Prototype Sistem Keamanan Brankas Berbasis Sensor Sidik Jari

Hanif Indra Ramadhan dan Raden Supriyanto

Universitas Gunadarma
Jalan. Margonda Raya 100, Depok
E-mail : ramadhan28123@gmail.com, supriyanto.r@gmail.com

Abstrak

Brankas merupakan suatu sarana penyimpanan yang digunakan untuk menyimpan barang-barang berharga milik individu ataupun kelompok. Seiring dengan perkembangan teknologi, diperlukan solusi keamanan yang lebih maju dan handal untuk memberikan perlindungan yang optimal terhadap akses tidak sah dan risiko pencurian pada brankas. Penelitian ini bertujuan untuk membuat prototype sistem keamanan Brankas dengan fitur sidik jari dan kode OTP guna meningkatkan tingkat keamanan dan kontrol akses. Metode penelitian yang dilakukan meliputi studi literatur, perancangan, pembuatan alat, dan uji coba. Pada hasil penelitian, ditemukan bahwa penggunaan sensor sidik jari sebagai metode autentikasi utama berhasil meningkatkan tingkat keamanan akses pada Brankas. Sensor sidik jari mampu mengidentifikasi pengguna yang sah dengan tingkat akurasi yang tinggi, memperkuat kontrol akses. Hasil uji coba menunjukkan bahwa sistem ini efektif dalam mengamankan Brankas dari akses tidak sah. Dengan demikian, integrasi sensor sidik jari dengan OTP pada sistem keamanan Brankas memberikan solusi yang handal dalam melindungi barang-barang berharga dari risiko pencurian. .

Kata kunci : Brankas, Keypad 4x4 Matrix, OTP, Solenoid, Sensor Sidik Jari, Wemos D1 R32

Pendahuluan

Brankas harus memiliki sistem keamanan yang canggih untuk mencegah terjadinya pencurian. Keamanan juga merupakan aspek penting dari menyimpan barang berharga. Banyak orang mengalami kesulitan untuk menjaga barang berharga mereka, terutama resiko kehilangan atau pencurian. Seiring dengan perkembangan teknologi, diperlukan solusi keamanan yang lebih maju dan handal untuk memberikan perlindungan yang optimal terhadap akses tidak sah dan risiko pencurian.

Purwarupa sistem keamanan Brankas dibangun dengan metode verifikasi dua tahap, yaitu menggunakan sensor sidik jari dan kode OTP. Tujuan dari pengembangan sistem ini adalah untuk meningkatkan tingkat keamanan dan kontrol akses pada Brankas, sehingga barang-barang berharga dapat disimpan dengan lebih aman dan terhindar dari risiko pencurian atau akses tidak sah. Dengan menggabungkan teknologi sidik jari dan kode OTP, diharapkan sistem ini dapat memberikan perlindungan yang lebih handal dan menghadirkan solusi keamanan yang efisien bagi pengguna.

Cara kerja dari alat ini yaitu, pertama pengguna harus mendaftarkan sidik jari mereka sebelum menggunakan Brankas. Proses pendaftaran memerlukan pengguna untuk memasukkan password yang sesuai. Jika password sesuai, pengguna akan diminta untuk input sidik jari mereka pada sensor. Setelah proses pendaftaran selesai, sidik jari akan tersimpan. Ketika pengguna ingin membuka Brankas, mereka harus menempatkan sidik jari mereka pada sensor. Sistem akan memverifikasi sidik jari dengan data yang tersimpan dalam memori. Jika sidik jari terkonfirmasi, langkah selanjutnya adalah melakukan autentikasi kedua. Pengguna akan diminta untuk memasukkan OTP melalui keypad. Jika kode OTP yang dimasukkan benar, maka pintu Brankas akan terbuka, namun jika OTP yang dimasukkan salah, sistem akan memberikan pemberitahuan melalui output LCD dan memicu bunyi buzzer sebagai tanda bahwa akses ditolak. Untuk menjaga keamanan dan mengoptimalkan kinerja alat, jumlah pengguna yang dapat mendaftarkan sidik jari dibatasi menjadi hanya 3 sidik jari saja. Hal ini akan memastikan bahwa hanya pengguna yang sah yang dapat mengakses Brankas dengan menggunakan metode verifikasi sidik jari dan kode OTP yang telah ditentukan.

Metode Penelitian

Dalam penelitian ini, perancangan alat menggunakan aplikasi Fritzing. Fritzing adalah aplikasi

perangkat lunak yang dirancang khusus untuk merancang dan menggambarkan sirkuit elektronika atau skematik layout secara visual. Perancangan ini menggambarkan bagaimana tata letak setiap kabel pin komponen yang terhubung ke mikrokontroler Wemos D1 R32. Perancangan skematik ini melihatkan komponen perangkat keras input, proses, konektor, dan output. Diantaranya: Keypad Matrix 4x4, dan Sensor Fingerprint FPM10A sebagai input. Mikrokontroler Wemos D1 R32 sebagai pemrosesan. PCF8574 I2C sebagai konektor antara Keypad dan LCD ke Wemos, Baterai sebagai tegangan eksternal untuk Solenoid. Dan yang terakhir yaitu Buzzer dan LCD yang berperan sebagai output pada alat.

