



RANCANG BANGUN PROTOTIPE SISTEM KUNCI SIDIK JARI DENGAN APLIKASI IOT

Adelia Octora Pristisahida¹, Achmad Faqihul Fajar²,

^{1,2}Program Studi Teknik Elektro, Universitas Nahdlatul Ulama Yogyakarta, Yogyakarta
 Jl. Lowanu No.47, Sorosutan, Kec. Umbulharjo Kota Yogyakarta Daerah Istimewa Yogyakarta
 Telp (0274) 414 708, 419 769

E-mail: ¹adelia@unu-jogja.ac.id , ²faqihul.elk17@student.unu-jogja.ac.id

ARTICLE INFO

Article History :

Article entry : 01-30-2023
 Article revised : 05-06-2023
 Article received : 16-08-2023

Keywords :

Fingerprints, Digital Key Systems, Internet of Things

ABSTRACT

As a security for a house or cupboard, security locks on doors, windows and cupboards still use a conventional system using a main lock and key. With today's rapid technological developments, there needs to be development to create a more modern and practical digital key system. The lock system created in this study is a type of digital lock that uses a fingerprint sensor with IoT applications. The components used in this tool are a fingerprint sensor, reed switch as input and Wemos D1 Mini as a microcontroller that processes data from input. System output will be displayed using the LCD on the device and sent to the cellphone using a telegram chat bot. The test uses two fingerprint samples with different patterns with names on the sensors as ID1 and ID2, with the security level on the fingerprint sensor at level 3. With a confidence rate value of >70 (more than) as a reference for success or failure of the fingerprint unlocking attempt, if the confidence rate reference value > 70 is met, the lock will open and will automatically send a notification to the telegram bot. With the results of the average confidence rate on fingerprints with ID 1 is 120.4 confidence rate and the average value on fingerprints with ID 2 is 149.4 confidence rate.

1. PENDAHULUAN

Tindak kejahatan berupa pencurian merupakan jenis kejahatan yang paling tinggi persentasenya dibandingkan dengan jenis tindak kejahatan lainnya. Berdasarkan data dari Badan Pusat Statistik pada tahun 2018 dari 83931 wilayah administrasi setingkat desa, persentase wilayah yang mengalami tindak pencurian mencapai 45,01 %. Angka pencurian yang tinggi di Indonesia terpicu oleh banyak faktor. Mulai dari masalah ekonomi, dorongan dari kecanduan obat terlarang, maupun karena adanya kesempatan (Statistik Kriminal 2021, t.t.).

Penggunaan kunci konvensional sampai saat ini masih dominan, karena faktor ekonomis dan sudah familiar atau dikenal masyarakat umum. Namun disisi lain kefamiliaran kunci pintu bagi masyarakat umum, maka kunci pintu konvensional juga familiar bagi para pencuri. Banyak metode yang dilakukan untuk dapat membobol kunci pintu, mulai dari cara mencongkel, membuat kunci duplikat ataupun

dengan cara menggunakan alat berupa lockpick yang terdiri dari 2 batang besi kecil dengan bentuk khusus, untuk menekan pegas pin dalam kunci dan memutar bagian dalam kunci. Faktor lain yang dapat memancing kejahatan adalah saat korban lengah lupa mengunci pintu saat berpergian atau meninggalkan kunci menempel di pintu saat berpergian [2].

Dengan perkembangan teknologi yang pesat saat ini, perlu ada pengembangan untuk membuat sistem kunci digital yang lebih modern dan praktis. Salah satu pengembangan dari sistem kunci digital tersebut yakni penggunaan sistem kunci sidik jari. Penggunaan sidik jari sebagai kunci bertujuan untuk memberikan kemudahan, dan mencegah serta meminimalisir kemungkinan tindak pencurian. Karena sistem kunci digital, salah satunya dengan sidik jari belum familiar bagi para pencuri di Indonesia [3].

