduino UNO microcontroller as the main controller which has a token authentication system synchronized with Google Authenticator. The One Time Password (OTP) code obtained is then inputted into the 4x4 Keypad Matrix. When the inputted code is correct, the microcontroller will then send a command to the Metal Oxide Field Effect Transistor (MOSFET) to turn on the solenoid. The designed prototype is categorized as an IoT implementation with the purpose of using it on the door of a house without using a key to open or close the door.

Keywords: *2FA (Two Factor Authentication), Google Authenticator, Arduino UNO, One Time Password (OTP), Keypad Matrix 4x4, Internet of Things (IoT)*

PENDAHULUAN

Saat ini penggunaan kunci konvensional masih banyak digunakan. Namun penggunaan kunci konvensional memiliki resiko seperti kehilangan kunci, duplikasi oleh pihak yang tidak bertanggung jawab yang menyebabkan tindakan kriminal. Oleh karena itu butuh pengembangan lebih lanjut untuk optimasi kunci pintu konvensional yaitu dengan membentuk kunci pintar secara digital. Sistem kunci pintu pintar (Smart Door Lock) merupakan sistem yang memanfaatkan Internet of Things (IoT) dalam penerapannya. Sistem ini dikhususkan pada lingkungan rumah dengan tujuan meningkatkan keamanan dan kemudahan akses pengguna.

Perkembangan teknologi telah meningkat seara pesat, maka dari itu kata sandi tidaklah cukup. Pada kasus penggunaan kata sandi, peretas hanya membutuhkan kata sandi untk bisa mengakses akun pengguna[1]. Pada penelitian sebelumnya, keamanan pintu menggunakan kode Quick Response (QR) untuk mengakses pintu. Peneliti menggunakan Bluetooth HC 05 untuk menyambungkan aplikasi barcode scanner pada android dengan Arsuino sebagai microcontroller. Perangkat diuji pada aplikasi Jelly Bean Android[2]. Penelitian lainnya, servo digunakan untuk sistem keamanan pintu menggunakan One Time Password (OTP) dan keypad Matrix 4x4 untuk akses pengguna. Saat kode OTP dimasukkan ke keypad benar, pintu akan otomatis terbuka dan akan terkunci lagi setelah 60 detik[3]. Penelitian selanjutnya, buzzer dikeluarkan untuk mengeluarkan bunyi saat kata sandi yang dimasukkan salah. Processor dan microcontroller yang membutuhkan Global Sistem for Mobile (GSM Module) untuk jaringan komunikasi anatar processor[4].

Oleh karena itu, pada penelitian ini penulis membuat kunci pintu pintar dengan menggunakan Arduino UNO sebagai microcontroller utama dengan tujuan kontrol pintu tersambung dengan jaringan internet melalui Wireless Fidelity (WI-Fi) untuk memudahakan pengguna. Sistem keamanan pada kunci menggunakan aplikasi otentikasi Two

Fator Authentiation (2FA) yaitu Google Authentiator. Google Authenticator berfungsi untuk memberikan kode OTP kepada pengguna untuk mengakses pintu. Kelebihan dari sistem keamanan ini, pengguna tetap dapat menerima kode tanpa koneksi internet.

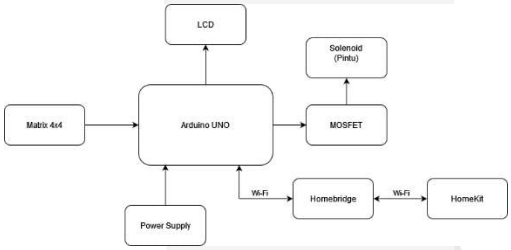
Tujuan dan Manfaat

Tugas akhir ini bertujuan untuk meranang serta merealisasikan kunci pintu pintar. Beberapa manfaat yang diperoleh dalam perancakan dan implementasi kunci pntu pintar ini adalah:

1.Mengembangkan penelitian sebelumnya tentang sistem kunci pintu pintar.
2.Merancang purwarupa kunci pintu dengan menggunakan autentikasi 2FA.
3.Membuat purwarupa kunci pintu.
4.Menganalisis hasil perancangan purwarupa kunci pintu.