Rancangan Skematik Alat

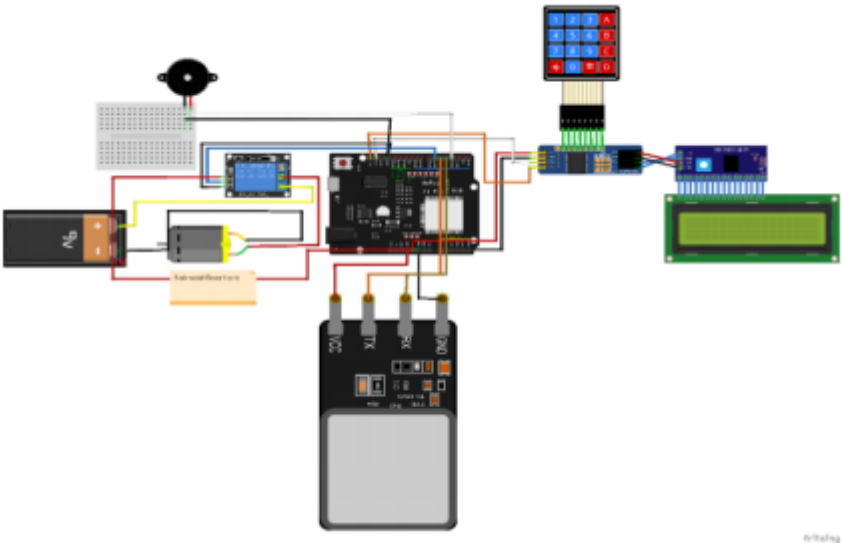
Dalam perancagan sistem kemanan kotak penyimpanan difokuskan untuk memberikan perlindungan dan keamanan ekstra pada kotak penyimpanan, sehingga hanya pengguna yang memiliki akses yang sah, yaitu yang memiliki sidik jari terdaftar dan mengetahui password yang benar (OTP (One Time Password)) yang dapat membuka dan mengakses isi kotak. Dengan adanya sistem keamanan ini, diharapkan dapat mencegah akses yang tidak sah atau pencurian barang berharga di dalam kotak penyimpanan.

Penjelasan pada Gambar 1, alat ini memiliki input atau masukan menggunakan sensor sidik jari dan keypad matrix, sensor sidik jari digunakan untuk verifikasi sidik jari dan pendaftaran sidik jari. Keypad matrix berfungsi untuk input password yang didapat setelah verifikasi sidik jari, dalam program keypad matrix juga terdapat beberapa fungsi seperti, menambah data sidik jari, menghapus data sidik jari, dan mengganti password. Password yang dimaksud adalah password untuk memberikan akses khusus kepada pengguna dalam melakukan tugas-tugas tertentu, seperti menambahkan sidik jari, dan menghapus sidik jari.

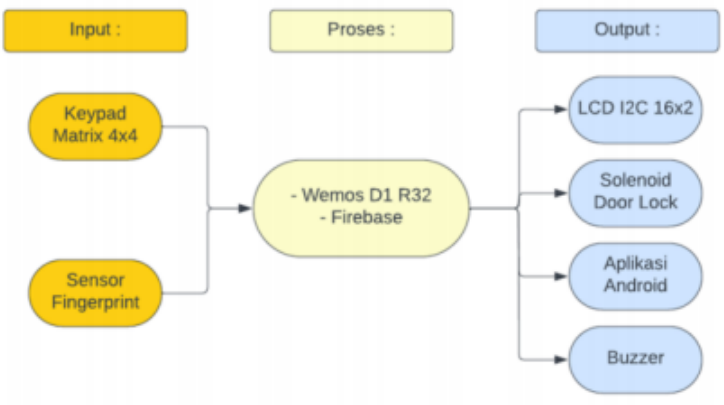
Rancangan Blok Diagram

Analisa blok diagram dalam penelitian ini terdiri dari tiga bagian utama, yaitu input, proses, dan output. Gambar 2 memberikan gambaran yang lebih rinci mengenai bagian-bagian tersebut. Dalam blok diagram ini, langkah-langkah proses secara sistematis disajikan untuk memudahkan pemahaman tentang cara kerja sistem keamanan brankas.

