



Embedded System

SISTEM KEAMANAN PINTU DENGAN FITUR REMOTE KEYLESS MENGGUNAKAN METODE PENDEKATAN PUF

Muhamad Noveri Ramadhan ¹, Dodon Yendri ^{*2}

^{1,2}Departemen Teknik Komputer, FTI Universitas Andalas Limau Manis Kec. Pauh, Kota Padang, Sumatera Barat 25163 Indonesia

ARTICLE INFORMATION

Received: August 1, 2025 Revised:
September 14, 2025
Available online: October 31, 2025

KEYWORDS

Smart door lock, remote keyless, PUF, bluetooth, ESP32

CORRESPONDENCE

E-mail: dodon@it.unand.ac.id

A B S T R A C T

Modern home security systems are increasingly important for providing peace of mind, especially when occupants frequently leave their homes. As a primary access point, doors are crucial for maintaining security. Smart door locks offer enhanced security features compared to traditional mechanical locks. However, technologies relying on smartphones or PINs have vulnerabilities to attacks such as brute force and various digital security threats. Additionally, human memory limitations pose challenges in maintaining security. This study develops a door security system with remote keyless features using a Physical Unclonable Function (PUF) approach and Bluetooth connectivity. The system utilizes RSSI values to provide remote reminders, ensuring automatic locking at certain distances. Test results show that this system effectively provides unique security and convenience for users. The use of servo motors ensures precision in locking, while the ESP32 is used for communication and generating unique PUF values, making the system more secure and resistant to duplication.

PENDAHULUAN

Sudah banyak teknologi yang dapat menunjang keamanan rumah agar penghuni pun dengan nyaman tinggal didalamnya ataupun meninggalkan tempat tinggal nya agar dapat beraktivitas dengan tenang diluar rumah. Menurut studi [1] 7 dari 10 orang sering meninggalkan rumahnya setiap hari, setidaknya sejauh 1.6 km dari rumahnya. Sangat diperlukan pengamanan agar seseorang memiliki rasa tenang, nyaman, serta yakin dengan rumah yang ditinggalkannya agar dalam kondisi aman.

Pintu menjadi salah satu akses dan fitur utama untuk mempertahankan keamanan rumah secara fisik [2], jika pertahanan utama pada rumah memiliki keamanan yang lemah akan sangat mudah disusupi dan diakses. Kebanyakan kunci pintu masih berupa kunci fisik dengan sistem mekanik dengan banyak kelemahan [3], kemudian berkembang dengan memanfaatkan teknologi agar memberikan keamanan pada rumah melalui pintu yang efektif efisien, serta kenyamanan penghuni ketika meninggalkan rumah. Teknologi pintu yang memiliki fitur yang

memudahkan pengguna dan memberikan keamanan lebih, umumnya disebut dengan *smart door lock* [4].

Namun saat ini kebanyakan teknologi ini sudah banyak yang bergantung dengan *smartphone* ataupun menggunakan pin, yang memiliki kelemahan. Keamanan menggunakan pin memiliki kelemahan serta kerentanannya saat peretasan dengan memasukkan pin secara acak dan teratur dengan kombinasi pin yang ditebak atau disebut *brute force*. Dibutuhkan waktu 20 detik untuk melakukan *brute force* pada kombinasi 4 angka sehingga keamanan pin yang rentan [3]. Kemudian *smartphone* saat ini memiliki banyak ancaman keamanannya, diantara ancaman keamanan lewat *smartphone* ialah kebocoran data, *malware*, phishing, serangan *hacker*, meretas komunikasi, hingga kebiasaan pengguna itu sendiri [4]. Banyaknya ancaman keamanan *smartphone* yang bermacam tersebut akan membuat *smartphone* semakin memiliki keamanan yang sangat rentan. Selanjutnya memori manusia sendiri dapat menjadi masalah yang perlu diperhatikan.

Ketika mengerjakan banyak hal dalam waktu singkat, memori manusia akan sulit untuk mengingat semuanya. Ini terjadi karena adanya kekurangan fungsi pada bagian memori jangka pendek (*short-term memory*) [5]. Memori ini digunakan untuk kebutuhan harian, yang memiliki penyimpanan sedikit dan digunakan untuk mengingat dalam jangka waktu yang relatif singkat yaitu $\pm 15-30$ detik [5] [6]. *Short-term memory* akan sangat mudah untuk terganggu, setiap informasi baru yang masuk ke memori ini akan dengan mudah untuk menggantikan informasi lama yang sudah ada. Informasi yang tersimpan pada memori ini akan sangat rentan untuk hilang atau terlupakan, karena pada memori ini semakin banyak informasi yang disimpan akan sangat sulit untuk di ingat kembali (*recall*) [7]. Maka dari itu, diperlukan sebuah pengingat (*reminder*) untuk meminimalisir informasi yang hilang pada memori ini, serta mempermudah mengingat kembali [8]. Banyak teknologi yang dapat mengadaptasi sistem pengingat untuk menjadi salah satu fitur nya seperti pada [9] yang menggunakan PDA (*Personal Digital Assistant*) dengan RFID didalamnya sebagai sistem pengingat pada *smart home* yang akan membantu pengguna untuk menampilkan daftar pekerjaan yang akan dikerjakan ketika meninggalkan rumah.

Saat ini kunci berbentuk *remote* sudah mulai banyak dipakai walaupun baru diterapkan pada produk transportasi, seperti pada kunci mobil hingga sepeda motor pun saat ini sudah menerapkan teknologi ini. Dengan menggunakan teknologi kendali *remote* ini dapat menggantikan kunci fisik dengan sistem mekanik, menjadi kunci fisik *remote* dengan kendali dan pemantauan jarak jauh.

Pada penelitian [10], dibuat sistem pengaman pintu dengan memiliki fitur *system alert* yang menggunakan kartu tag RFID sebagai autentikasi pengamanan pintu. Kemudian pada penelitian [11] dengan keamanan menggunakan *Bluetooth Low Energy* (BLE) untuk sistem kunci pintar dengan pendekatan utama PUF (*Physical Unclonable Function*). Dengan pendekatan PUF, keamanan kunci menjadi lebih aman sebab kunci tidak akan dapat digandakan (*cloning*) dengan mudah serta tidak memakan banyak biaya karena *hardware* yang diperlukan untuk pendekatan PUF sudah tersedia pada chip BLE.

Berdasarkan uraian diatas maka dirancanglah sebuah sistem untuk dapat mengamankan pintu rumah dengan sistem pengingat jarak jauh dengan menggunakan kunci *remote keyless* sebagai kunci. **“SISTEM KEAMANAN KUNCI PINTU DENGAN FITUR REMOTE KEYLESS MENGGUNAKAN METODE PENDEKATAN PUF”**. Sistem ini dirancang dengan menggunakan modul *bluetooth* untuk koneksi *peer-to-peer*, dengan pengunci tipe *deadbolt lock*. Keamanan pintu ini dapat dikunci manual dengan sistem *thumbturn* yang dapat diputar dan diaktifkan dengan menekan tombol pada kunci *remote keyless*

disekitar pintu. Sistem akan dapat mengontrol dan memberikan tanda sebagai pengingat pada kunci agar pada jarak tertentu pengguna dapat mengetahui keadaan pintu ketika ditinggalkan. RSSI (*Received Signal Strength Indication*) adalah pengukuran terhadap daya yang diterima oleh sebuah perangkat *wireless*. Pintu dapat langsung otomatis terkunci pada jarak tertentu, apabila pengguna lupa untuk mengunci pintu. Kunci akan memanfaatkan metode PUF untuk memberikan keunikan pada kunci sehingga tidak dapat digandakan.