Studi penggunaan mikrokontroler untuk memberikan kemudahan bagi manusia telah

dilakukan, baik untuk sistem dengan perangkat elektronika maupun untuk sistem tenaga. Salah satu penggunaannya adalah di sistem parkir berbasis mikrokontroler dan penerapan IoT pada kasus pembangkit listrik tenaga mikrohidro (PLTM), membuktikan perlunya untuk meneliti lebih banyak lagi terkait IoT ini di berbagai bidang. Menurut penelitian yang telah ada, penerapan IoT ini juga dapat dilakukan berbasis SMS gateway (Bachri & Kunci, 2019; Prasetyo dkk., 2022; Supriyono1 dkk., 2022).

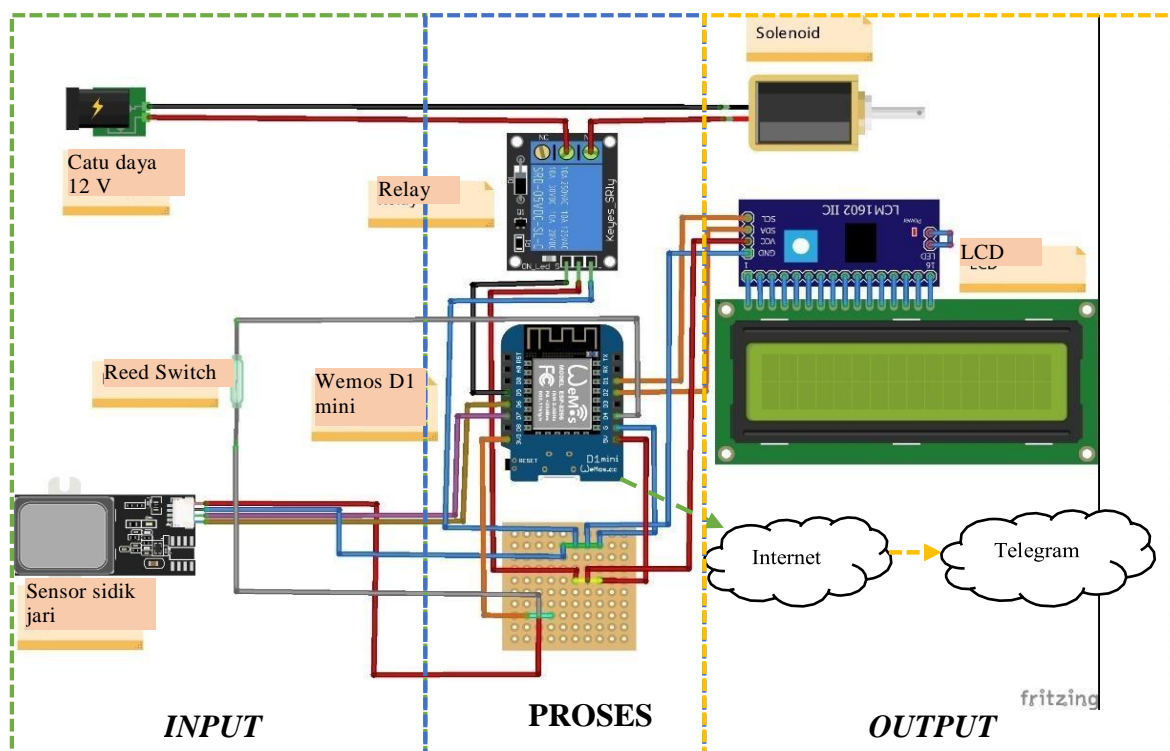
Penelitian terkait kunci pengaman telah banyak dilakukan. Sistem kunci ada yang dapat menggunakan Reed Switch dan PI, dengan output sensor dikirimkan melalui SMS dengan menggunakan modul GSM. Sistem kunci dengan menggunakan kendali Wemos D1 Mini dan Sensor PIR HC-SR501 sensor mendeteksi jika ada gerakan, lalu mengirimkan notifikasi ke ponsel melalui telegram. Sistem kunci juga dapat menggunakan RFID dan tombol angka pada alat, password akan dikirimkan ke ponsel melalui Bluetooth digunakan sebagai kunci cadangan jika RFID tertinggal [7]–[9].