MODEL SISTEM DAN PERANCANGAN

Komponen dari kunci pintu pintar dengan 2FA adalah Matrix Keypad 4x4, Arduino UNO, LCD, Solenoid, Power Supply, MOSFET, Wi-Fi, dan Homebridge sebagai penghubung Aplikasi HomeKit dengan Arduino UNO. Gambar dibawah merupakan diagram blok dari rancangan kunci pintu pintar dengan 2FA.



Gambar 1. Diagram Blok Sistem Kunci Pintu Pintar dengan Two Factor Authentication

Mikrokontroller Arduino mendapatkan sumber daya sebesar 5V dari power supply. Keypad Matrix 4x4 digunakan untuk memasukkan kode PIN yang telah diatur oleh pengguna dan kode OTP yang didapatkan dari aplikasi Google Authenticator. Arduino akan melakukan pengekan kode PIN yang dimasukkan benar atau salah. Pengeekan ini melalui . Kemudian Arduino yang terhubung dengan Internet melalui sinyal Wi-Fi akan mengecek benar atau salah kode OTP yang dimasukkan, kemudian status kode OTP akan terlihat pada layar LCD. Jika kode yang dimasukkan benar, maka MOSFET akan aktif dan solenoid akan bergerak masuk dan pintu terbuka. Apabila kode OTP salah, MOSFET tidak akan aktif dan solenoid tidak akan bergerak.

Keypad Matrix 4x4 digunakan untuk memasukkan kode PIN yang telah diatur sebelumnya dan kode OTP yang didapat dari Google Authenticator. Juga sebagai pengatur Arduino UNO untuk memilih jaringan Wi-Fi yang sudah diatur sebelumnya, dan juga untuk mengatur ulang kode PIN.

Gambar 2. Keypad Matrix 4x4

Pada Gambar 2, tombol 0-9 digunakan sebagai input kode PIN dan kode OTP oleh pengguna. Tombol A digunakan untuk mengganti koneksi Wi-Fi ke perangkat Wi-Fi yang sudah diatur sebagai perangkat Wi-Fi utama, sedangkan tombol B digunakan untuk mengganti koneksi Wi-Fi ke perangkat Wi-Fi cadangan. Tombol C digunakan untuk merubah kode PIN pada perangkat Arduino UNO, dan tombol D digunakan untuk menghapus inputan kode PIN maupun kode OTP terakhir bila terjadi kesalahan dalam pengetikan kode PIN maupun kode OTP. Tombol bintang (*) dan tanda pagar (#) tidak digunakan.

Gambar 3. Menu awal saat tidak ada koneksi internet

Pada Gambar 3 menampilkan menu awal ketika tidak ada koneksi internet atau ketika tidak ada jaringan Wi-Fi yang tersedia. Ketiadaan konektivitas Wi-Fi ditandai oleh huruf N pada pojok kanan atas layar yang berarti Not Connected. Sebaliknya, ketika perangkat tersambung ke Wi-Fi dan memiliki koneksi internet, maka huruf yang ditampilkan adalah C yang berarti Connected. Gambar 4 memperlihatkan menu awal ketika ada koneksi internet.

Gambar 4. Menu awal ketika tidak ada koneksi internet

Alur Jaringan

Secara teknis, Arduino UNO tidak dapat terhubung langsung dengan aplikasi HomeKit. Karena hal ini, Homebridge diperlukan sebagai penerjemah protokol yang digunakan oleh HomeKit yaitu HomeKit Acessory Protocol (HAP) melalui Multicast Domain Name System (mDNS) ke protokol yang lebih umum seperti Hyper Text Transfer Protocol (HTTP) dengan bantuan plugin Homebridge-Http.