LANDASAN TEORI

Deadbolt Lock

Deadbolt lock merupakan tipe kunci pintu yang biasanya memiliki bentuk profil silindris dan pelindung standar nya berbentuk lingkaran. Umumnya kunci dengan tipe *deadbolt* ini menggunakan *bolt* untuk dapat mengamankan pintu dalam keadaan tertutup, *bolt* pada mekanisme penguncian ini merupakan sebuah bar besi dan dapat digerakkan untuk dapat mengunci pintu. *Bolt* ini digerakkan oleh sebuah *thumb turn* atau kunci yang memiliki mekanisme penguncian yang terpisah. Mekanisme penguncian biasanya memiliki bentuk silinder dan terdapat mekanisme yang terhubung dengan sistem bautnya. Kunci bekerja dengan memperpanjang *bolt* ke wadah yang terdapat pada kusen pintu untuk dapat mengamankan dan sulit untuk dibuka secara paksa menggunakan *pick lock* atau bor. Tipe kunci ini, memiliki 3 tingkat keamanan sesuai standar [12]. Ketiga tingkatan ini secara sederhana terbagi atas tingkat 1 sampai 3. Tingkat pertama merupakan kunci dengan kualitas terbaik, sedangkan tingkat ketiga merupakan *deadbolt* yang akan memberikan keamanan yang cukup namun tidak sebaik tingkat pertama.

Remote Keyless

Sistem *remote keyless* merupakan teknologi yang umumnya berkembang pada dunia otomotif. Sistem kunci keamanan ini bekerja secara otomatis ketika pengguna masih dalam jangkauan kendaraan, yang berfungsi untuk mengontrol kendaraan dari jarak jauh. Seperti menghidupkan mesin, membuka pintu, membuka kunci setang, dan banyak lagi. Sistem ini juga digunakan pada Gedung untuk mengamankan sebuah area didalam gedung. Pada awalnya sistem ini bekerja pada frekuensi radio antara 315 MHz dan 433.92 MHz, namun seiring berkembangnya zaman pada pertengahan tahun 1990 sistem *remote keyless* ini sudah mengimplementasikan enkripsi pada setiap kunci untuk mencegah pencurian dan *spoofing*. Sebuah *chip controller* pada *receiver* akan mengubah frekuensi yang diterima setiap

pengaksesan kunci, yang biasanya fitur keamanan ini disebut dengan *rolling code*.

PUF (Physical Unclonable Function)

PUF merupakan sebuah fungsi yang memiliki input atau output, atau sebuah prosedur yang dapat dikerjakan perangkat tertentu. Input didalamnya merupakan disebut *challenge* dan sebuah keadaan fisik dari perangkatnya. Dengan input yang diberikan prosedur PUF akan menghasilkan output dengan *response*, sehingga prosedur ini akan membentuk pasangan *challenge-response*. PUF dapat memungkinkan untuk melakukan autentikasi dan menyimpan kunci rahasia tanpa perlu mengamankan EEPROM dan menggunakan perangkat keras tambahan. Ini karena konsep dari PUF yang akan memberikan kerahasiaan dari karakteristik *integrated circuit* (IC). Dengan cara kerja keamanan ini membuat implementasi PUF memiliki karakteristik utama yang penting yaitu perilaku yang tidak dapat diprediksi sehingga sistem tidak akan mungkin untuk diduplikasi. [13]

Received Signal Strength Indicator (RSSI)

RSSI merupakan indikator kekuatan sinyal yang diterima terhadap penerima sinyal pada titik tertentu. RSSI dapat dinyatakan sebagai sebuah rasio antara sinyal terima pada titik tertentu, terhadap sinyal terima dari titik referensi. Semakin tinggi RSSI yang dibaca maka kualitas sinyal semakin baik yang memberikan tanda bahwa jarak perangkat semakin dekat. RSSI rentan terhadap *noise*, *multi-path fading*, gangguan, dan faktor lain yang mengakibatkan fluktuasi besar dalam kekuatan sinyal yang diterima. Faktor tersebut akan membuat lingkungan dalam ruangan yang sulit untuk mendapatkan *line-of-sight* (LOS), RSSI dan penentuan lokasi dapat dipengaruhi oleh *multipath* dan *shadow*.

Bluetooth

Bluetooth merupakan sebuah teknologi yang memberikan fleksibilitas dalam pengembangannya. Memberikan dua opsi radio, teknologi *Bluetooth* memberikan layanan pengembang dengan *full-stack versatile* dan solusi tepat dengan tujuan untuk dapat terus mengembangkan keperluan koneksi nirkabel [14]. *Bluetooth* menggunakan gelombang radio untuk mengirimkan informasi antara dua perangkat secara langsung. Gelombang yang digunakan pada *Bluetooth* lebih lemah daripada yang digunakan pada Wi-Fi atau sinyal pada ponsel pintar. Dengan gelombang radio yang lebih lemah berarti lebih sedikit daya yang digunakan untuk menghasilkan gelombangnya, sehingga umumnya *Bluetooth* bekerja pada jarak yang kurang dari 10 meter. Namun

koneksi *Bluetooth* pada kedua perangkat yang terhubung akan terus aktif selama kedua perangkat masih pada jarak yang dapat dijangkau, tanpa menggunakan router atau perangkat yang menjembatani mereka.

Bluetooth bekerja pada 79 frekuensi radio berbeda antara 2.4 GHz. Frekuensi ini juga digunakan Wi-Fi namun *Bluetooth* menggunakan daya yang kecil sehingga sedikit berbeda dan membuat komunikasi Wi-Fi diabaikan. Ketika dua perangkat terhubung maka secara otomatis mereka akan memilih frekuensi dari 79 frekuensi yang ada, kemudian ketika sudah berhasil terhubung maka kedua perangkat ini akan terus berkomunikasi pada frekuensi tersebut. Koneksi akan terputus hanya apabila kedua perangkat terpisah diluar jarak jangkauan dan akan terhubung kembali apabila jika sudah dalam jarak jangkauan kembali. Keamanan pada *Bluetooth* dapat diaplikasikan dengan mengatur koneksi hanya diterima untuk perangkat yang sudah teridentifikasi dan terpercaya [15].

Mikrokontroler

Mikrokontroler merupakan chip mikrokomputer yang secara fisik berupa sebuah *Integrated Circuit* (IC). Biasanya digunakan pada sebuah sistem kecil, murah dan tidak membutuhkan perhitungan kompleks seperti PC. Mikrokontroler sering ditumekan pada peralatan seperti kulkas, kompor digital, *microwave*, mesin cuci, *remote control*, dsb. Didalam mikrokontroler terdapat bagian utama sebagai pemrosesan pusat nya yaitu CPU (*Central Processing Unit*), RAM (*Random Access Memory*), ROM (*Read-Only Memory*) dan port *input output*. Selain bagian-bagian tersebut terdapat beberapa perangkat keras yang dapat digunakan untuk banyak keperluan seperti untuk komunikasi serial, interupsi, pencacahan, dll. Pada beberapa mikrokontroler sudah menyediakan ADC (*Analog-to-Digital Converter*), USB controller, CAN (*Controller Area Network*) dan lain – lain.

ESP32

ESP32 merupakan perangkat keras berupa *System on Chip* [16]. Dengan sistem SoC yang memiliki biaya yang tidak banyak serta berdaya rendah dengan mode ganda Wi-Fi kemudian dilengkapi kemampuan *Bluetooth*. Mikrokontroler ini sudah dilengkapi dengan *Bluetooth* versi 4.2 dan BLE sehingga dengan versi *Bluetooth* ini sudah dapat digunakan untuk keamanan pintar (*smart security*) [17]. ESP32 menggunakan *dual core* yang berjalan di intruksi Xtensa LX16.