Pada penelitian ini, selain penggunaan kunci sidik jari, pengembangan lain dari sistem kunci digital yakni penggunaan sistem IoT (Internet of Things), yang memungkinkan sistem kunci digital berkomunikasi ke pengguna melalui jaringan internet. Pengembangan sistem kunci pintu dengan IoT memungkinkan pemantauan dari jarak jauh yang salah satu tujuannya untuk keamanan. Dengan adanya ponsel pintar berbasis android, memberikan kemudahan dalam pemantauan sistem kunci IoT dengan menggunakan aplikasi berbasis android.

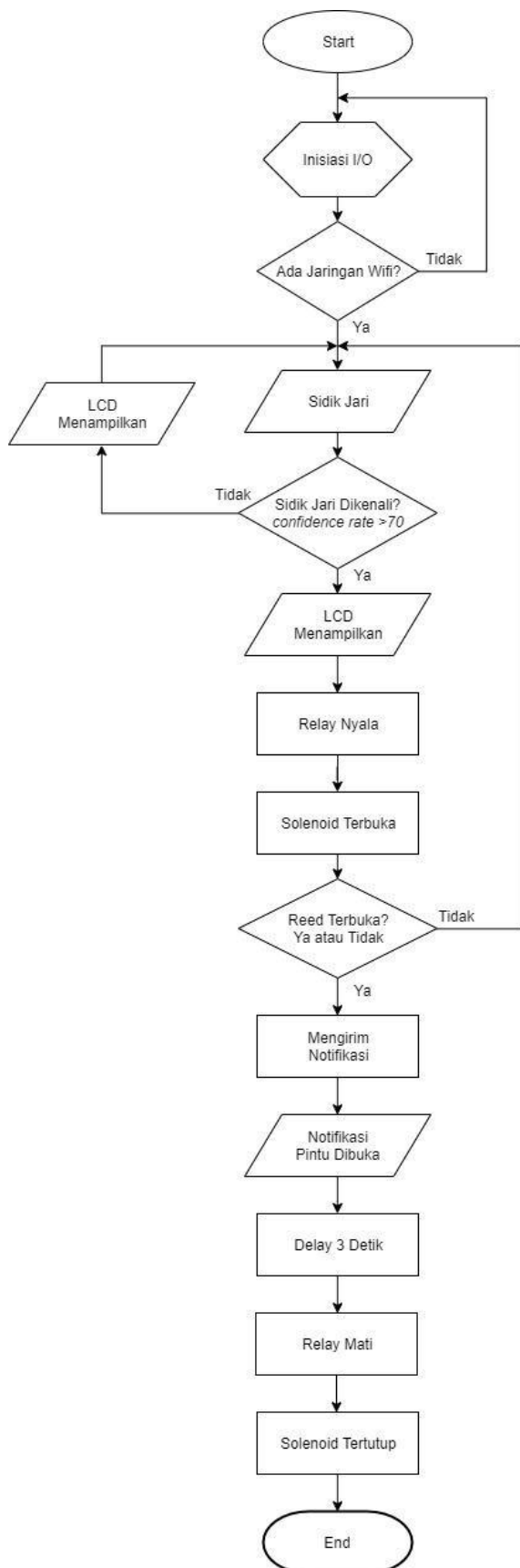
2. METODOLOGI PENELITIAN

Dalam proses penelitian ini metodologi penelitian yang dilakukan adalah:

- Tahapan awal yakni, studi pustaka dilakukan untuk mengumpulkan literatur yang berkaitan dengan penelitian yang diangkat. Mencari referensi dari berbagai sumber seperti artikel ilmiah, buku, jurnal yang berhubungan dengan faktor pengamanan kunci pintu dan mengetahui komponen yang digunakan.
- Tahap pengumpulan data menggunakan metode observasi dan identifikasi komponen yang akan digunakan dalam sistem dan mekanismenya.
- Pada perancangan alat terdapat beberapa susunan tahapan, yaitu blok input, blok proses, dan blok output. Tahap Implementasi alat dan bahan yang telah 4 terkumpul, dibuat sesuai rancangan, analisis, dan diagram blok yang telah dibuat.
- Pada tahap ini alat akan dicoba dan diamati apakah alat dapat bekerja dengan baik. Pengujian dilaksanakan untuk mengamati bagaimana kerja alat berdasarkan rancangan yang telah dibuat. Dan hasil dari pengujian akan dianalisa dan dibahas berdasarkan data yang terkumpul dan merujuk literatur yang telah dikumpulkan.
- Pada tahap evaluasi berdasarkan dari hasil penelitian yang dipaparkan.