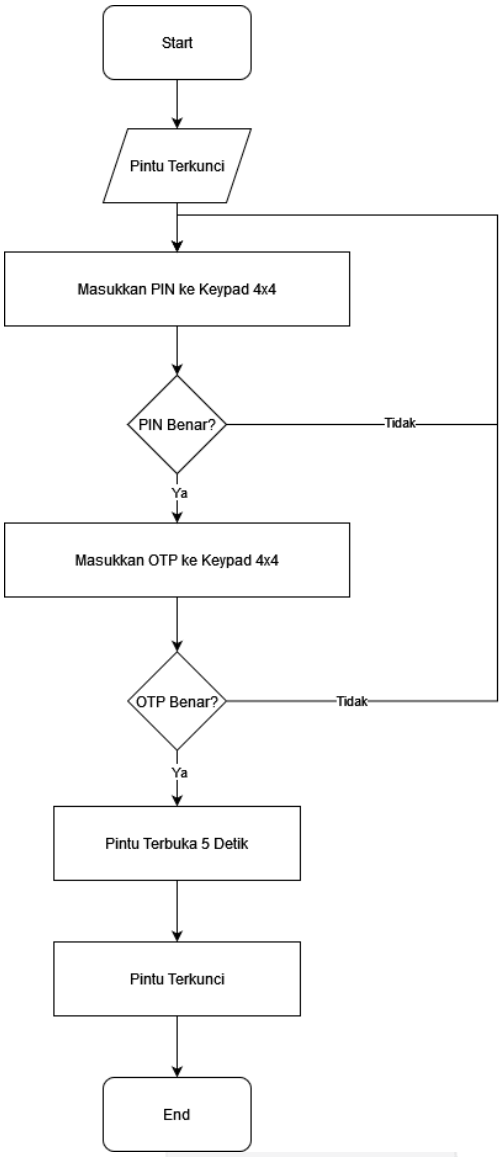
Bonjour HAP adalah salah satu protokol yang mengiklankan perangkat pada sebuah jaringan agar terdeteksi oleh setiap perangkat pada jaringan tersebut. Konektivitas antara Homebridge dan HomeKit dilakukan melalui Bonjour HAP. Disisi lain, Arduino UNO telah diatur agar menjadi peladen dan siap menerima request HTTP. Tugas Homebridge disini adalah ketika aplikasi tersebut menerima paket protokol HAP dari HomeKit, aplikasi Homebridge akan memanggil url yang sudah diatur pada aplikasi Homebridge. Saat url ini dipanggil, fungsi yang bersangkutan akan aktif.

Gambar 5 memperlihatkan parameter untuk menyalakan perangkat dengan nama on_url membutuhkan url http://192.168.0.104/on untuk dipanggil, sedangkat untuk mematikan perangkat digunakan parameter dengan nama off_url yang membutuhkan url http://192.168.0.104/off untuk dipanggil.

Gambar 5. Tangkapan layar konfigurasi Homebridge

Flowchart

Berikut adalah gambar flowchart cara kerja dari prototipe kunci pintu pintar:



Gambar 6. Flowchart Kunci Pintu Pintar dengan Two Factor Authentication

Pengguna memasukkan kode PIN yang telah dibuat sebelumnya pada keypad matrix 4x4. Saat PIN yang dimasukkan benar, akan muncul kata 'Correct' pada layar LCD dan beralih ke tampilan 'Input OTP'. Kemudian pengguna membuka aplikasi Google Authenticator untuk mendapatkan kode OTP yang terdiri dari 6 digit berupa angka. Setelah itu pengguna memasukkna kode OTP ke keypad matrix 4x4. Status benar atau salah kode OTP dimunculkan pada layer LCD. Jika kode OTP yang dimasukkan benar, solenoid pada pintu akan terbuka selama 5 detik, sedangkan apabila OTP yang dimasukkan salah maka pintu akan tetap terkunci dan kemabali ke tampilan awal yaitu 'Input PIN'.