METODOLOGI PENELITIAN

Rancangan Umum Sistem



Gambar 1 Rancangan Umum Sistem

Rancangan umum dari penelitian ini dapat dilihat pada Gambar 1 yaitu sistem yang akan dibuat yaitu sistem kunci pada pintu dan sistem kunci dengan fitur *remote keyless*. Kedua sistem ini akan terhubung dengan koneksi *Bluetooth* dengan menggunakan ESP32. Pada sistem kunci yang ada pada pintu terdapat motor dc yang akan memutar kunci dengan sistem *deadbolt* untuk membuka dan menutup bar *deadbolt*. Untuk dapat membuka dan menutup terdapat *worm wheel & worm gear*, sehingga motor dc dapat diletakkan secara vertikal didalam kotak kunci. Sistem ini menggunakan sumber daya baterai, sehingga sumber listrik dari sistem ini dipasok dari baterai ini. Kemudian, untuk dapat menampilkan status dari sistem kunci ini digunakan LED agar pengguna mengetahui status dari kunci. Mulai dari sistem dihidupkan, koneksi dari sistem, hingga sistem telah mengunci pintu sepenuhnya.

Sistem kunci *remote keyless* terdapat tombol untuk memberikan data sinyal kepada kunci yang ada dipintu, dan dilengkapi dengan LED RGB serta Motor getar untuk pemberitahuan kepada pengguna. Sumber daya listrik pada sistem kunci ini menggunakan baterai dengan jenis Li-po karena bentuk nya yang lebih kecil.

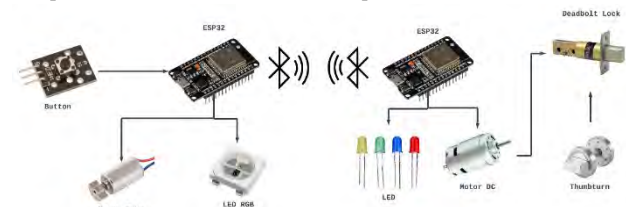
Sistem dapat bekerja secara manual dan otomatis, sistem akan otomatis mengunci apabila sistem *remote keyless* terdeteksi berjarak >6meter dari sistem kunci pintu. Motor DC akan bergerak secara otomatis ketika sistem membaca jarak sudah >6meter yang akan memutar kunci *deadbolt* untuk mengunci pintu dan memberikan informasi kepada pengguna berupa LED berwarna biru serta menggerakkan motor getar pada sistem *remote keyless*. Untuk sistem manual bekerja ketika tombol ditekan. Tombol ditekan pertama kali akan memberikan tanda bahwa sistem ingin memverifikasi informasi, kemudian akan menghidupkan LED berwarna hijau berkedip – kedip untuk menunjukkan bahwa sistem *bluetooth* sudah menyala dan kemudian menunjukkan LED jika menyala merah akan memberikan informasi bahwa sistem gagal mengautentikasi, dan jika menyala hijau tetap yang memberikan informasi bahwa

sistem sudah terautentikasi. Dengan menekan tombol sekali lagi akan menggerakkan motor DC pada sistem kunci pintu dan memberikan informasi LED menyala biru jika berhasil menutup kunci pintu.

Rancangan Proses

Rancangan Perangkat Keras

Rancangan perangkat keras menampilkan fisik dari sistem yang direpresentasikan ke dalam ilustrasi pada Gambar 2 berikut.



Gambar 2 Rancangan Perangkat Keras

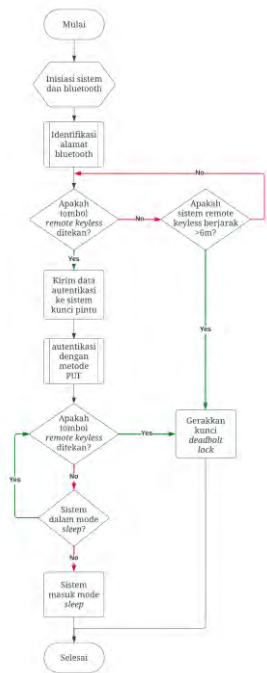
Pada Gambar 2 diatas terdapat beberapa komponen hardware yang diperlukan untuk sistem dapat bekerja yaitu:

1. Button pada sistem akan digunakan untuk *input-an* dalam sistem *remote keyless*
2. ESP32 digunakan untuk komunikasi antar sistem *remote keyless* dengan sistem kunci pintu serta untuk melakukan autentikasi kunci *remote keyless*
3. Motor Getar pada sistem ini digunakan pada sistem *remote keyless* untuk memberikan informasi berupa getaran ketika kunci pintu sudah terkunci.
4. LED RGB digunakan pada sistem *remote keyless* untuk memberikan informasi berupa warna – warna LED dengan informasi tertentu.
 - a. Warna hijau berkedip – kedip memberikan tanda bahwa sistem sedang mencoba memverifikasi sistem *remote keyless*.
 - b. Warna hijau menyala tetap memberikan tanda sistem sudah berhasil memverifikasi sistem dan sudah terautentikasi.
 - c. Warna merah memberikan tanda sistem gagal mengautentikasi sistem *remote keyless*.
 - d. Warna biru memberikan tanda bahwa sistem telah berhasil menggerakkan motor DC dan menutup kunci pintu.
5. LED digunakan pada sistem kunci pintu untuk memberikan informasi keadaan kunci pintu apakah keadaan pintu sedang dikunci atau belum dikunci.
6. Motor DC pada sistem digunakan untuk menggerakkan kunci *deadbolt* dibuka atau ditutup pada kunci pintu
7. Kunci *Deadbolt* digunakan sebagai keamanan pada pintu, tipe kunci ini digunakan karena kemanannya yang baik untuk kunci pintu serta sistem yang mudah diimplementasikan pada sistem.

8. *Thumbturn* digunakan pada sistem ini untuk menutup kunci pintu dari sisi dalam, untuk memudahkan dan memberikan keamanan pada bagian dalam.
9. Baterai pada sistem ini digunakan sebagai sumber daya energi pada sistem *remote keyless*.

Rancangan Perangkat Lunak

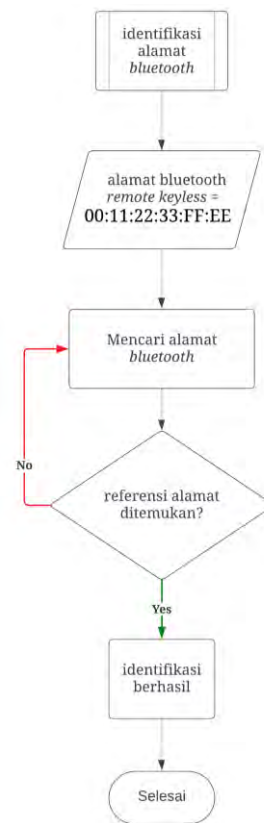
Pada perancangan perangkat lunak dijabarkan alur proses rangkaian kerja sistem secara keseluruhan yang didasarkan pada *flowchart*.



Gambar 3 Rancangan Perangkat Lunak

Rancangan Autentikasi Sistem

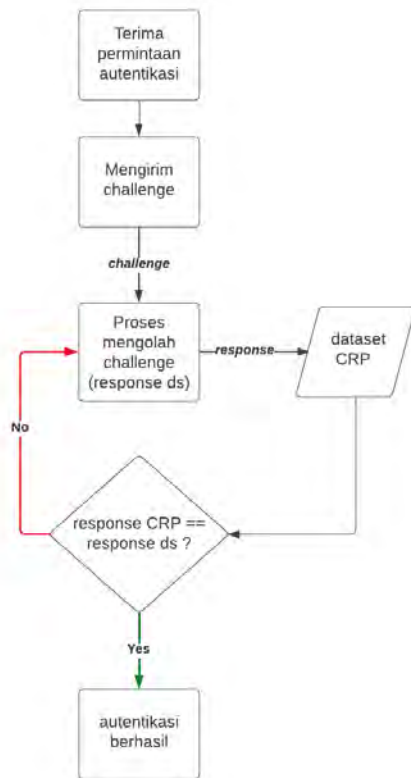
Untuk dapat memberikan keamanan pada sistem serta membuat kunci unik yang tidak dapat digandakan maka sangat diperlukan autentikasi pada sistem. Digunakan metode pendekatan PUF dengan CRP agar autentikasi dapat dilakukan dengan menggunakan *Bluetooth*. Disamping itu autentikasi pada alamat *Bluetooth* juga digunakan agar sistem hanya dapat terkoneksi pada satu alamat perangkat saja. Maka digunakan alamat MAC *Bluetooth* karena alamat ini tidak dapat digandakan ke perangkat lainnya.