Gambar 1. Blok Diagram Alat



Gambar 2. Flowchart Kerja Alat

2.1. Blok Diagram dan Flowchart

Blok diagram penelitian ini ditampilkan pada Gambar 1. Terlihat pada gambar, Wemos akan mencari apakah ada jaringan internet tersedia, jika jaringan tersedia wemos akan mencoba terhubung ke jaringan tersebut. Sensor sidik jari yang digunakan merupakan tipe optikal, mendeteksi pola sidik jari berupa gambar dan membandingkan dengan data gambar yang tersimpan berdasarkan kontras antara kontur berupa ridge dan valley dari gambar input sidik jari. Input dari sensor sidik jari akan masuk ke mikrokontroler Wemos D1 Mini yang akan menjalankan perintah untuk mengirimkan pesan notifikasi ke telegram menggunakan perintah bot telegram yang memberi peringatan jika ada percobaan membuka kunci [10].

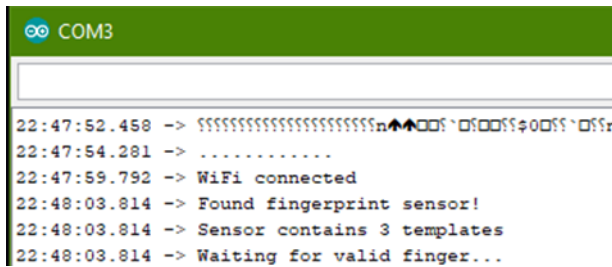
Jika sidik jari dikenali maka wemos akan mengirim sinyal ke relay untuk terbuka jika sidik jari dikenali, jika tidak relay akan tetap tertutup. Saat relay terbuka solenoid akan aktif dan membuka kunci selama 3 detik lalu terkunci kembali. Reed digunakan sebagai input untuk mengetahui apakah pintu sudah dibuka atau tidak, jika pintu dibuka bot akan mengirim notifikasi, jika tidak terbuka notifikasi tidak dikirim. LCD digunakan sebagai output untuk menampilkan output sistem pada alat, menampilkan apakah sidik jari dikenali atau tidak dan apakah alat sudah dalam posisi siaga, alur kerja ditampilkan pada Gambar 2 [11].

2.2. Pengujian alat

Pengujian sistem dilaksanakan untuk mengetahui apakah alat dapat bekerja dan mengetahui apakah alat yang digunakan sudah tersinkron. Pengujian dilakukan menggunakan jari telunjuk kanan dari dua orang pengguna, dilakukan pengulangan sebanyak sepuluh kali dengan selisih 10 detik tiap pengulangan. Kondisi sensor fingerprint pada saat pengujian berisi template sidik jari dari pengguna yang akan diujikan, dengan tingkat pengamanan level 3. Untuk membuka kunci digunakan nilai confidence rate sebagai acuan jika nilai confidence rate >70 (lebih dari) terbaca pada sensor maka kunci akan terbuka dan sistem akan mengirim notifikasi. Pada pengujian digunakan koneksi tethering dari ponsel, dengan kondisi koneksi awal pengujian ditampilkan pada gambar 3.



Gambar 3. Ping awal pengetesan



Gambar 4. Serial monitor posisi siaga

Pengujian terdiri dari 5 komponen pengujian yakni ID fingerprint, tingkat confidence rate dari pembacaan sensor fingerprint, kondisi solenoid, lama waktu masuk notifikasi dan kondisi koneksi. Dari 5 komponen pengujian berikut akan dianalisa dan dibahas pada bab berikutnya. Tampilan serial monitor pada saat alat dalam posisi siaga ditampilkan pada gambar 4.