PENGUJIAN DAN ANALISIS

Sistem dirancang agar dapat membuka pintu saat kondisi PIN dan kode OTP benar. Pengujian dilakukan dengan scenario inputan:

-PIN kata sandi benar, kode OTP benar sebanyak 10 kali.

-PIN kata sandi benar, kode OTP salah sebanyak 10 kali.

-PIN kata sandi salah, kode OTP benar sebanyak 10 kali.

-PIN kata sandi salah, kode OTP salah sebanyak 10 kali.

Tabel 1. Kondisi ketika PIN dan OTP benar

PIN	OTP	Kondisi
Benar	Benar	Pintu Terbuka
Benar	Benar	Pintu Terbuka
Benar	Benar	Pintu Terbuka
Benar	Benar	Pintu Terbuka
Benar	Benar	Pintu Terbuka
Benar	Benar	Pintu Terbuka
Benar	Benar	Pintu Terbuka
Benar	Benar	Pintu Terbuka
Benar	Benar	Pintu Terbuka
Benar	Benar	Pintu Terbuka

Berdasarkan Tabel 1 percobaan pengujian dengan input PIN benar dan OTP benar didapatkan hasil 100% berhasil, dimana kunci pintu dapat terbuka tanpa ada kendala pada sistem.

Tabel 2. Kondisi Ketika PIN benar dan OTP salah

PIN	OTP	Kondisi
Benar	Salah	Pintu Tertutup
Benar	Salah	Pintu Tertutup
Benar	Salah	Pintu Tertutup
Benar	Salah	Pintu Tertutup
Benar	Salah	Pintu Tertutup
Benar	Salah	Pintu Tertutup
Benar	Salah	Pintu Tertutup
Benar	Salah	Pintu Tertutup
Benar	Salah	Pintu Tertutup

Benar	Salah	Pintu Tertutup

Berdasarkan Tabel 2 percobaan pengujian dengan input PIN benar dan OTP salah didapatkan hasil 100% gagal, dimana kunci pintu tidak terbuka tanpa ada kendala pada sistem.

Pada kondisi PIN salah dan OTP benar maupun PIN salah dan OTP salah, tidak akan bisa terjadi karena ketika PIN salah pengguna tidak diperbolehkan memasukkan OTP dan dikembalikan ke tampilan masukkan PIN.

Pengujian Throughput

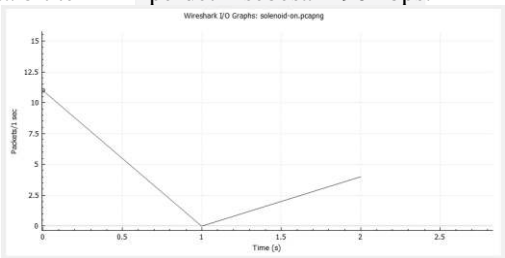
Pengujian Throughput dilakukan menggunakan aplikasi Wireshark, hasil dari Throughput diperoleh dari pengiriman paket melalui Homebridge ke Arduino UNO. Pengujian Throughput ini bertujuan untuk melihat waktu respon sistem dari pertama perintah buka atau tutup kunci dikirim sampai arduino benar-benar membuka atau menutup solenoid.

Statistics

Measurement	Captured
Packets	15
Time span, s	2.566
Average pps	5.8
Average packet size, B	63
Bytes	950
Average bytes/s	370
Average bits/s	2961

Gambar 7. Statistik Wireshark saat capture paket untuk menyalakan solenoid

Pada Gambar 7, statistik pada Wireshark menunjukan bahwa komunikasi antara Homebridge dengan Arduino UNO memakan waktu sebanyak 2,56 detik dengan jumlah 15 paket terkirim, dan rata rata bit terkirim perdetik sebesar 2961 bps.



Gambar 8. Grafik *input* dan *output* wireshark saat *capture* paket untuk menyalakan solenoid

Pada Gambar 8, Grafik input dan output menunjukkan berapa kecepatan paket terkirim tiap detiknya. Dimulai dengan 11 paket perdetik di detik ke nol, turun menjadi 0 paket perdetik di detik ke satu dan naik lagi menjadi 4 paket perdetik di detik kedua.

