PERANCANGAN PURWARUPA SISTEM KEAMANAN BRANKAS MENGGUNAKAN VERIFIKASI BIOMETRIK SIDIK JARI DENGAN INTEGRASI PADA APLIKASI TELEGRAM

[1]*Jonathan M. Christiano**,[2]*Susilo*, [3]*Stepanus*
[1,2,3] *Program Studi Teknik Elektro Fakultas Teknik Universitas Kristen Indonesia,*
[1,2,3] *Jl. Mayjen Sutoyo No.2 Cawang, Jakarta Timur 13630, DKI Jakarta*
**Corresponding author.* [1]jonathanmccc1@gmail.com

Abstrak

Keamanan aset berharga merupakan aspek penting dalam sistem penyimpanan seperti brankas guna mencegah akses tidak sah dan pembobolan. Sistem keamanan konvensional yang menggunakan kunci mekanis atau kombinasi angka memiliki keterbatasan dari sisi keamanan dan kepraktisan, sehingga diperlukan solusi yang lebih andal. Penelitian ini bertujuan untuk merancang dan merealisasikan sistem keamanan brankas berbasis biometrik sidik jari yang terintegrasi dengan aplikasi Telegram berbasis Internet of Things (IoT) sebagai media monitoring dan notifikasi jarak jauh. Sistem menggunakan mikrokontroler NodeMCU ESP8266 sebagai pengendali utama, sensor sidik jari AS608 sebagai media autentikasi, relay sebagai penghubung aktuator, serta solenoid door lock sebagai mekanisme pengunci. Telegram dimanfaatkan untuk mengirimkan notifikasi secara real-time saat terjadi akses berhasil maupun gagal. Metode Research and Development (R&D) diterapkan melalui tahapan perancangan, implementasi, dan pengujian sistem. Hasil pengujian menunjukkan bahwa sistem mampu mengenali sidik jari terdaftar dengan tingkat keberhasilan 100%, dengan ratarata waktu respons pengenalan 3,600 detik dan pengiriman notifikasi 3,470 detik. Berdasarkan hasil tersebut, sistem yang dikembangkan mampu meningkatkan keamanan brankas dan memudahkan pemantauan jarak jauh.

***Kata Kunci**: Brankas, Sidik Jari, Internet of Things, Telegram*

Abstract

The security of valuable assets is an important aspect of safe storage systems to prevent unauthorized access and burglary. Conventional security methods using mechanical keys or numeric combinations have limitations in terms of security and usability, thus requiring a more reliable solution. This research aims to design and implement a fingerprint biometric-based safe security system integrated with the Telegram application using Internet of Things (IoT) technology for remote monitoring and notification. The system utilizes a NodeMCU ESP8266 microcontroller as the main controller, an AS608 fingerprint sensor for authentication, a relay module, and a solenoid door lock as the locking mechanism. Telegram is used to deliver real-time notifications to users for both successful and failed access attempts. The Research and Development (R&D) method is applied, covering system design, implementation, and testing. Experimental results show that the system successfully recognizes registered fingerprints with a 100% success rate. The average fingerprint recognition response time is 3.600 seconds, while the notification delivery time via Telegram is 3.470 seconds. These results indicate that the developed system enhances safe security and enables effective remote monitoring.

***Keywords**: Safe, Fingerprint, Internet of Things, Telegram*

PENDAHULUAN

Keamanan aset berharga sangat penting untuk mencegah pencurian. Pada masa lalu, aset seperti uang dan surat berharga disimpan di lemari, namun cara ini kurang aman karena mudah dibobol. Seiring perkembangan teknologi, digunakan brankas sebagai solusi penyimpanan yang lebih aman dengan sistem pengunci. Saat ini, brankas umumnya menggunakan PIN atau kombinasi angka. Namun penggunaan sistem penguncian tersebut kurang efisien dikarenakan pengguna terkadang lupa akan pin dari kombinasi brankas tersebut [1]. Kekurangan tersebut berpotensi diretas oleh pihak yang tidak bertanggung jawab.