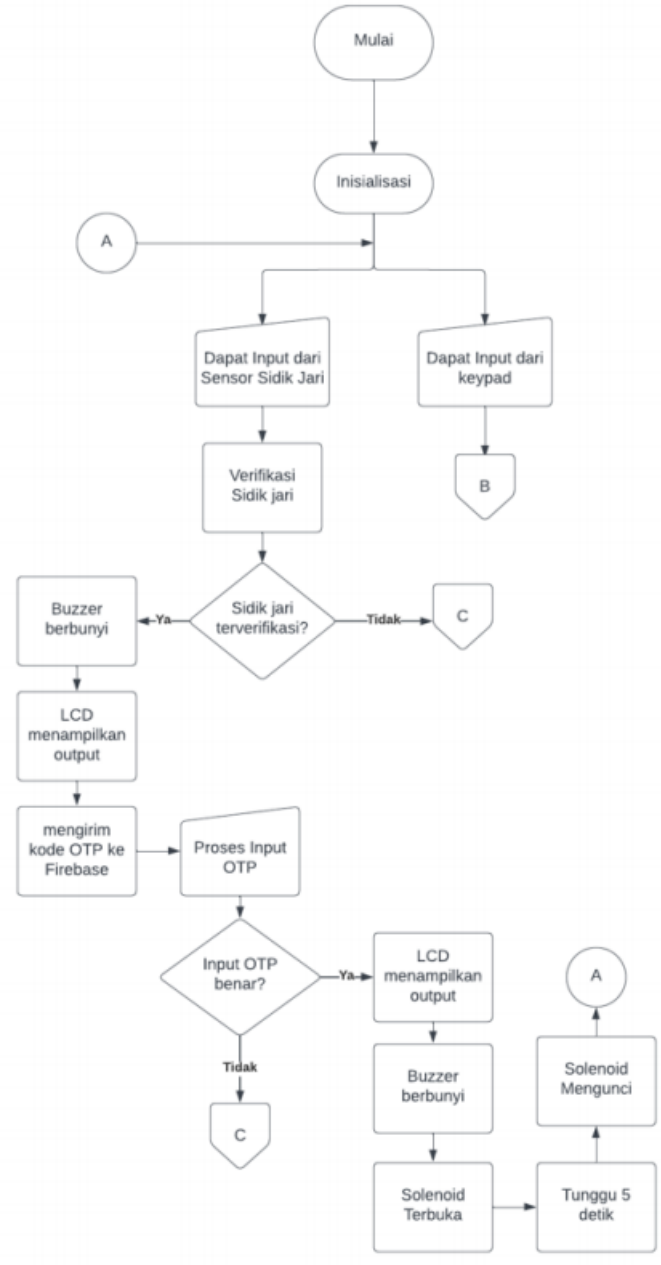
Pada bagian input terdapat dua komponen yaitu keypad matrix dan sensor fingerprint, keypad matrix berfungsi untuk memasukan password dan menjalankan perintah tertentu, sensor sidik jari berfungsi untuk indentifikasi sidik jari. Bagian proses melibatkan mikrokontroler Wemos D1 R32 sebagai pusat kontrol yang telah diprogram sesuai fungsinya. Firebase digunakan sebagai media pengiriman dan penerimaan data dalam penelitian ini. Data yang diperoleh dari mikrokontroler akan dikirim ke Firebase, dan selanjutnya Firebase akan meneruskan data tersebut ke aplikasi Android untuk menerima data OTP yang nantinya kode OTP tersebut digunakan untuk membuka kunci pintu kotak penyimpanan. Relay berperan sebagai pengontrol untuk menggerakan solenoid lock. Output pada alat ini terdapat 4 macam, yaitu LCD I2C sebagai penampil kalimat berdasarkan input dari pengguna, Solenoid door lock untuk membuka kunci pintu, buzzer sebagai output suara, dan aplikasi android sebagai penerima kode OTP.