Throughput delay yang didapatkan dari pengambilan data dari wireshark adalah:

$$Throughput\ Delay = \frac{\text{Jumlah bit}}{\text{Waktu Delay}}$$

$$Throughput\ Delay = \frac{7600\ bit}{2{,}56\ s} \cong 2968\ bps$$

Pada purwarupa yang diuji dalam penulisan tugas akhir ini, penulis menggunakan sumber daya yang berasal dari powerbank dengan keluaran sebesar 5 V. Jumlah daya yang digunakan oleh penulis adalah sebesar 10.000 mAh. Kapasitas powerbank atau jumlah daya powerbank yaitu :

$$\text{Jumlah Daya} = \text{Tegangan X Arus}$$

$$\text{Jumlah Daya} = 5 \text{ X } 10.000$$

$$Jumlah\ Daya = 50.000\ mili\ watt\ hour$$

Pengukuran ini dilakukan menggunakan multimeter sebagai alat untuk mengukur daya arus listrik.

Tabel 3. Pengukuran Daya Saat Kondisi Solenoid Terbuka dan Tertutup

No.	Komponen	Solenoid Tertutup		Solenoid Terbuka	
		Arus	Tegangan	Arus	Tegangan
1.	LCD	28 mA	4,53 V	28 mA	4,85 V
2.	Powerbank	0 mA	5.011 V	905 mA	4,8 V
3.	MOSFET	0 mA	0 V	950 mA	4.4 V
4.	Keypad	0 mA	0,01 V	0 mA	0.01 V
5.	Arduino UNO	129 mA	4,965 V	129 mA	4,965 V

Purwarupa rupa yang dibuat mempunyai batasan maksimum durasi alat tetap bekerja. Maksimum durasi pada purwarupa menggunakan sumber daya powerbank ini yaitu :

$$\text{Durasi Maksimal} = \frac{\text{Kapasitas } Powerbank}{\text{Total Konsumsi Daya}}$$

$$= \frac{\text{Kapasitas } Powerbank}{\text{Daya mosfet} + \text{Daya Arduino} + \text{Daya LCD}}$$

$$= \frac{50000\ mWh}{4{,}18\ W + 0{,}64\ W + 0{,}18\ W}$$

$$= \frac{50\ Wh}{\cong 5{,}00\ W} \cong 10\ Hours$$

Melalui perhitungan diatas dapat disimpulkan bahwa durasi maksimal purwarupa tetap aktif adalah kurang lebih 10 Jam jika daya power supply yang digunakan terisi penuh.

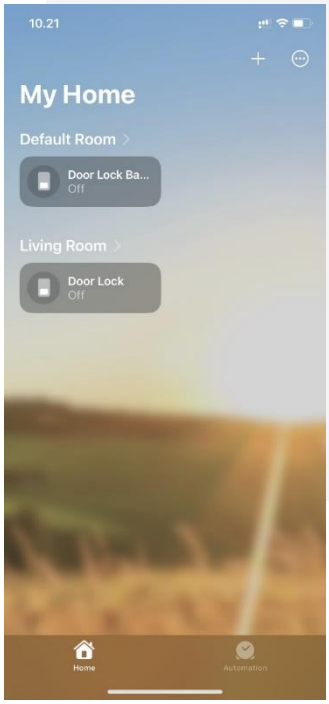
Hasil Perancangan

Hasil perancangan desain sistem perangkat keras didapatkan realisasi seperti pada gambar 9.

Gambar 9. Realisasi Desain Perangkat Keras

Implementasi Antarmuka Aplikasi

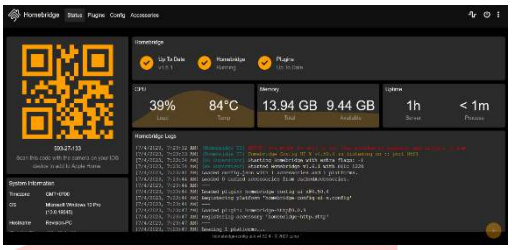
Antarmuka aplikasi adalah media interaksi antara pengguna dengan aplikasi, yang mana pengguna dapat melihat tampilan keadaan pintu dari aplikasi Home Kit.