Gambar 4 Flowchart Identifikasi pada Koneksi Bluetooth

Proses alur kerja sistem ini dijelaskan bagaimana autentikasi pada koneksi alamat *Bluetooth* di kedua sistem. Ketika alamat referensi pada sistem kunci pintu sama dengan alamat *Bluetooth* yang meminta untuk terhubung. Maka sistem yang meminta dalam hal ini ialah sistem *keyless remote* sudah teridentifikasi dan diizinkan untuk berkomunikasi.

Rancangan Autentikasi Sistem



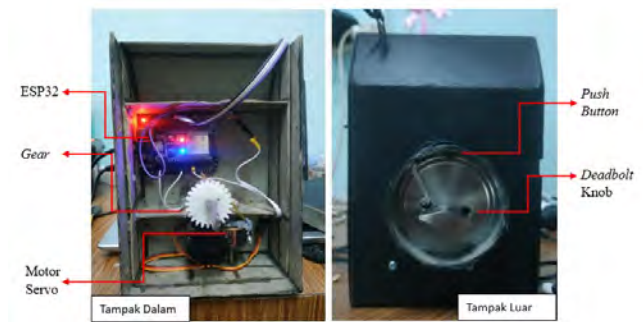
Gambar 4 Flowchart Identifikasi pada Koneksi Bluetooth

Pada gambar 4 dapat dilihat *flowchart* autentikasi sistem kunci pintu dengan pendekatan PUF, autentikasi ini menggunakan protokol pasangan *challenge – response*. Sistem *remote keyless* akan mengirimkan permintaan autentikasi dalam hal ini disebut dengan *challenge* kemudian permintaan ini akan diproses dan menghasilkan *response* yang disebut dengan *response ds*. Selanjutnya *response* yang dihasilkan akan dibandingkan dengan *response* yang ada di dataset. Jika tidak sama sistem akan mengulang sampai *challenge* sesuai dan jika sama maka sistem telah berhasil meng autentikasi.

HASIL DAN ANALISA

Implementasi perangkat keras

Terdapat beberapa komponen perangkat keras yang digunakan menghasilkan sebuah sistem yang telah dirancang sebelumnya. Berikut merupakan perangkat keras yang dirangkai dapat dilihat pada gambar di bawah ini.



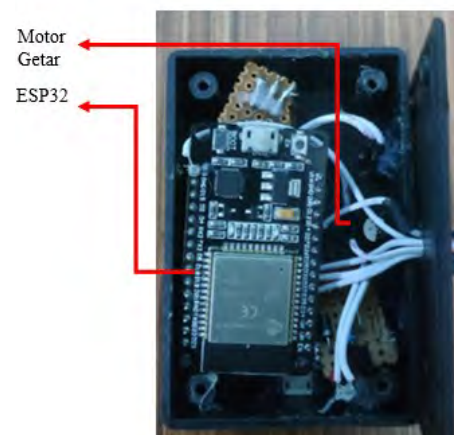
Gambar 5 Sistem Kunci Bagian Dalam Pintu

Pada gambar 5 menampilkan sistem pada kunci bagian dalam pintu. Tampak dalam sistem menampilkan bagian dalam sistem yang terdapat komponen ESP32, Motor servo yang terhubung dengan *gear* untuk menggerakkan kunci *deadbolt*. Kemudian pada tampak luar terdapat komponen *push button* dan *deadbolt knob*.



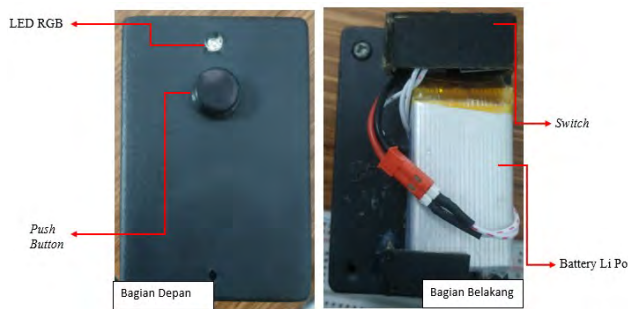
Gambar 6 Sistem Kunci Bagian Luar Pintu

Dapat dilihat pada gambar 4.2 merupakan tampilan sistem kunci pada bagian luar pintu yang akan memberikan informasi kepada pengguna kondisi pintu. LED Merah akan menyala jika pintu dalam keadaan tidak terkunci, LED Biru akan menyala ketika pintu sudah terkunci, sedangkan LED Hijau akan menyala jika sistem *remote keyless* sudah



terhubung dengan sistem kunci pintu.

Gambar 6 Sistem Remote Keyless Bagian Dalam



Gambar 7 Sistem Remote Keyless Bagian Luar

Seperti pada gambar 6 dan 7, dapat dilihat perangkat keras yang digunakan pada sistem kunci pintu untuk penelitian ini. Pada bagian dalam *remote keyless* terdapat ESP32 dan Motor Getar, serta pada bagian luar dapat dilihat komponen LED RGB, *push button*, *battery*, dan *switch*. Berikut penjelasan mengenai komponen yang digunakan pada gambar – gambar 5, 6, 7, dan 8:

- Button* pada sistem digunakan untuk masukan pada sistem *remote keyless* dan juga pada kunci pintu untuk sistem kunci manual pengganti knob.
- LED RGB digunakan pada sistem *remote keyless* untuk memberikan informasi tertentu berupa warna :
 - Hijau memberikan tanda sistem Master meminta untuk autentikasi
 - Merah memberikan tanda sistem gagal untuk autentikasi
 - Biru memberikan tanda bahwa sistem berhasil menggerakkan kunci untuk membuka dan menutup
- LED digunakan pada sistem kunci pintu untuk memberikan informasi tertentu
- ESP32 digunakan untuk komunikasi antar sistem *remote keyless* dengan sistem kunci pintu serta untuk melakukan autentikasi kunci *remote keyless*.
- Motor getar pada sistem ini digunakan pada sistem *remote keyless* untuk memberikan informasi berupa getaran ketika kunci pintu sudah terkunci
- Switch digunakan untuk mengatur aliran daya masuk *battery* ke ESP32 pada sistem *remote keyless*
- Battery Li Po* digunakan sebagai sumber daya pada sistem *remote keyless*
- Motor Servo digunakan untuk memutar kunci *deadbolt* membuka atau menutup menggunakan *gear*
- Deadbolt knob* untuk memutar kunci secara manual

Pengujian dan Analisa

Pengujian dan Analisa Perangkat Keras

A. Pengujian dan Analisis ESP32

Pengujian pada ESP32 dilakukan untuk memastikan komunikasi *bluetooth* antara sistem kunci *remote keyless* dengan kunci yang ada pada pintu berjalan dengan baik. Pengujian komunikasi ESP32 dilakukan dengan cara mendapatkan nilai RSSI untuk efektivitas komunikasi pada kedua sistem. Pengujian dengan menempatkan sistem kunci *remote keyless* beberapa meter dari sistem kunci pintu dan menganalisa nilai RSSI rata – rata yang dihasilkan pada jarak tertentu. Dengan menggunakan rumus mencari rata – rata RSSI seperti persamaan:

Tabel 1 Hasil Pengujian RSSI ESP32

Percobaan	Jarak (cm)	RSSI (dBm)	Δ RSSI	Rata – Rata RSSI
1	100 (Variabel X)	-28	0	$= \frac{-139}{5}$ $= -27.8 \approx -28$
2		-25	-3	
3		-27	2	
4		-30	3	
5		-29	-1	
1	120	-31	2	$= \frac{-160}{5}$ $= -32$
2		-34	-1	
3		-33	3	
4		-32	-1	
5		-30	-1	
6	360	-43	1	$= \frac{-220}{5}$ $= -44$
7		-44	1	
8		-45	1	
9		-43	-2	
10		-45	2	
11	570	-46	1	$= \frac{-220}{5}$ $= -47$
12		-47	1	
13		-45	-2	
14		-48	3	
15		-49	1	
16	750	-49	0	$= \frac{-220}{5}$ $= -49.8 \approx -50$
17		-50	1	
18		-49	-1	
19		-51	-2	
20		-50	-1	

Dengan menggunakan persamaan 2.1 dengan nilai A merupakan variabel X yaitu nilai RSSI rata – rata pada jarak 100 cm, kemudian n merupakan Path loss exponent, dengan mengikuti tabel 4.2 dibawah karena pengujian dilakukan pada lingkungan ruang terbuka (*Free Space*) didapatkan nilai n adalah 2. Berikut perhitungan untuk nilai RSSI pada jarak 120, 360, 590, dan 750.