Gambar 1: Rangkaian skematik alat



Gambar 2: Blok Diagram



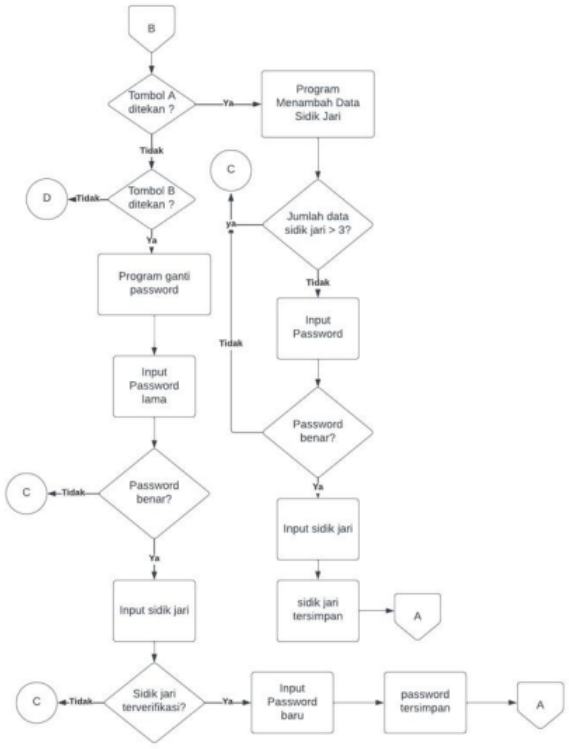
Gambar 3: Flowchart 1

Rancangan Flowchart

Pada bagian ini akan menjelaskan flowchart tentang sistem keamanan kotak penyimpanan menggunakan sensor sidik jari dan otp. Flowchart terdiri dari 3 gambar (Gambar 3, 4 dan 5), masing-masing gambar akan mempunyai penjelasanya sendiri. Flowchart dimulai proses inisialisasi, proses inisialisasi adalah langkah-langkah awal yang dilakukan sebelum alur utama program dimulai. Proses ini berfungsi untuk menyiapkan segala sesuatu yang diperlukan sebelum program dapat berjalan dengan benar. Proses inisialisasi dalam alat ini adalah mengatur nilai awal variabel, dan memulai perangkat keras yang digunakan dalam program.

Setelah program siap dan dalam keadaan stand by, maka program akan menunggu input dari sidik jari dan keypad, pada flowchart digunakan simbol "manual input", karna program akan menunggu input dari pengguna untuk masuk ke program selanjutnya. Untuk membuka kunci pintu brankas maka pengguna harus input sidik jari untuk verifikasi, akan berlanjut untuk proses verifikasi sidik jari, ada decision (kondisi) apakah sidik jari terverifikasi. Dalam proses ini program akan membandingkan sidik jari yang didapatkan dengan data sidik jari yang tersimpan, jika sidik jari cocok dengan data salah satu sidik jari, maka flowchart akan ke proses "ya", proses buzzer menyala yaitu buzzer memberikan output suara sesuai yang telah diprogram untuk menandakan bahwa sidik jari terverifikasi, dan proses LCD menampilkan output bahwa sidik jari terverifikasi.

Kemudian proses mengirim kode OTP ke Firebase, Wemos akan men-generate angka acak sebanyak 6 digit sebagai kode OTP yang nantinya akan dikirim ke Firebase, setelah Firebase mendapatkan data OTP maka akan diteruskan ke aplikasi yang telah dibuat. Kemudian masuk ke proses input OTP, proses input OTP menggunakan simbol "manual input" karna menunggu pengguna untuk input OTP yang telah didapatkan. Kemudian decision "Input OTP benar?", apakah OTP yang dimasukan pengguna benar, jika ya maka LCD akan menampilkan output bahwa OTP yang diinput benar, dan buzzer akan berbunyi, dan solenoid akan terbuka yaitu bagian depan (Plunger) akan mengecil yang membuat kunci pintu brankas terbuka. Kemudian proses tunggu 5 detik, artinya solenoid akan terbuka selama 5 detik kemudian menutup kembali, setelah menutup maka flowchart akan lanjut ke connector A, connector A akan menuju ke program awal yaitu menunggu input. Pada decision jika pilihanya tidak maka akan berlanjut ke connector C, pada connector C terdapat 2 proses yaitu Buzzer berbunyi dan LCD menampilkan output, 2 proses ini sebagai tanda untuk kesalahan input. Kemudian saat program kembali menunggu input, ada simbol "manual input" Dapat input dari keypad, jika proses tersebut berjalan berarti pengguna telah menekan keypad sebagai input, kemudian flowchart akan menuju ke connector "B".

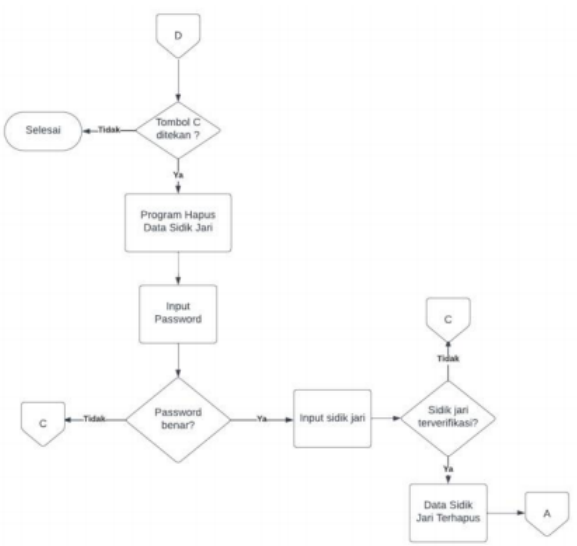


Gambar 4: Flowchart 2

Pada bagian flowchart 2 (Gambar 4) menjelaskan tentang proses input dari keypad. Diawali dengan connector "B" yang sebelumnya program mendapat input dari keypad. Kemudian program akan memerikasa apakah tombol A yang ditekan, jika ya maka akan masuk proses program menambah data sidik jari. Ada decision untuk memeriksa apakah jumlah data sidik jari sudah lebih dari 3, jika ya maka akan berlanjut ke connector "C", jika tidak maka program akan menjalankan input password, program akan menunggu pengguna untuk input password yang sesuai, kemudian decision apakah password benar, jika benar akan masuk proses input sidik jari, pengguna diminta untuk mendaftarkan sidik jari mereka, jika sudah maka sidik jari akan tersimpan dan berlanjut ke connector "A". Jika pada decision "Tombol A ditekan?" itu pilihanya tidak, maka alur flowchart akan ke decision berikutnya yaitu apakah tombol B ditekan, jika iya maka akan masuk proses program ganti password.