2.3 Hasil Pengujian

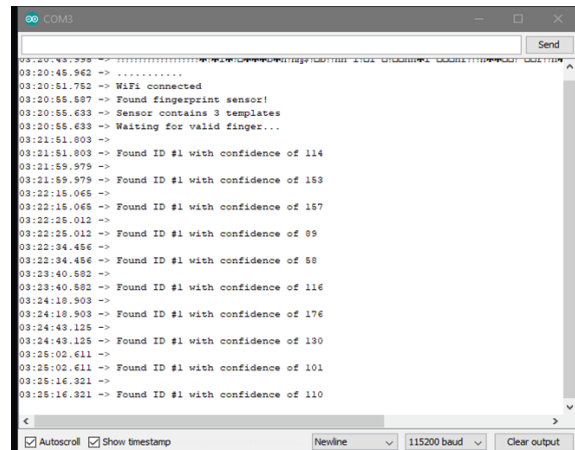
Pengujian alat dilakukan dengan mengamati nilai confidence rate yang dihasilkan oleh sensor sidik jari. Nilai confidence rate merupakan hasil dari seberapa nilai kecocokan sidik jari yang ditempelkan pada sensor, karena nilai ini berdasarkan dari kejelasan penangkapan sensor nilai bisa bervariasi pada tiap perulangan percobaan yang dilakukan. Faktor yang dapat mempengaruhi mulai dari jari yang basah, berminyak, posisi jari saat ditempelkan maupun tergores atau luka pada permukaan sidik jari. Pada dasarnya pada semua jenis pola sidik jari memiliki nilai confidence rate yang sama, karena nilai confidence rate merupakan nilai dari perbandingan antara data sidik jari ditempelkan pada sensor dengan yang tersimpan dalam memori sensor sidik jari [12].

Tabel 1. Hasil Uji ID 1

No	ID Pengguna 1	Sensor Fingerprint	Solenoid
1	Dikenali	114 confidence	Terbuka
2	Dikenali	153 confidence	Terbuka
3	Dikenali	157 confidence	Terbuka
4	Dikenali	89 confidence	Terbuka
5	Tidak Dikenali	58 confidence	Terkunci
6	Dikenali	116 confidence	Terbuka
7	Dikenali	176 confidence	Terbuka
8	Dikenali	130 confidence	Terbuka
9	Dikenali	101 confidence	Terbuka
10	Dikenali	110 confidence	Terbuka
Rata-rata		120.4 confidence	

Hasil pengujian dengan pengaturan nilai minimal confidence rate >70 dilakukan sebanyak sepuluh kali pengulangan dengan hasil pengujian dari sidik jari ID 1 ditampilkan pada tabel 1.

Hasil pembacaan output dari sistem yang terbaca pada serial monitor ditampilkan pada gambar 5 [13].



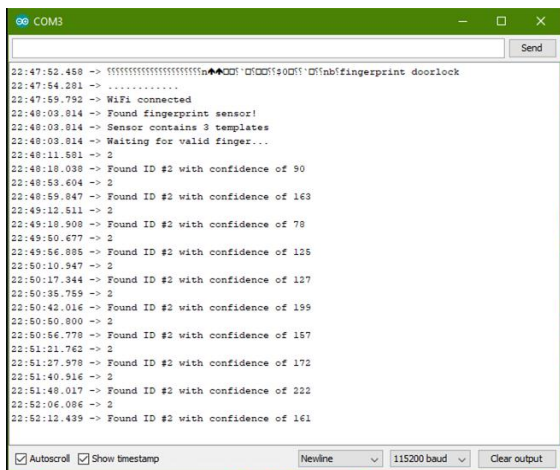
Gambar 5. Serial Monitor Uji ID 1

Hasil pengujian dengan pengaturan nilai minimal confidence rate >70 dilakukan sebanyak sepuluh kali pengulangan dengan hasil pengujian dari sidik jari ID 2 ditampilkan pada tabel 2.