Tabel 2 Path Loss Exponent

Environment	Path Loss Exponent (n)
Free Space	2
Urban Area Cellular Radio	2.7 – 3.5
Shadowed Urban Cellular Radio	3 – 5
Line-of-Sight in Building	1.6 – 1.8
Obstruction in Building	4 – 6
Obstruction in Factories	2 – 3

Berdasarkan hasil nilai RSSI yang didapat dari ESP32 dan nilai RSSI didapatkan tabel perbandingan 3.

Tabel 3 Perbandingan Hasil Pengujian

Percobaan	Jarak (Centimeter)	RSSI Perhitungan	RSSI ESP32	Selisih Nilai
1	100	-32	-28	4
2	120	-33	-32	1
3	360	-39	-44	5
4	570	-45	-47	2
5	750	-51	-50	1

Pengujian dengan ESP32 dilakukan untuk mendapatkan nilai RSSI yang sesuai dengan nilai nyata. Pengujian dilakukan dengan membandingkan nilai RSSI perhitungan dengan nilai RSSI pada alat yang dapat dilihat dari tabel 4.3. Selisih nilai digunakan untuk mengukur kesesuaian nilai RSSI ESP32 dengan RSSI Perhitungan. Maka didapatkan hasil sebagai berikut:

$$\text{Persentase Gagal} = \frac{\text{Jumlah Selisih Nilai}}{\text{Jumlah RSSI Perhitungan}} \times 100\%$$

$$\text{Persentase Gagal} = \frac{4 + 1 + 5 + 2 + 1}{32 + 33 + 39 + 46 + 51} \times 100\%$$

$$\text{Persentase Gagal} = \frac{13}{201} \times 100\%$$

$$\text{Persentase Gagal} = 6.5\%$$

$$\text{Nilai Akurat} = 100\% - \text{Persentase Gagal}$$

$$\text{Nilai Akurat} = 100\% - 6.5\%$$

$$\text{Nilai Akurat} = 93.5\%$$

Dari hasil pengujian perangkat keras ESP32 dapat diketahui bahwa semakin jauh jarak antara perangkat maka akan semakin kecil nilai RSSI yang diterima. Kemudian, berdasarkan perhitungan yang didapatkan nilai akurat sebesar 93.5% dan persentase gagal pada pengujian ini sebesar 6.5%, hal ini dapat dipengaruhi oleh kondisi lingkungan dan posisi perangkat ketika pengujian.

Pengujian dan Analisa Motor Servo

Pengujian dilakukan dengan cara mengukur sudut putaran pada motor servo agar dapat memutar kunci *deadbolt* sehingga dapat dapat mengunci secara penuh. Berdasarkan gambar 4.1 untuk dapat mengunci secara penuh panjang kunci *deadbolt* yang keluar sepanjang 2,5cm.

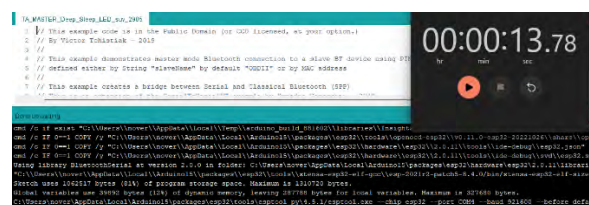
Tabel 4 Pengujian Putaran Motor terhadap Posisi Deadbolt

Percobaan	Sudut	Posisi Deadbolt (cm)
1	20°	0 cm
2	40°	0 cm
3	60°	0.3 cm
4	80°	1 cm
5	100°	2.5 cm

Berdasarkan tabel 4 untuk putaran 20 hingga 40 derajat belum cukup untuk mengeluarkan kunci *deadbolt* sedikitpun. Kemudian pada putaran hingga sudut 60 derajat hanya mengeluarkan kunci sepanjang 0,3cm begitu juga dengan putaran sudut 80 derajat yang hanya mengeluarkan kunci sepanjang 1cm. Kemudian pada putaran sudut 100 derajat kunci *deadbolt* dapat mengeluarkan kunci sepanjang 2,5cm sehingga untuk dapat mengunci sepenuhnya diperlukan putaran 100 derajat pada sistem ini.

Pengujian dan Analisa Perangkat Lunak

Pengujian dan analisis perangkat lunak dilakukan untuk mengetahui implementasi dari perangkat lunak agar berjalan dengan baik atau tidak serta mengetahui keluaran yang dihasilkan sesuai dengan tujuan yang dirancang. Pengujian dilakukan dengan melihat penggunaan *memory* yang diperlukan dan performa dari berapa lama waktu *upload* program yang telah dirancang. Perangkat lunak ini akan menguji penggunaan *memory* dan kinerja pada ESP32. Pengujian dilakukan pada kedua sistem yaitu pada kunci *remote keyless (Master)* dan pada sistem kunci pintu (*Client*).



Gambar 8 Waktu dan Penggunaan Memory pada Sistem Remote Keyless (Master)

Pada gambar 4.18 terlihat waktu yang diperlukan untuk sistem pada Master berhasil *compile* dan *upload* program kedalam ESP32 dengan total waktu yang dihasilkan 13 detik. Serta jumlah *memory* yang digunakan saat proses *compile*

terjadi dapat dilihat bahwa jumlah *sketch* maksimum yang dapat disimpan oleh ESP32 adalah 1310720 bytes, dan pada program ini menggunakan *sketch* sebesar 1062617 bytes atau 81% dari jumlah kapasitas penyimpanan memori. Program ini juga menggunakan 39892 bytes memori dinamis atau 12% dari total kapasitas maksimum yang berjumlah 327680 bytes.



Gambar 9 Waktu dan Penggunaan Memory pada Sistem Kunci Pintu

Pada gambar 4.19 terlihat waktu yang diperlukan untuk sistem pada Master berhasil *compile* dan *upload* program kedalam ESP32 dengan total waktu yang dihasilkan 14 detik. Serta jumlah *memory* yang digunakan saat proses *compile* terjadi dapat dilihat bahwa jumlah *sketch* maksimum yang dapat disimpan oleh ESP32 adalah 1310720 bytes, dan pada program ini menggunakan *sketch* sebesar 1059545 bytes atau 80% dari jumlah kapasitas penyimpanan memori. Program ini juga menggunakan 39060 bytes memori dinamis atau 11% dari total kapasitas maksimum yang berjumlah 327680 bytes.

Pengujian dan Analisa Sistem Keseluruhan

Pengujian dan Analisa Jarak Konektivitas Bluetooth

Pada pengujian ini bertujuan untuk mengetahui jarak kerja dari sistem antara *remote* dan kunci pintu. Dengan menguji sistem pada jarak yang ditentukan serta menguji penguncian otomatis sistem.