Perkembangan teknologi memungkinkan peningkatan sistem keamanan brankas, salah satunya melalui Internet of Things (IoT). Dengan sistem Internet of Things (IoT) pengguna dapat memantau dan mengendalikan secara realtime alat-alat rumah yang terkoneksi [2]. Sistem ini juga dapat dikombinasikan dengan sensor lain, seperti sensor biometrik, untuk meningkatkan keamanan.

Penelitian oleh Yuda Irawan dkk. (2022) berjudul *"Sistem Keamanan Smart Brankas Menggunakan Fingerprint Android"*[3] membahas permasalahan pengguna yang sering lupa, kehilangan kunci, atau lupa kata sandi sehingga gagal mengakses brankas. Penelitian ini menggunakan metode prototype dan menghasilkan sistem keamanan otomatis berbasis sidik jari melalui aplikasi smartphone. Namun, sistem ini memiliki kelemahan karena tidak mendukung monitoring jarak jauh dan menggunakan koneksi Bluetooth yang rentan terhadap gangguan.

Penelitian oleh Fahmi Rabbani dkk. (2019) berjudul *"Sistem Pengaman Brankas Berbasis GPS Tracking & IoT"*[4] membahas tingginya tingkat kriminalitas dan keterbatasan keamanan brankas komersial. Penelitian ini menggunakan metode R&D dan menghasilkan sistem keamanan brankas berbasis IoT dengan pemantauan jarak jauh melalui aplikasi Blynk, dilengkapi alarm saat pembobolan serta modul GPS dan SIM A6 untuk notifikasi SMS dan pelacakan lokasi. Namun, sistem ini belum dilengkapi mekanisme autentikasi yang kuat untuk meningkatkan keamanan.

Penelitian oleh Moh. Muthohir dan Sendi Prayogi (2021) berjudul *"Prototype Sistem Keamanan Brankas Menggunakan Teknologi RFID Berbasis Arduino Uno"*[5] membahas kelemahan sistem brankas berbasis kombinasi nomor yang kurang efektif. Penelitian ini menggunakan metode R&D dan menghasilkan prototype sistem keamanan berbasis RFID. Hasil pengujian menunjukkan sistem bekerja sesuai harapan, namun disarankan penambahan UPS agar tetap berfungsi saat listrik padam serta proteksi tambahan untuk mengantisipasi kehilangan tag RFID.

Berdasarkan penelitian sebelumnya, penerapan teknologi keamanan seperti fingerprint, RFID, dan GPS tracking pada brankas masih memiliki berbagai kelemahan. Beberapa di antaranya adalah keterbatasan sistem monitoring jarak jauh, rentannya koneksi Bluetooth, kegagalan sistem, serta belum optimalnya mekanisme otentikasi. Selain itu, kebutuhan akan sumber daya cadangan seperti UPS dan proteksi tambahan terhadap kehilangan media akses juga menjadi perhatian penting.

Oleh karena itu, penelitian ini mengusulkan pengembangan sistem keamanan brankas berjudul *"Perancangan Purwarupa Sistem Keamanan Brankas Menggunakan*

Verifikasi Biometrik Sidik Jari dengan Integrasi pada Aplikasi Telegram". Sistem ini menggunakan otentikasi biometrik berupa pemindaian sidik jari berbasis Internet of Things (IoT) dengan sensor AS608 yang mampu mengambil gambar sidik jari dalam waktu kurang dari satu detik.

Sistem keamanan yang dikembangkan juga terintegrasi dengan aplikasi Telegram sebagai media monitoring jarak jauh yang memberikan notifikasi secara real-time. Pendekatan ini diharapkan dapat mengatasi kelemahan penelitian sebelumnya serta menghasilkan sistem keamanan brankas yang lebih aman, efisien, dan responsif bagi pengguna.