Tabel 2. Hasil Uji ID 2

No	ID Pengguna 1	Sensor Fingerprint	Solenoid
1	Dikenali	90 confidence	Terbuka
2	Dikenali	163 confidence	Terbuka
3	Dikenali	78 confidence	Terbuka
4	Dikenali	125 confidence	Terbuka
5	Dikenali	127 confidence	Terbuka
6	Dikenali	199 confidence	Terbuka
7	Dikenali	157 confidence	Terbuka
8	Dikenali	172 confidence	Terbuka
9	Dikenali	222 confidence	Terbuka
10	Dikenali	161 confidence	Terbuka
Rata-rata		149.4 confidence	-

Pembacaan output dari sistem yang terbaca pada serial monitor ditampilkan pada Gambar 6

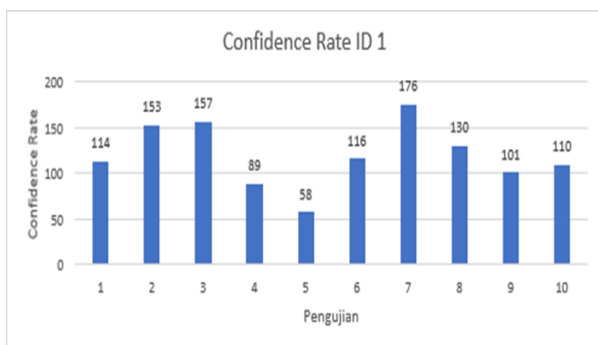


Gambar 6. Serial monitor uj ID 2

3. PEMBAHASAN

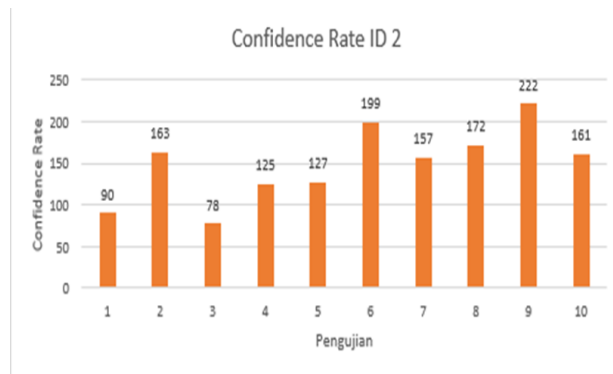
a. Analisis

Dari hasil pengujian didapatkan hasil confidence rate yang bervariasi. Pada sidik jari ID 1 selisih nilai terbaca sebesar 118 confidence rate, dan rata-rata 120.4 confidence rate. Pada pengujian ID 1 nilai tertinggi 176 confidence rate, terdapat nilai terendah 58 confidence rate, yang belum memenuhi nilai minimal untuk menjalankan perintah kirim notifikasi dan membuka solenoid. Ditampilkan pada gambar 7.



Gambar 7. Grafik Confidence Rate Pada ID 1

Dari hasil pengujian pada sidik jari ID 2 selisih nilai terbaca sebesar 144 confidence rate, dan rata-rata 149.4 confidence rate. Pada ID 2 nilai tertinggi pada 222 confidence rate, nilai terendah adalah 78 confidence rate. Ditampilkan pada gambar 8.



Gambar 8. Grafik Confidence Rate Pada ID 2

b. Pembahasan

Selisih pada pembacaan dapat terjadi karena noise atau gangguan yang terjadi saat sensor mendeteksi sidik jari, gangguan yang dapat menyebabkan penurunan tangkapan sensor untuk membaca gambar tangkapan sidik jari, gangguan dapat berupa debu, air ataupun minyak pada permukaan sidik jari. Pada sistem pengujian selain pengaruh dari permukaan sidik jari yang diujikan, terdapat juga faktor dari level pengamanan yang diseting pada sensor [14].

Tingkat atau level pengamanan pada sensor sidik jari yang digunakan yakni menggunakan chip zianthec as608, terdiri dari level 1 sampai 5. Seting level 1 sebagai yang terendah dan level 5 sebagai yang tertinggi. Pada seting level 1 nilai FAR (False Acceptance Rate) ditinggikan dan nilai FRR (False Rejection Rate) direndahkan. Pada seting 5 nilai FAR (False Acceptance Rate) direndahkan dan nilai FRR (False Rejection Rate) ditinggikan [14].