Tabel 5 Pengujian Jarak Konektivitas Bluetooth

No.	Jarak (cm)	Masukan Remote Keyless	Hasil Pengujian
1	120	Buka	Kunci pintu terbuka
2		Tutup	Kunci Pintu tertutup
3	360	Buka	Kunci pintu terbuka
4		Tutup	Kunci pintu tertutup
5	570	Buka	Kunci Pintu terbuka
6		Tutup	Kunci pintu tertutup
7	720	Buka	Kunci pintu tertutup
8		Tutup	Kunci pintu tertutup

Pada tabel 5 dapat dilihat dengan memanfaatkan nilai RSSI yang sudah ada, ketika sistem *remote keyless* berada di jarak 120, 360, dan 570 cm masih dapat memberikan masukan pada sistem kunci pintu. Namun ketika jarak 720 cm *remote keyless* tidak akan dapat mengirimkan masukan lagi karena sistem *remote keyless* sudah dalam mode *sleep* dan otomatis mengunci sistem kunci pintu.

Pengujian dan Analisa Kunci Unik dengan Pendekatan Metode PUF

Pada pengujian ini dilakukan dengan membandingkan hasil yang didapat menggunakan 2 sistem ESP32 yaitu, sistem imitasi (ESP32 B) dan sistem master yang sebenarnya (ESP32 A). Data unik didapat dengan memanfaatkan *start-up value* (suv) yang dihasilkan setiap perangkat, sehingga dapat melihat keunikan yang dimiliki. Pengujian akan dilakukan dengan melihat data unik yang dihasilkan oleh kedua ESP32 dan kemudian membandingkan data yang telah dihasilkan oleh ESP32 dengan sistem imitasi. Hasil pengujian dapat dilihat pada tabel 6 berikut.

Tabel 6 Pengujian Data Unik pada ESP32

No.	Data Lama	Data Baru			
		ESP32 A	Nilai sama	ESP32 B	Nilai sama
-	Inisiasi	184 35 194 109 210 116 60 37 163 232 116 16 212 131 216 0 254 151 173 159 98 249 193 69 205 25 131 65 13 115 34 158	-	81 217 170 166 148 175 127 182 41 87 94 168 147 147 165 126 117 218 206 93 163 247 52 115 105 234 20 126 98 19 222 95	-
1		184 35 194 194 109 210 116 60 37 163 232 116 16 212 131 216 0 254 151 173 159 98 249 193 69 205 25 131 65 13 115 34 158	28	89 217 174 167 148 174 127 180 41 87 92 168 131 147 231 254 117 218 204 93 163 251 52 115 105 202 20 126 66 19 222 95	21
2		184 42 194 77 146 118 60 161 163 168 124 16 212 130 151 173	28	81 217 174 167 148 239 127 180 41 87 94 168 147 147 231 126 117	18

No.	Data Lama	Data Baru			
		ESP32 A	Nilai sama	ESP32 B	Nilai sama
	201 0 254 151 173 159 98 249 193 69 204 25 139 65 13 115 34 158	159 98 249 193 69 204 25 131 65 9 115 34 158		218 238 93 163 243 116 115 105 234 20 126 226 19 222 95	
3	152 43 210 77 154 86 60 33 163 232 124 16 212 131 217 0 254 151 173 159 98 249 193 69 204 25 131 65 9 115 34 158	184 35 210 77 154 86 60 161 163 168 124 16 212 131 205 0 254 151 175 159 98 249 193 133 204 25 139 65 9 115 2 158	28	81 217 174 167 148 175 123 180 41 87 92 168 147 147 167 254 117 218 206 93 163 247 116 115 105 202 20 126 98 19 220 79	22
4	184 35 210 77 154 86 60 161 163 168 124 16 212 131 205 0 254 151 175 159 98 249 193 133 204 25 139 65 9 115 2 158	152 35 194 77 138 86 60 37 163 168 124 16 212 131 216 0 254 151 173 159 106 249 129 133 204 25 131 65 9 115 98 158	29	81 89 170 166 156 175 123 182 41 87 94 168 155 147 167 254 117 218 206 93 163 247 116 115 105 234 20 118 98 19 220 79	20
5	152 35 194 77 138 86 60 37 163 168 124 16 212 131 216 0 254 151 173 159 106 249 129 133 204 25 131 65 9 115 98 158	184 35 192 77 146 86 60 33 163 168 124 16 212 131 221 0 254 151 175 159 98 233 193 69 204 25 131 65 9 115 34 30	29	81 217 174 167 148 239 123 180 41 87 86 168 131 147 231 254 117 218 204 221 163 247 116 115 105 234 20 126 226 19 222 95	17
6	184 35 192 77 146 86 60 33 163 168 124 16 212 131 221 0 254 151 175 159 98 233 193 69 204 25	184 35 194 77 218 84 60 161 163 168 124 16 212 131 216 0 254 151 173 155 106 249 193 5 204 25 139 65 25 115 34 158	27	81 217 170 167 148 175 123 182 41 87 94 168 155 147 39 126 117 218 206 93 163 247 52 115 105 234 20 126 194 51 222 95	20

No.	Data Lama	Data Baru			
		ESP32 A	Nilai sama	ESP32 B	Nilai sama
	131 65 9 115 34 30				
7	184 35 194 77 218 84 60 161 163 168 124 16 212 131 216 0 254 151 173 155 106 249 193 5 204 25 139 65 25 115 34 158	152 99 194 77 218 118 60 161 163 168 124 16 212 130 217 0 254 151 175 159 106 233 193 5 204 25 131 65 9 115 34 158	30	81 89 170 167 148 191 107 180 41 87 94 168 131 147 231 126 117 218 206 93 163 251 52 115 105 194 20 126 98 19 222 79	20
8	152 99 194 77 218 118 60 161 163 168 124 16 212 130 217 0 254 151 175 159 106 233 193 5 204 25 131 65 9 115 34 158	184 35 210 109 154 118 60 165 163 168 124 16 212 131 205 0 254 151 173 159 98 249 193 133 204 25 131 65 9 115 34 30	27	89 217 174 135 148 175 123 182 41 119 94 168 131 147 247 126 117 218 206 93 163 247 52 115 105 202 20 126 98 19 220 95	23
9	184 35 210 109 154 118 60 165 163 168 124 16 212 131 205 0 254 151 173 159 98 249 193 133 204 25 131 65 9 115 34 30	184 43 210 109 154 118 60 165 163 168 124 16 212 131 221 0 254 151 45 155 98 233 193 197 204 25 139 65 25 243 34 158	29	81 217 174 167 148 239 127 180 41 119 94 168 131 147 167 254 117 219 206 93 163 247 116 243 105 202 4 126 98 19 222 95	21
10	184 43 210 109 154 118 60 165 163 168 124 16 212 131 221 0 254 151 45 155 98 233 193 197 204 25 139 65 25 243 34 158	24 35 194 109 154 86 60 161 131 168 124 16 212 131 220 0 254 151 175 155 106 233 193 69 204 25 131 65 25 115 2 30	28	81 217 174 167 149 175 123 182 41 87 94 168 131 147 231 254 117 219 206 93 163 243 116 115 105 202 20 126 226 19 220 79	21

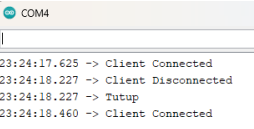
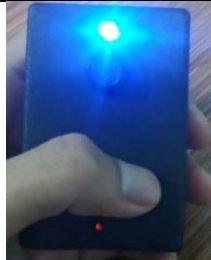
Pada tabel 6, dapat dilihat dari perbandingan 2 nilai unik yang dihasilkan oleh kedua ESP32, walaupun terlihat sama namun

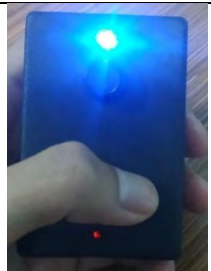
terdapat kombinasi angka yang membuat kedua ESP32 memiliki karakteristik tersendiri. Karakteristik inilah yang menjadi data unik untuk setiap ESP32 sehingga tidak dapat di gantikan oleh perangkat lain. Dari 10 percobaan yang sudah dilakukan dari 32 nilai data yang dimiliki untuk proses autentikasi, nilai sama paling sedikit adalah 27 dan nilai sama paling banyak adalah 30. Didapatkan kesimpulan bahwa nilai sama tidak akan pernah sama dengan jumlah nilai yang dimiliki.