KERANGKA TEORI

2.1 Teori Umum

2.1.1 Brankas

Brankas adalah lemari atau kotak besi yang dirancang untuk melindungi barang berharga, dokumen penting, dan aset dari pencurian, kebakaran, serta kerusakan lainnya[6]. Umumnya terbuat dari baja tahan api dan dilengkapi sistem penguncian seperti kombinasi mekanis, kunci elektronik, hingga biometrik. Istilah "brankas" berasal dari bahasa Belanda *Brandenkast* yang berarti lemari tahan api. Penggunaannya meliputi rumah, kantor, hingga institusi keuangan.

Jenis brankas dibedakan berdasarkan fungsi dan ketahanannya, seperti brankas baja yang fokus pada perlindungan fisik, brankas tahan api untuk perlindungan dari kebakaran, serta brankas tahan api dan dobrak yang memiliki perlindungan paling tinggi. Secara fisik, brankas juga bervariasi dari yang portabel hingga tertanam di dinding atau lantai.

Perkembangan brankas telah berlangsung sejak lama dan mengalami kemajuan pesat pada abad ke-19 seiring perkembangan teknologi metalurgi dan mekanika[7]. Sistem penguncian pun terus berkembang dari kunci tradisional hingga teknologi modern seperti PIN digital dan sidik jari. Saat ini, brankas tidak hanya berfungsi sebagai tempat penyimpanan, tetapi juga sebagai sistem keamanan utama yang terus disempurnakan mengikuti perkembangan teknologi.



Gambar 2. 1 Brankas

Sumber : https://sl.bing.net/hWcz3upNlfM

2.1.2 Sistem Keamanan Brankas

Sistem keamanan brankas merupakan aspek penting dalam melindungi barang berharga dari pencurian dan akses tidak sah, yang telah berkembang dari metode konvensional ke teknologi modern. Sistem tradisional menggunakan kombinasi roda angka yang mengandalkan mekanisme kompleks, namun masih rentan jika kode diketahui atau dibobol dengan alat tertentu.

Perkembangan teknologi menghadirkan sistem elektronik dan biometrik seperti sidik jari, pengenalan wajah, serta PIN atau OTP. Penggabungan verifikasi ganda, misalnya sidik jari dan OTP, terbukti meningkatkan keamanan dan membatasi akses hanya bagi pengguna terdaftar[8].

Pada sistem modern, sidik jari pengguna diverifikasi dengan data tersimpan, kemudian dilanjutkan dengan pengiriman kode OTP sebagai autentikasi tambahan. Proses ini dikendalikan mikrokontroler yang mengaktifkan

aktuator seperti solenoid atau motor servo untuk membuka brankas. Sistem juga dilengkapi alarm atau notifikasi sebagai peringatan terhadap upaya pembobolan[9].

2.1.3 Sistem Cerdas

Sistem cerdas atau *artificial intelligence* (AI) merupakan bidang ilmu komputer yang berfokus pada pengembangan mesin yang mampu meniru kemampuan manusia dalam berpikir, belajar, dan mengambil keputusan[10]. Sistem ini dapat memproses data dengan kecepatan dan akurasi tinggi melalui berbagai pendekatan seperti pembelajaran mesin, pengenalan pola, sistem pakar, pengolahan bahasa alami, dan robotika.

Pada dasarnya, sistem cerdas mengotomatisasi aktivitas kognitif manusia menggunakan algoritma dan model matematis, serta memiliki kemampuan belajar dari pengalaman (*machine learning*) sehingga dapat beradaptasi tanpa intervensi langsung. Teknologi ini banyak diterapkan pada berbagai bidang, seperti sistem rekomendasi, diagnosa medis, kontrol otomatis, dan sistem keamanan canggih.

2.1.4 Biometrik

Biometrik adalah metode identifikasi dan verifikasi individu berdasarkan karakteristik biologis atau perilaku yang unik, seperti sidik jari, wajah, retina, iris, suara, dan pola tangan[11]. Metode ini bekerja dengan mengambil data biometrik, mengekstraksi fitur, lalu mencocokkannya dengan template yang tersimpan dalam database[12].