Pada seting prototipe yang dibuat menggunakan seting level 3, yang merupakan pengaturan bawaan dari seting library. Pada analisa lama pengiriman notifikasi, terdapat beberapa faktor yang menyebabkan perlambatan dalam pengiriman notifikasi, diantaranya sebagai berikut:

- Faktor penggunaan logika if (logika perbandingan),
- Faktor ping atau latensi data (perlambatan pada pengiriman data),
- Faktor searching time pada sensor sidik jari,
- Faktor delay pada fungsi program pembuka solenoid.

Pada faktor pencarian template sidik jari mengacu pada datasheet sensor AST (Average Searching Time) = <1s, maka dapat terjadi perlambatan pengiriman notifikasi karena jika respon sensor terlambat. Pada faktor delay pada fungsi program pembuka solenoid, jika program diatas baris

program tersebut sudah tereksekusi maka sistem otomatis akan masuk ke kondisi delay, pada kondisi tersebut sistem akan memberhentikan input dan output sampai waktu delay habis. Pada sistem terdapat delay 3 detik setelah logika pembandingan dan fungsi program pembuka solenoid, dan bisa terjadi keterlambatan selama ± 3 detik jika delay telah dijalankan.

Fitur sidik jari pada minutiae atau detail kecil pada sidik jari yang berperan dalam mengenali pola unik sidik jari. Dalam pola minutiae yang terdapat bifurcation, crossover, island, ridge end dan core. Lebih berperan dalam identifikasi pola unik sidik jari, karena dari tiga pola dasar sidik jari bisa menjadi unik dan tidak sama satu sama lain karena posisi dan bentuk akhir fitur fisik diatas yang berbeda [9].

Jika sidik jari telah terbaca dan dikenali saat pintu terbuka reed switch akan mendeteksi apakah pintu terbuka atau tidak, pada pengujian reed switch berhasil mendeteksi dan mengirim notifikasi jika pintu terbuka, dan mengirim notifikasi kembali jika pintu sudah tertutup.

Karena sistem kunci menggunakan sidik jari sebagai kuncinya maka kunci tidak bisa tertinggal karena sidik jari menempel pada tangan pemiliknya. Selain itu kunci pintu juga tidak bisa dibuka dengan menggunakan kunci duplikat maupun lockpick. Karena tidak ada lubang kunci yang terlihat pada pintu untuk dibuka dengan menggunakan menggunakan kunci duplikat maupun lockpick.

5. PENUTUP

Di jaman yang serba digital seperti saat ini, tentu berharap agar dapat lebih praktis dalam menjalani hidup sehari-hari. Kunci berbasis sidik jari dibuat agar manusia dapat hidup lebih nyaman, bepergian tanpa harus membawa barang yang banyak. Sistem kunci berbasis sidik jari dengan aplikasi IoT ini dapat digunakan dengan baik. Nilai rata-rata *confidence rate* pada sidik jari yang digunakan sebagai contoh termasuk baik dan mudah untuk digunakan. Waktu rata-rata untuk pengiriman pesan ke ponsel juga dalam waktu yang dapat ditoleransi, yaitu sekitar 4-5 detik. Kunci berbasis sidik jari tidak perlu repot membawa barang kemana-mana seperti kunci manual atau kartu ID, karena menggunakan jari pengguna sebagai pembuka kunci. Kekurangan dari penelitian ini adalah ketika daya untuk sistem kunci terputus dan baterai cadangan untuk kunci telah habis. Namun ini dapat diatasi dengan menyiapkan hubungan ke power bank yang sifatnya portabel, mudah dipindahkan.