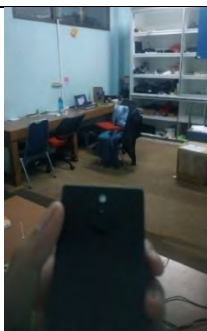
Pengujian dan Analisa Sistem Keseluruhan

Pada pengujian ini, sistem akan diuji untuk mengetahui keberhasilan kerja sistem. Sistem akan berjalan ketika sudah disambung dengan *power supply*. Jika sistem sudah saling terhubung, autentikasi akan dilakukan dan kemudian ketika sudah ter-autentikasi sistem kunci pintu dapat dikendalikan dari jarak jauh. Namun sistem kunci pintu akan otomatis terkunci apabila *remote keyless* berada >6meter. Motor getar dan LED RGB pada *remote keyless* akan menyala ketika ada respon dari kunci pintu untuk memberikan sinyal informasi kepada pengguna.

Tabel 7 Tabel Pengujian Keseluruhan

Fungsi	Proses pada Serial Monitor	Hasil Sistem
Bluetooth pada sistem remote keyless dan kunci pintu berhasil tersambung.		 
remote keyless mengirim permintaan autentikasi dan mengirim data unik pertama.	<pre>Client Connected data yg diterima : a isi recdata : a dtpuf pertama diterima: 56 35 210 77 210 84 60 Client Disconnected 60 37 163 168 125 16 212 131 221 64 254 151 : 175 159 106 233 193 1 206 25 131 65 9 115 2 22</pre>	

Fungsi	Proses pada Serial Monitor	Hasil Sistem
Sistem kunci pintu memberikan feedback.	<pre>23:33:05.519 -> Client Disconnected 23:33:05.519 -> Tutup</pre>	 
Remote keyless masuk kedalam mode sleep dan mengulang proses inialisasi bluetooth. Kemudian siap mengirim data unik kedua.		
Sistem kunci pintu mengolah data unik kedua yang diterima dan memberikan izin autentikasi remote keyless.	<pre>isi recdata : a mengirimkan "ankitgudf" dtpuf diterima: 152 35 210 77 146 118 60 37 163 168 12 dtpufstr : 152 35 210 77 146 118 60 37 163 168 124 14 dtpufstrlama : 56 35 210 77 210 84 60 37 163 168 125 1 numbers[0] : 56 numbers[0] : 152 numbers[1] : 35 numbers[1] : 35 numbers[2] : 210 numbers[2] : 210 numbers[3] : 77 numbers[3] : 77 numbers[4] : 210 numbers[4] : 146 numbers[5] : 88 numbers[5] : 118 numbers[6] : 60 numbers[6] : 60 numbers[7] : 37 numbers[7] : 37 numbers[8] : 163 numbers[8] : 163 numbers[9] : 168 numbers[9] : 168 numbers[10] : 125 numbers[10] : 124 numbers[11] : 16 numbers[11] : 16 numbers[12] : 212 numbers[12] : 212 numbers[13] : 131 numbers[13] : 130 numbers[14] : 221 numbers[14] : 216 numbers[15] : 64 numbers[15] : 0 numbers[16] : 254 numbers[16] : 254 numbers[17] : 151 numbers[17] : 151 numbers[18] : 175 numbers[18] : 175 numbers[19] : 159 numbers[19] : 159 numbers[20] : 106 numbers[20] : 98 numbers[21] : 233 numbers[21] : 233 numbers[22] : 193 numbers[22] : 193 numbers[23] : 1 numbers[23] : 149 23:33:46.939 -> results[31] : 0 23:33:46.939 -> batas : 26 23:33:47.124 -> mengirim : yes 23:33:47.124 -> dtpufstrlama: 152 35 23:33:47.124 -> dtpufstr: 152 35 210</pre>	
Tombol pada remote keyless ditekan untuk membuka	<pre>data yg diterima : b isi recdata : b Buka data yg diterima : c isi recdata : c Tutup</pre>	

Fungsi	Proses pada Serial Monitor	Hasil Sistem
dan menutup kunci <i>deadbolt</i> .		  
Tombol pada sistem kunci pintu ditekan untuk membuka dan menutup kunci pintu secara manual.	 Tutup Buka Tutup Buka	
<i>Remote keyless</i> berada pada jarak >6 meter untuk penguncian secara otomatis.	Client Disconnected Tutup timestamp	

Dapat dilihat pada tabel 7 merupakan pengujian keseluruhan yang telah dilakukan, sistem *bluetooth* akan otomatis terhubung apabila sistem kunci pintu dalam keadaan *standby* dan sistem

remote keyless hidup pada jarak <6 meter. Setelah terkoneksi untuk pertama kali setelah mati, sistem *remote keyless* akan meminta autentikasi dengan mengirimkan data unik kepada sistem kunci pintu. Sistem kunci pintu akan mengidentifikasi bahwa data unik yang dimiliki baru pertama kali, sehingga akan meminta data unik kedua kepada *remote keyless* dan sistem *remote keyless* akan masuk dalam mode *sleep*. Setelah mengulang dari keadaan mode *sleep* hingga terhubung kembali, sistem *remote keyless* akan mengirimkan data unik kedua untuk kemudian diolah pada sistem kunci pintu. Pada pengolahan data unik ini, jika terdapat >26 kombinasi angka yang sama maka sistem akan memberikan izin kepada *remote keyless* untuk membuka atau menutup kunci pintu. Sistem kunci pintu dapat dibuka dan ditutup dari bagian dalam dengan menekan tombol yang ada didekat *knob*. Sistem akan otomatis terkunci ketika sudah berada diluar jarak jangkauan yaitu pada jarak >6 meter, sistem otomatis ini memanfaatkan nilai RSSI yang ada pada sistem *remote keyless*.

PENUTUP

Kesimpulan

Berdasarkan hasil pengujian serta implementasi sistem yang telah dijabarkan pada poin-poin diatas. Maka dapat dirumuskan beberapa poin kesimpulan sebagai berikut:

1. Dengan memanfaatkan nilai RSSI dari koneksi *bluetooth*, pengguna dapat mengetahui *remote keyless* sudah diluar jangkauan dengan kunci pintu sehingga sistem otomatisasi kunci pintu dapat dilakukan.
2. LED RGB dan Motor getar yang terdapat pada sistem *remote keyless* berhasil menyampaikan informasi sinyal kepada pengguna sehingga setiap perlakuan yang dilakukan pada *remote keyless* dan kunci pintu dapat diketahui oleh pengguna.
3. Dari hasil percobaan pada penelitian ini, Motor DC sudah cukup kuat untuk menggerakkan kunci dengan sistem *deadbolt*. Namun ketika perakitan terdapat kesulitan yang dialami dengan menggunakan Motor DC, yaitu mengukur putaran motor untuk menentukan posisi putaran kunci yang sesuai. Sehingga penulis mengganti Motor DC dengan menggunakan Motor Servo yang lebih mudah dan efektif dalam mengatur sudut putaran motor. Dengan menggunakan motor servo sistem kunci *deadbolt* akan presisi dalam putaran posisinya untuk fungsi membuka dan menutup kunci.
4. Sistem *remote keyless* memanfaatkan ESP32 untuk komunikasi serta untuk dapat menghasilkan nilai unik sebagai salah satu cara penggunaan keamanan dengan pendekatan metode PUF. Nilai ini dihasilkan dari karakteristik transistor yang dimiliki perangkat,

sehingga dapat menghasilkan *start-up value* (suv). Dengan memanfaatkan nilai ini, sistem berhasil memberikan keamanan yang unik sistem *remote keyless* sehingga tidak dapat digandakan.