Gambar 10. Tampilan menu awal HomeKit

Server yang digunakan pada prorotype kunci pintu pintar dengan 2FA ini yaitu server Homebridge.

Berikut tampilan server Home Bridge ketika terkoneksi dengan Wi-Fi dan Arduino.



Gambar 11. Server Homebridge

Struktur Kode

Berikut adalah struktur kode pada Arduino UNO.

No.	Method	Deskripsi Metode
1	initCon()	Mengkoneksikan Wi-Fi apabila Wi-Fi utama dan Wi-Fi cadangan sedang down.
2	printConnection()	Menampilkan status koneksi pada layar LCD. Status C apabila terkoneksi, status N apabila tidak terkoneksi.
3	verifyOTP()	Memverifikasi kode OTP dan mengirimkan sinyal untuk membuka solenoid
4	verifyPassword()	Memverifikasi kata sandi
5	clearData()	Membersihkan input PIN atau OTP
6	updateTime()	Memperbarui setiap waktu jam berubah, di samakan dengan aplikasi jam perangkat lunak softwareRTC ke NTP
7	writeStringToEEPROM()	Menyimpan *value* string ke memori bawaan Arduino
8	readStringFromEEPROM()	Membaca *value* string dari memori bawaan Arduino
9	changePassword()	Masuk ke mode penggantian kode PIN untuk mengganti kode PIN dan menyipan kode PIN baru

Pengukuran Jangkauan Wi-Fi

Dalam pengukuran jangkauan Wi-Fi penulis melakukan uji coba untuk mengukur berapa jarak lingkup Wi-Fi back up dari Handphone (HP) pengguna ke Arduino UNO. Berikut hasil pengukuran jangkauan Wi-Fi ke sumbernya.

Tabel 4. Tabel Pengukuran Jangkauan Wi-Fi

No	Jarak (Meter)	Kondisi	
		Tersambung	Tidak Tersambung
1	0	✓	
2	1	✓	
3	5	✓	
4	10	✓	
5	15	✓	
6	20		✓
7	25		✓
8	30		✓

Hasil pengukuran pada Tabel 4 adalah jangkauan koneksi antara sumber Wi-Fi dengan perangkat purwarupa tetap tersambung adalah sebesar maksimal kurang lebih 15 meter. Lebih dari 15 meter

didapatkan hasil koneksi antara sumber Wi-Fi dan purwarupa tidak terambung.

PENUTUP

Kesimpulan

Pada pengujian dan pembahasan yang telah dilakukan oleh penulis tentang sitem kunci pintu pintar dengan autentikasi dua faktor, dapat diambil kesimpulan sebagai berikut:

1.OTP yang dihasilkan dari Google Authenticator teruji sejalan dengan RTC pada penulisan kode di Arduino Uno. OTP yang dihasilkan oleh Google Authenticator akan berubah setiap 30 detik.

2. Solenoid terbuka selama 5 detik setelah kode PIN dan OTP dimasukkan dalam kondisi benar.

3. Jumlah daya yang dibutuhkan untuk menjalankan purwarupa kunci pintu pintar yaitu sebesar 50.000 mWh. Throughput yang dihasilkan pada pengukuran purwarupa kunci pintu pintar adalah sebesar 1.551 bps

4. Tingkat keberhasilan kunci pintu pintar saat membuka dan menutup dalam kondisi kode PIN yang dimasukkan benar dan kode OTP benar adalah 100%. Cakupan Wi-Fi tersambung pada penelitian adalah maksimal 15 meter.