Teknologi biometrik banyak digunakan dalam sistem keamanan untuk mengontrol akses, seperti pada pintu, lemari penyimpanan, atau brankas, guna memastikan hanya individu yang berwenang yang dapat mengaksesnya.



Gambar 2. 2 Metode Biometrik

Sumber : https://pin.it/1MpRf9GES

2.1.4 Fingerprint

Fingerprint (sidik jari) adalah metode identifikasi dengan mengambil gambar pola unik pada kulit jari manusia[13]. Teknologi ini awalnya digunakan pada sistem keamanan ponsel, namun kini berkembang luas pada berbagai aplikasi seperti kunci pintu pintar, identifikasi identitas, dan sistem absensi.

Penggunaan fingerprint terus meningkat karena tingkat keamanannya tinggi, mengingat setiap individu memiliki pola sidik jari yang unik sehingga dapat merepresentasikan karakteristik masing-masing pengguna.



Gambar 2. 3 Sidik Jari

Sumber : https://sl.bing.net/eHMN1RP1tAG

2.1.5 Internet of Things (IoT)

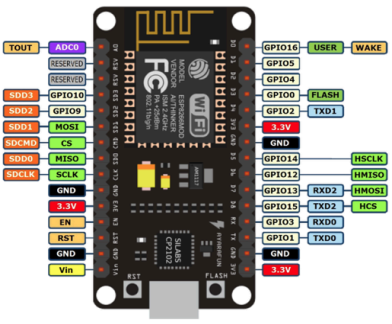
Internet of Things (IoT) merupakan konsep yang memanfaatkan konektivitas internet secara terus-menerus

untuk menghubungkan berbagai perangkat, sehingga dapat mempermudah aktivitas sehari-hari melalui sistem cerdas. IoT mencakup integrasi perangkat seperti sensor, aktuator, dan perangkat lunak yang saling terhubung dan dapat dikendalikan atau dipantau secara otomatis[14].

2.2 Teori Perangkat Keras

2.2.1 NodeMCU ESP8266

Mikrokontroler adalah sistem komputer mini dalam satu chip yang mencakup CPU, memori, dan input/output, serta berfungsi sebagai pengendali utama dalam perangkat elektronik, khususnya pada proyek IoT. Salah satu contohnya adalah NodeMCU yang memiliki keunggulan pada konektivitas WiFi dan pin GPIO yang mendukung berbagai sensor dan aktuator. NodeMCU ESP8266 merupakan mikrokontroler populer untuk pengembangan IoT karena fungsinya yang beragam dan biaya yang relatif murah. Modul ini dilengkapi koneksi WiFi terintegrasi tanpa perangkat tambahan, serta memori sebesar 4 MB yang dapat diprogram menggunakan Arduino IDE untuk menjalankan berbagai tugas secara bersamaan.

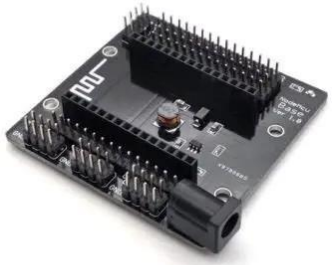


Gambar 2. 4 NodeMCU ESP8266

Sumber : https://sl.bing.net/eySIWmOI72q

2.2.2 Expansion Board NodeMCU

Expansion board adalah komponen tambahan yang digunakan untuk memperluas fungsi NodeMCU dan dirancang agar dapat dipasang langsung pada modul tersebut.



Gambar 2. 5 Board Expansion NodeMCU

Sumber : https://sl.bing.net/i8mgnzTf92W

2.2.3 Sensor Fingerprint AS608

Sensor fingerprint AS608 adalah modul pemindai sidik jari yang populer dalam proyek IoT dan dapat terintegrasi dengan mikrokontroler seperti NodeMCU, ESP32, atau Arduino. Sensor ini mampu menyimpan hingga 120 rekaman sidik jari, mendukung deteksi dan verifikasi pengguna. Dengan tingkat penerimaan palsu (FAR) <0,001%, kemungkinan sensor ditipu oleh sidik jari tidak terdaftar sangat kecil, meskipun tingkat penolakan palsu (FFR) tetap memungkinkan kegagalan identifikasi akibat kesalahan teknis atau pemindaian.