REFERENSI

- [1] "1. Statistik Kriminal 2021".
- [2] A. Gusti Ramakumbo NIM, "Magnetic Door Lock Menggunakan Kode Pengaman Berbasis Atmega 328."
- [3] C. Bell, "What Is the Internet of Things?," *Windows 10 for the Internet of Things*, hlm. 1–19, 2016, doi: 10.1007/978-1-4842-2108-2_1.
- [4] H. J. Prasetyo, F. B. Hartono, dan A. Wuryandari, "Model Sistem Parkir dengan Mikrokontroler," *Jurnal JE-UNISLA : Electronic Control, Telecommunication, Computer Information and Power System*, vol. 7, no. 2, hlm. 113–118, Sep 2022, Diakses: 29 Januari 2023. [Daring]. Tersedia pada: <https://jurnalteknik.unisla.ac.id/index.php/elektronika/article/view/888>
- [5] A. Supriyono¹, M. J. Afroni², dan O. Melfazen³, "Penerapan SCADA Berbasis IoT untuk Simulator Kontrol Panel pada Contoh Kasus Pembangkit Listrik Tenaga Mikrohidro (PLTM)," *Jurnal JE-UNISLA : Electronic Control, Telecommunication, Computer Information and Power System*, vol. 7, no. 2, hlm. 119–126, Sep 2022, doi: 10.30736/JE-UNISLA.V7I2.889.
- [6] A. Bachri dan K. Kunci, "Rancang Bangun Smart Kontrol Lampu Penerangan Jalan Umum Berbasis SMS Gateway," *Jurnal JE-UNISLA : Electronic Control, Telecommunication, Computer Information and Power System*, vol. 4, no. 2, hlm. 256–264, Okt 2019, doi: 10.30736/JE.V4I2.363.
- [7] A. Ghifari Aditya, I. Permana Solihin, dan Y. Widiastwi, "Sistem Kunci Pintu RFID dan Password Berbasis Arduino Uno dengan One Time Password melalui SMS," *Prosiding Seminar Nasional Mahasiswa Bidang Ilmu Komputer dan Aplikasinya*, vol. 1, no. 1, hlm. 81–91, Jul 2020, Diakses: 29 Januari 2023. [Daring]. Tersedia pada: <https://conference.upnvj.ac.id/index.php/senamika/article/view/236>
- [8] F. Panca Juniawan, D. Yuny Sylfania, T. Informasika, S. Atma Luhur, J. Jend Sudirman, dan S. Baru, "Prototipe Sistem Keamanan Rumah Menggunakan Kombinasi Sensor dan SMS Gateway," *Jurnal Teknoinfo*, vol. 13, no. 2, hlm. 78–83, Jul 2019, doi: 10.33365/JTI.V13I2.304.
- [9] R. Wahyuni, A. Rickyta, U. Rahmalisa, dan Y. Irawan, "Home Security Alarm Using Wemos D1 And HC-SR501 Sensor Based Telegram Notification," *Journal of Robotics and Control (JRC)*, vol. 2, no. 3, hlm. 200–204, Mei 2021, doi: 10.18196/JRC.2378.
- [10] G. Urban, "Jacob Fraden: Handbook of modern sensors: physics, designs, and applications, 5th ed.," *Analytical and*

- Bioanalytical Chemistry* 2016 408:21, vol. 408, no. 21, hlm. 5667–5668, Mei 2016, doi: 10.1007/S00216-016-9637-2.
- [11] I. Novianto, L. Kurniasari, A. Octora Pristisahida, B. Kusuma Prasaja, dan U. Nahdlatul Ulama, “Implementasi Filter Kalman untuk Optimasi Pengukuran Sensor Suhu NTC pada Kompor Listrik Malam Berbasis Fuzzy,” *Jurnal Darma Agung*, vol. 30, no. 3, hlm. 132–143, Nov 2022, doi: 10.46930/OJSUDA.V30I3.1949.
- [12] V. B. Joshi dan M. S. Raval, “Adaptive Threshold for Fingerprint Recognition System Based on Threat Level and System Load,” *Procedia Comput Sci*, vol. 171, hlm. 498–507, Jan 2020, doi: 10.1016/J.PROCS.2020.04.053.
- [13] S. Rozga, “Introduction to Chat Bots,” *Practical Bot Development*, hlm. 1–28, 2018, doi: 10.1007/978-1-4842-3540-9_1.
- [14] S. Shanawaz Basha dan & N. Musrat Sultana, “Spectral Minutiae Fingerprint Recognition System”.