Saran

Saran penulis untuk pengembangan kunci pintu pintar dengan autentikasi dua faktor ini adalah:

1. Solenoid dan sumber daya disarankan menggunakan daya 12V karena solenoid 5V tidak ada mekanisme kunci bawaan.

2. Menggunakan RTC fisik karena memiliki cadangan baterai.

DAFTAR PUSTAKA

[1] Beritateknologi.id. Google Authenticator, Apa Artinya?. Diakses pada 3 Juni 2021, dari link https://beritateknologi.id/google-authenticator-apa-artinya/

[2] Hazarah, Atikah. (2017). Rancang Bangun Smart Door Lock Menggunakan QR Code dan Solenoid. Jurnal Teknologi Informatika dan Terapan, 4(1), 5-9.

[3] Z, E. Orzi, Nduanya U. I., dan Oleka C. V. (2019). Microcontroller Based Digital Door Lock Security System Using Keypad. International Journal of Latest Technology in Enginering, Management and Applied Science (IJLTEMAS), 8(1), 92-97.

[4] Prabhakar, A. Y. dkk. (2019). Password Based Door Lock System. International Research Journal of Engineering and Technology (IRJET), 6(2), 1154-1157

[5] Statista.com. (2020, 13 Agustus). Number of Internet Users in Indonesia 2023. Diakses pada 28 Maret 2021, dari link https://www.statista.com/statistics/254456/number-of-internet-users-in-indonesia/

[6] Kominfo.go.id. (2019, 19 Juni). Kebutuhan Solusi IoT Tinggi, Peluang Bagi Makers Lokal. Diakses pada 28 Maret 2021, dari link https://kominfo.go.id/content/detail/19375/kebutuhan-solusi-iot-tinggi-peluang-bagi-makers-%20lokal/0/berita_satker

[7] Authy.com. What is 2FA. Diakses pada 28 Maret 2021, dari link https://authy.com/what-is-2fa/

[8] Searchsecurity.techtarger.com. Two Factor Authentication. Diakses pada 28 Maret 2021 pada link https://searchsecurity.techtarget.com/definition/two-factor- authentication

[9] Learning.me. Pengertian Arduino UNO. Diakses pada 28 Maret 2021 pada link https://ilearning.me/sample-page-162/arduino/pengertian-arduino-uno/

[10] Elektronika-dasar.web.id. (2021, 10 Februari). Matrix Keypad 4x4 Untuk Mikrokontroler. Diakses pada 28 Maret 2021 pada link https://ilearning.me/sample-page-162/arduino/pengertian-arduino-uno/

[11] Mikroavr.com. (2018, 14 Mei). Pengertian MOSFET, Cara Kerja dan Manfaatnya. Diakses pada 14 Juli 2023 pada link https://mikroavr.com/pengertian-mosfet-dan-manfaat-nya/

[12] Homebridge.io. Bringing HomeKit support where there is none. Diakses pada 14 Juli 2023 pada link https://homebridge.io/

[13] Apple.com. The foundation for smarter home. Diakses pada 14 Juli 2023 pada link https://www.apple.com/home-app/

[14] Kho, Dickson. Pengertian LCD (Liquid Crystal Display) dan Prinsip Kerja LCD. Diakses pada 18 Juli 2023 pada link https://teknikelektronika.com/pengertian-lcd-liquid-crystal-display-prinsip-kerja-lcd/

[15] SAHRETECH. Pengertian Two Factor Authentication, Jenis dan Alasan Menggunakannya. Diakses pada 18 Juli 2023 pada link https://www.sahretech.com/2022/01/pengertian-two-factor-authentication.html

[16] Erintafifah. (2021, 08 Oktober). Mengenal Perangkat Lunak Arduino IDE. Diakses pada 18 Juli 2023 pada link https://www.kmtech.id/post/mengenal-perangkat-lunak-arduino-ide

[17] CompTIA. What is Wireshark and How Is It Used?. Diakses pada 31 Juli 2023 pada link https://www.comptia.org/content/articles/what-is-wireshark-and-how-to-use-it