Saran

Dari hasil implementasi dan hasil pengujian sistem yang sudah dilakukan, terdapat beberapa saran yang diharapkan dapat menjadi referensi untuk penelitian selanjutnya:

1. Sistem *gear* yang dimiliki pada sistem masih belum maksimal dalam putaran kunci untuk fungsi manual, sehingga perlu sistem *gear* yang baik dan sesuai agar putaran pada kunci dapat dilakukan dengan memanfaatkan *knob* pintu yang ada untuk membuka dan mengunci pintu dari dalam.
2. Pada penelitian selanjutnya dapat membuat sistem keamanan dengan metode pendekatan PUF lebih baik lagi. Karena pada penelitian ini data unik suv yang digunakan hanya 32 kombinasi angka dan dalam bentuk bilangan desimal, maka untuk meningkatkan keunikan sistem dapat dilakukan dengan menambah jumlah kombinasi data unik serta menggunakan kombinasi bilangan heksadesimal.
3. Untuk penelitian selanjutnya, disarankan untuk menggunakan baterai pada sistem kunci pintu.

REFERENSI

- [1] Geopath, "Geopath Reports More People Leaving Home Every Day," *Billboard Insider*, 13 May 2020. [Online]. Available: <https://billboardinsider.com>. [Accessed 4 March 2023].
- [2] A. N. Mas Erwan, M. N. H. Muzaffar Alfian and M. S. Mohamad Adenan, "Smart Door Lock," *International Journal of Recent Technology and Applied Science*, vol. 3, no. 1, pp. 1-15, 2021.
- [3] A. Muhaimin, "Prototype Sistem Keamanan Pintu Kandang Dan Pemberian Pakan Ternak Puyuh Otomatis Berbasis Mikrokontroler," *Journal on Computer Hardware, Signal Processing, Embedded System and Networking*, vol. 03, no. 01, pp. 1-17, 2022.
- [4] K. Fikri, "Prototipe Sistem Keamanan Pintu Rumah Berbasis Single Board Computer(SBC)," *Journal on Computer Hardware, Signal Processing, Embedded System and Networking*, vol. 01, no. 01, pp. 37-45, 2020.
- [5] L. Bosnjak, J. Sres and B. Brumen, "Brute-force and dictionary attack on hashed real-world passwords," in *2018 41st International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)*, Maribor, 2018.
- [6] P. Weichbroth and L. Lysik, "Mobile Security : Threats and Best Practices," *Mobile Information Systems*, 2020.
- [7] M. Cascella and Y. Al Khalili, *Short Term Memory*, Florida: StatPearls Publishing: Treasure Island, 2019.
- [8] W. Sinlapanuntakul, K. Harris and B. S. Wesley, "Primacy and Recency Effects on Position Error in Short-Term Memory Recall," *Beyond: Undergraduate Research Journal*, vol. 5, no. 1, 2021.
- [9] H. Shevlin, "Current Controversies in the Cognitive Science of Short-term Memory," *Current Opinion in Behavioral Sciences*, vol. 32, no. 24, pp. 148-154, 2020.
- [10] R. N. Brewer, M. R. Morris and S. Lindley, "How to Remember What to Remember : Exploring Possibilities for Digital Reminder Systems," in *ACM Proceedings of the ACM on Interactive, Mobile, Wearable, and Ubiquitous Technologies*, 2017.
- [11] H.-H. Hsu, C.-N. Lee and Y.-F. Chen, "An RFID-Based Reminder System for Smart Home," in *International Conference on Advanced Information Networking and Applications*, 2011.
- [12] P. O. Makanjuola, E. S. Shokenu, H. O. Araromi, P. O. Idowu and J. D. Babtunde, "An Rfid-Based Access Control System Using Electromagnetic Door Lock and an Intruder Alert System," *Journal of Engineering Research and Reports*, vol. 22, no. 11, pp. 7-17, 2022.
- [13] M. A. Prada-Delgado, A. Vázquez-Reyes and I. Baturone, "Physical Unclonable Keys for Smart Lock Systems using Bluetooth Low Energy," in *IECON 2016 - 42nd Annual Conference of the IEEE Industrial Electronics Society*, Seville, 2016.
- [14] Builders Hardware Manufacturers Association, *ANSI/BHMA A156.40 American National Standard for Residential Deadbolts*, New York: BHMA, 2015.
- [15] C. Lipps, A. Weinand, D. Krummacker, F. Christoph and H. D. Schotten, "Proof of Concept for IoT Device Authentication based on SRAM PUFs using ATMEGA

- 2569-MCU," in *1st International Conference on Data Intelligence and Security*, Kaiserslautern, 2018.
- [16] Bluetooth SIG, Inc, "Learn About Bluetooth," Bluetooth SIG, Kirkland, 2023.
- [17] S. P. Raikar, "How Does Bluetooth Work?," *britannica*, 4 March 2022. [Online]. Available: <https://www.britannica.com/story/how-does-bluetooth-work>. [Accessed 2 June 2023].
- [18] F. Ghaniyyah, "Sistem Monitoring Penggunaan Air Kamar Kos," *Journal on Computer Hardware, Signal Processing, Embedded System and Networking Vol 04*, pp. 80-87, 2023.
- [19] A. C. R. Aldawira, H. W. Putra, N. Hanafiah, S. Surjarwo and A. Wibisurya, "Door Security System for Home Monitoring Based on ESP32," *4th International Conference on Computer Science and Computational Intelligence 2019*, vol. 157, pp. 673-682, 2019.
- [20] S. Kurniawan, "MASJID DALAM LINTASAN SEJARAH UMAT ISLAM," *Jurnal Khatulistiwa – Journal of Islamic Studies*, 2014.
- [21] Aisyah Presipitari Harahap, Ady Rizalsyah Thahir, Sri Handjajanti, "PERAN MASJID SEBAGAI PEMBENTUK IDENTITAS TEMPAT," *Jurnal AGORA*, 2020.
- [22] Rifaldy Ramadhan Latief, Andani Achmad, Supriadi Sahibu, "APLIKASI PENCARIAN USTADZ UNTUK WILAYAH KOTA MAKASSAR MENGGUNAKAN ALGORITMA FLOYD WARSHALL DAN HAVERSINE FORMULA BERBASIS ANDROID," *SEBATIK 1410-3737*, 2019.
- [23] Edwin Adrin Wihelmus Sanadi, Andani Achmad, Dewiani, "Pemanfaatan Realtime Database di Platform Firebase Pada Aplikasi E-Tourism Kabupaten Nabire," *JPE*, vol. 22 No. 1, 2018.
- [24] FIBA, 2020 Official Basketball Rules, Mies, Switzerland: FIBA Central Board, 2021.
- [25] D. J. Afandi, "Analisis Kemampuan Dribble, Passing, dan Shooting (1 Point, 2 Point , 3 Point) Bolabasket (Study pada Tin Putri SMA Negeri 3 Pamekasan)," *Jurnal Prestasi Olahraga*, 2017.
- [26] E. P. WALTON, "PERBEDAAN FREKUENSI LATIHAN SHOOTING DAN KOORDINASI TERHADAP KEMAMPUAN MENEMBAK FREETHROW BOLABASKET SISWA PUTRA SMP NEGERI 2 KABUPATEN BANGKA," *Edutainment Jurnal Ilmu Pendidikan dan Kependidikan*, 2018.
- [27] W. K. R. T. R. B. M. A. M. Fajar Awang Irawan, "Analisis biomekanika free throw basket sesuai kaidah dave hopla," *Jurnal Keolahragaan*, 2021.
- [28] R. F. Kevin Rahmat Trisnoyo, "TABUNGAN PINTAR BERBASIS SINGLE BOARD COMPUTER," *Journal on Computer Hardware, Signal Processing, Embedded*, 2020.