Input password lama yaitu pengguna diminta untuk input password lama yang tersimpan, jika ya maka akan masuk ke proses input sidik jari. Pengguna diminta untuk input sidik jari sebagai proses identifikai. Pada decision Sidik Jari Terverifikasi, saat sidik jari didapatkan maka program akan membandingkan sidik jari yang didapatkan dengan sidik jari yang tersimpan, jika sidik jari cocok maka akan berlanjut ke proses input password baru, pengguna akan diminta untuk input password baru sebanyak 4 digit, jika pengguna sudah selesai input password

barunya, maka password akan tersimpan. Kemudian program akan berlanjut ke connector "A" yaitu proses menunggu input.



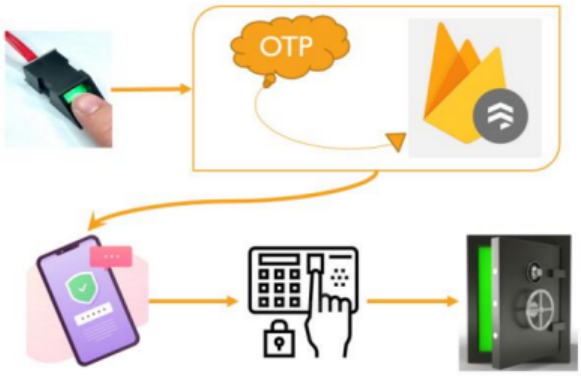
Gambar 5: Flowchart 3

Pada flowchart 3 (Gambar 5) akan menjelaskan untuk alur program keypad saat input yang didapatkan tombol C. Pada decision akan memeriksa apakah tombol C ditekan, jika ya maka akan lanjut ke program hapus data sidik jari, pengguna diminta untuk input password yang sesuai, kemudian decision apakah password yang diinput benar, jika ya maka program akan meminta input sidik jari. Saat sidik jari didapatkan maka program akan membandingkan sidik jari yang didapatkan dengan sidik jari yang tersimpan, jika sidik jari cocok maka berlanjut ke proses Data Sidik Jari Terhapus, yaitu penghapusan seluruh data sidik jari, kemudian program akan menuju connector "A" yaitu menunggu input.

Rancangan Aplikasi

Pada Bagian ini akan dijelaskan perancangan program aplikasi yang akan dibuat. Aplikasi yang akan dibuat memiliki tujuan utama untuk penerimaan kode OTP yang mana kode OTP ini dibuat oleh program mikon yang ada pada brankas. Pada tahap instalasi pertama kali, pengguna diminta untuk memasukkan semacam kode unik sebagai metode login yang hanya tersedia dalam Brankas. Kode unik ini bertindak sebagai kunci penghubung antara aplikasi dan brankas.

Setelah proses login, aplikasi menginisiasi sinkronisasi antara perangkat smartphone dan brankas. Fitur ini memastikan bahwa pengguna memiliki otorisasi yang sah untuk mengakses brankas. Pada layar utama aplikasi, akan terdapat sebuah "label" yang menunjukkan status ketersediaan kode OTP. Kode OTP ini akan berubah jika pengguna menempelkan sidik jari yang terdaftar pada sensor, lihat Gambar 6).



Gambar 6: Cara kerja aplikasi

Hasil Pengujian Sensor Fingerprint

Pengujian Sensor Fingerprint FPM10A dilakukan untuk mengetahui seberapa akurat sensor dapat mendeteksi sidik jari yang terdaftar dan seberapa cepat sensor dapat mendeteksi sidik jari. Pengujian akan dilakukan sebanyak sepuluh kali masing-masing dengan menggunakan 3 sidik jari, diantaranya jempol kiri dan kanan, dan jari telunjuk kanan. Hasil pengujian dapat dilihat pada Tabel 1, 2 dan 3.

Tabel 1: Data Jempol Kiri

Sidik Jari = Jempol Kiri			
Percobaan Ke -	Posisi Jari	Waktu Dideteksi	Hasil (Output LCD)
1	Vertikal (Lurus)	0,5 detik	Terdeteksi
2	Miring(90^0)	0,5 detik	Terdeteksi
3	Terbalik (180^0)	0,7 detik	Terdeteksi
4	Vertikal (Lurus)	0,7 detik	Terdeteksi
5	Miring(90^0)	0,7 detik	Terdeteksi
6	Terbalik (180^0)	1 detik	Terdeteksi
7	Vertikal (Lurus)	1 detik	Terdeteksi
8	Miring(90^0)	1 detik	Terdeteksi
9	Terbalik (180^0)	1 detik	Terdeteksi
10	Vertikal (Lurus)	0,5 detik	Terdeteksi

Tabel 2: Data Jempol Kanan

Sidik Jari = Jempol Kanan			
Percobaan Ke -	Posisi Jari	Waktu Dideteksi	Hasil (Output LCD)
1	Vertikal (Lurus)	0,5 detik	Terdeteksi
2	Miring(90^0)	0,5 detik	Terdeteksi
3	Terbalik (180^0)	0,5 detik	Terdeteksi
4	Vertikal (Lurus)	0,5 detik	Terdeteksi
5	Miring(90^0)	0,7 detik	Terdeteksi
6	Terbalik (180^0)	1 detik	Terdeteksi
7	Vertikal (Lurus)	0,5 detik	Terdeteksi
8	Miring(90^0)	0,5 detik	Terdeteksi
9	Terbalik (180^0)	0,7 detik	Terdeteksi
10	Vertikal (Lurus)	0,5 detik	Terdeteksi

Tabel 3: Data Telunjuk Kanan

Sidik Jari = Telunjuk Kanan			
Percobaan Ke -	Posisi Jari	Waktu Dideteksi	Hasil (Output LCD)
1	Vertikal (Lurus)	0,5 detik	Terdeteksi
2	Miring(90°)	0,5 detik	Terdeteksi
3	Terbalik (180°)	0,5 detik	Terdeteksi
4	Vertikal (Lurus)	0,5 detik	Terdeteksi
5	Miring(90°)	0,5 detik	Terdeteksi
6	Terbalik (180°)	0,5 detik	Terdeteksi
7	Vertikal (Lurus)	0,8 detik	Terdeteksi
8	Miring(90°)	0,5 detik	Terdeteksi
9	Terbalik (180°)	0,8 detik	Terdeteksi
10	Vertikal (Lurus)	0,8 detik	Terdeteksi

Dari Hasil Pengujian pada sensor yang dilakukan maka kita dapat menghitung nilai rata-rata setiap tabel yang didapat dengan menggunakan rumus berikut:

$$Mean = \frac{Jumlah\ Data}{Banyaknya\ Data} \quad (1)$$

Hasil rata-rata yang didapatkan pada tabel 1 atau pengujian data jempol kiri yaitu didapatkan hasil yaitu 0,76, maka rata-rata sensor dapat mendeteksi sidik jari pada jempol kiri setiktar 0,76 detik. Kemudian untuk data jempol kanan dan telunjuk kanan didapatkan hasil 0,59 detik.

Hasil Pengujian Keypad

Pada pengujian keypad dilakukan untuk memeriksa apakah setiap tombol keypad yang ditekan, maka program akan menjalankan perintah yang sudah dibuat. Dalam alat ini tombol keypad yang diprogram ada 5 tombol, yaitu A, B, D, *, #. tombol keypad "*" digunakan untuk menghapus input password yang salah, tombol "#" digunakan untuk kembali ke menu awal.

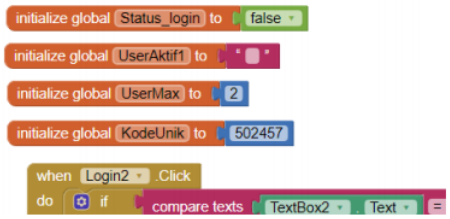
Hasil dari pengujian yaitu setiap tombol pada keypad jika ditekan akan berfungsi sesuai program yang telah dibuat, tetapi pada tombol "#" yang berfungsi untuk kembali ke menu awal kadang tidak berfungsi saat program sedang menjalankan bagian daftar sidik jari dan hapus sidik jari pada bagian menunggu input sidik jari, karna pada waktu tersebut program sedang menunggu input sidik jari dari sensor, jika ingin kembali ke menu awal maka disarankan untuk meng-input sidik jari yang tidak terdaftar, lihat Tabel 4.

Tabel 4: Hasil Pengujian Keypad

Tombol Keypad	Fungsi
A	Daftar Sidik Jari
B	Ganti Password
D	Hapus Data Sidik Jari
#	Kembali ke menu awal
*	Hapus input yang salah

Hasil Pengujian Aplikasi

Pada bagian ini akan dilakukan pengujian dari aplikasi yang telah dibuat. Pada program aplikasi terdapat beberapa fungsi, yaitu fungsi Login, Fungsi mendapatkan kode OTP, fungsi Logout, dan fungsi menyimpan status login.



Gambar 7: Variabel pada program aplikasi

Pada program aplikasi ini menggunakan 4 variabel, diantaranya (lihat Gambar 7):

Variabel Status Login: untuk menyimpan status login pada memori lokal aplikasi

Variabel User Aktif: untuk mengambil data User Aktif dari Firebase

Variabel User Max: sebagai batas login user

Variabel Kode Unik: sebagai Kode atau password untuk masuk ke aplikasi Saat pertama kali aplikasi dibuka, maka pengguna akan diminta untuk memasukan kode atau password untuk masuk ke aplikasi. Jika kode yang dimasukan benar, aplikasi akan menyimpan Status Login dengan mengubah variabel Status login menjadi true. Jika kode yang dimasukan salah, maka akan ada tampilan pop-up "Wrong Code".

Aplikasi ini membutuhkan koneksi internet untuk menghubungkan ke Firebase, data yang diambil dari Firebase ada dua data, yaitu data Jumlah pengguna, dan data kode OTP. Jika aplikasi tidak terhubung ke internet, maka data yang ditampilkan yaitu angka 0, artinya aplikasi tidak dapat terhubung ke Firebase.

Hasil Pengujian OTP

Pengujian OTP dilakukan untuk mengetahui berapa persen kode OTP yang berhasil dikirim ke Firebase setelah sensor sidik jari mendeteksi sidik jari yang terdaftar. Percobaan akan dilakukan sebanyak 10 kali percobaan dengan 3 sidik jari yang berbeda yaitu jempol kiri, jempol kanan, dan telunjuk kanan, lihat Tabel 5.

Dari hasil pengujian yang dilakukan, dapat disimpulkan dalam 10 kali pengujian pengiriman kode OTP, program berhasil mengirim kode OTP ke Firebase dengan tingkat kesuksekan 100%, dan waktu yang dibutuhkan rata-rata sekitar 6,6 detik.

Tabel 5: Data Pengujian OTP

Pengujian OTP			
Percobaan Ke -	Sidik Jari	Waktu pengiriman	Hasil
1	Jempol Kiri	7 detik	Terkirim
2	Jempol Kanan	7 detik	Terkirim
3	Telunjuk Kanan	7 detik	Terkirim
4	Jempol Kiri	6 detik	Terkirim
5	Jempol Kanan	6 detik	Terkirim
6	Telunjuk Kanan	6 detik	Terkirim
7	Jempol Kiri	8 detik	Terkirim
8	Jempol Kanan	6 detik	Terkirim
9	Telunjuk Kanan	7 detik	Terkirim
10	Jempol Kiri	6 detik	Terkirim

Analisis Hasil Keseluruhan

Hasil pengujian sensor sidik jari menunjukkan tingkat akurasi yang memadai dalam pendeteksian sidik jari yang terdaftar. Melalui pengujian ini dengan melibatkan tiga sidik jari yang telah terdaftar, dihasilkan hasil yang cukup konsisten dan akurat. Dalam sepuluh kali percobaan yang dilakukan untuk setiap sidik jari (jempol kiri, jempol kanan, dan telunjuk kanan), didapatkan rata-rata waktu pendeteksian sekitar 0,76 detik untuk jempol kiri, dan 0,59 detik untuk jempol kanan dan telunjuk kanan.

Pengujian pada program keypad menghasilkan hasil yang sesuai dengan ekspektasi. Terdapat lima tombol yang telah diprogram, dengan program utama yang memungkinkan pengguna untuk memasukkan kode OTP setelah sensor mendeteksi sidik jari yang terdaftar. Hasil pengujian ini menunjukkan bahwa program utama berfungsi dengan baik, memungkinkan pengguna untuk masuk ke langkah input kode OTP setelah autentikasi sidik jari berhasil. Namun terkadang, terdeteksi suatu masalah yang perlu diperhatikan. Keypad kadang-kadang tidak dapat mendeteksi tombol yang ditekan, terutama pada kolom bagian kiri keypad yang mencakup tombol 1, 4, 7, dan * (bintang). Untuk mengatasi masalah ini, disarankan untuk melakukan restart pada program Wemos. Dengan melakukan restart ini, diharapkan tombol-tombol tersebut dapat berfungsi kembali secara normal.

Hasil pengujian aplikasi berfokus pada dua halaman pada aplikasi yang dibuat. Halaman pertama adalah halaman login, dimana pengguna diminta memasukkan kode unik yang ada pada brankas untuk mengaksesnya. Ketika kode yang dimasukkan salah, aplikasi memberikan output "wrong password". Namun jika kode benar, pengguna akan diarahkan ke halaman utama. Di halaman utama, terdapat label untuk penerimaan kode OTP. Kode OTP hanya akan berubah ketika pengguna menempelkan sidik jari yang terdaftar pada sensor. Aplikasi ini memerlukan koneksi internet untuk berkomunikasi dengan Firebase. Dari pengujian ini, dapat disimpulkan bahwa aplikasi mampu menerima kode OTP yang dikirimkan dari Firebase, dengan catatan bahwa baik aplikasi dan perangkat harus terhubung ke internet.

Kemudian untuk hasil Pengujian OTP, pengujian ini dilakukan untuk menguji keberhasilan pengiriman kode OTP ke Firebase. Setelah dilakukan pengujian sebanyak 10 kali, program behasil untuk mengirimkan kode OTP ke Firebase. Namun terkadang ditemukan kegagalan dalam mengirimkan kode OTP ke Firebase. Kegagalan ini dipicu oleh pesan error "connection refused" yang muncul di serial monitor pada Arduino IDE. Penyebab error tersebut adalah karena adanya kesalahan dalam koneksi antara aplikasi dan Firebase. Solusi untuk mengatasi error ini adalah memastikan bahwa koneksi internet pada perangkat terjaga dan stabil.

Penutup

Berdasarkan hasil pengujian yang dilakukan, dapat disimpulkan bahwa sistem keamanan brankas yang dikembangkan telah menunjukkan tingkat kinerja yang memadai. Sensor sidik jari mampu mendeteksi sidik jari yang terdaftar dengan akurasi yang tinggi sekitar 0,76 detik, meskipun terdapat beberapa masalah kecil seperti waktu pendeteksian yang bervariasi. Pengujian pada keypad menunjukkan bahwa program utama berfungsi dengan baik, meskipun ada kelemahan dalam mendeteksi beberapa tombol yang ditekan. Aplikasi juga berhasil dalam menerima kode OTP dengan baik dengan rata-rata waktu yang diperlukan untuk mendapatkan kode sekitar 6,6 detik dengan koneksi internet yang stabil.

Pembuatan alat Sistem keamanan Brankas menggunakan sidik jari dan kode OTP masih jauh dari kata sempurna, untuk itu disarankan pengembangan alat ini dengan menambahkan fungsi atau komponen, seperti menambahkan sensor GPS sebagai aplikasi tracker pada brangkas. Kemudian kode OTP yang digunakan pada alat ini tidak memiliki batas waktu, ini memungkinkan kode OTP berisiko dapat diretas atau dicuri oleh pihak yang tidak berwenang, maka dari itu untuk pengembanganya bisa dibuat sistem pengatur waktu saat kode OTP didapatkan, misal kode OTP hanya berlaku 2 menit setelah itu kode OTP tidak dapat digunakan. Untuk pengembangan aplikasi karna aplikasi yang dibuat bertujuan hanya untuk mendapatkan kode OTP dari Firebase, bisa ditambahkan fungsi history atau riwayat, seperti riwayat kapan terakhir kali kode OTP dibuat, kemudian bisa buat fungsi untuk melihat siapa saja dan kapan seseorang telah melakukan pendaftaran sidik jari dan siapa yang telah menghapus data sidik jari.

Daftar Pustaka

[1] Suci Rahmawati, “Simulasi Membuka, Menutup Pintu Dan Menghidupkan Mesin Mobil Menggunakan Android”, Tugas Akhir, Politeknik Negeri Sriwijaya, 2015.

[2] A. W. Finaka, Y. Nurhanisah dan A. Syaifullah, "Mengenal One Time Password (OTP)", Indonesia Baik, diakses daring pada: https://indonesiabaik.id/index.php/infografis/mengenal-one-time-password-otp, 2022.

[3] Erintafifah, "Mengenal Perangkat Lunak Arduino IDE", KMTek, diakses daring pada: https://www.kmtech.id/post/mengenal-perangkat-lunak-arduino-ide, 2021.

[4] G. R. Payara dan R. Tanone, "Penerapan Firebase Realtime Database Pada Prototype Aplikasi Pemesanan Makanan Berbasis Android," J. Tek. Inform. dan Sist. Inf., vol. 4, no. 3, pp. 397–406, doi: 10.28932/jutisi.v4i3.870, 2018.

[5] Admin, "Apa Itu MIT App Inventor, Berikut Penjelasannya. elektronika-dasar-web", Program Studi Teknologi Informasi, UNISA Yogyakarta, diakses daring pada: https://psti.unisayogya.ac.id/2020/01/06/apa-itu-mit-app-inventor-berikut-penjelasannya/ , 2020.

[6] RF. Bagaskara, S.Y. Saputro dan N.Inayah, "Sistem Pintu Otomatis dengan Fingerprint berbasis Arduino Uno. Jurnal Tugas Akhir, Volume I, pp. 1-5, 2019.

[7] T. Wisnuadji, " Brankas dengan Sistem Keamanan", Seminar Nasional Riset dan Inovasi Teknologi (SEMNAS RISTEK) 2022, Volume III, pp. 947-951, 2022.

[8] Heri Ngarianto dan Alexander Agung Santoso Gunawan, "Pengembangan Automatic Pet Feeder Mengunakan Platform BlynkBerbasis Mikrokontroler ESP8266",Engineering, MAthematics and Computer Science Journal (EMACS), Vol 2. No.1, pp: 35-40, 3 April 2020.

[9] Yohanes C Saghoa, "Kotak Penyimpanan Uang Berbasis Mikrokontroler Arduino Uno",Jurnal Teknik Elektro dan Komputer,Vol 7. No 2, Oktober 2018.

[10] M.A. Baaqi dan S.P.F.R. Dito, Sistem Keamanan Kotak Amal Anti Maling Berbasis Arduino", Tugas Akhir Diploma Teknik Komputer, Tegal: Politeknik Harapan Bersama, 2019.