Gambar 2. 6 Sensor Fingerprint AS608

Sumber : https://sl.bing.net/j9K4iargT3A

2.2.4 Selenoid Doorlock

Solenoid doorlock adalah aktuator elektromagnetik yang digunakan untuk sistem penguncian pintu otomatis. Komponen ini bekerja dengan tegangan DC 12 volt untuk menghasilkan gaya

magnet yang menggerakkan pin pengunci sehingga pintu dapat dibuka atau dikunci secara elektrik.



Gambar 2. 7 Solenoid Doorlock

Sumber : https://sl.bing.net/h6T9EskHZW8

2.2.5 Relay

Relay merupakan komponen yang berfungsi sebagai saklar listrik yang dikendalikan oleh sinyal listrik, bekerja berdasarkan prinsip elektromagnetik dimana arus listrik pada kumparan menghasilkan medan magnet untuk menarik kontak mekanis sehingga terjadi perubahan kondisi terbuka atau tertutup (NO/NC). Relay 5V 1 Channel adalah komponen yang bekerja pada tegangan 5V DC dengan satu jalur pengendali, dirancang untuk memudahkan kontrol menggunakan sinyal dari mikrokontroler.



Gambar 2. 8 Relay

Sumber : https://sl.bing.net/ebB2dwt83Cm

2.2.6 Buzzer

Buzzer merupakan perangkat elektronik yang berfungsi sebagai alat keluaran (output) yang menghasilkan suara sebagai penanda atau peringatan pada kondisi tertentu, dan umum digunakan pada sistem keamanan, alarm, serta sistem berbasis mikrokontroler. Prinsip kerjanya adalah saat arus listrik dialirkan, kumparan (coil) bergetar dan menghasilkan gelombang suara yang dapat didengar manusia.



Gambar 2. 9 Buzzer

Sumber : https://sl.bing.net/gvZ6Z9U3fgW

2.2.7 Adaptor

Adaptor adalah perangkat catu daya yang mengubah tegangan listrik AC 220V menjadi DC 12V sesuai kebutuhan. Adaptor 12V/1A menghasilkan output 12V dengan arus maksimum 1A, dan banyak digunakan pada berbagai perangkat elektronika seperti mikrokontroler, motor DC, solenoid doorlock, dan lainnya.



Gambar 2. 10 Adaptor

Sumber : https://sl.bing.net/h6b974YrPci

2.2.9 Kabel Jumper

Kabel jumper adalah kabel penghantar listrik yang digunakan untuk menghubungkan titik pada rangkaian

elektronik, baik sementara maupun permanen. Kabel ini terdiri dari tiga jenis yaitu male-male, male-female, dan female-female, tersedia dalam berbagai ukuran seperti 10 cm dan 20 cm, serta banyak digunakan pada breadboard dan modul mikrokontroler karena mudah dipasang tanpa penyolderan.



Gambar 2. 11 Kabel Jumper

Sumber : https://sl.bing.net/cpBf7bJmoSW

2.3 Teori Perangkat Lunak

2.3.1 Arduino IDE

Arduino IDE merupakan software yang berisi editor teks untuk menulis kode, area pesan, konsol, toolbar, dan menu. Software ini dapat terhubung ke mikrokontroler melalui kabel data untuk mengunggah program dan berkomunikasi dengannya[15]. Fungsi utamanya adalah menyediakan platform untuk membuat kode dalam pengembangan sistem otomasi atau perangkat terhubung, serta mendukung berbagai tingkat pengguna dari pelajar hingga profesional.

2.3.2 Telegram

Telegram adalah aplikasi layanan pesan instan berbasis cloud yang berfokus pada kecepatan dan keamanan[16], serta dapat mengirim pesan, foto, video, dan dokumen. Dalam proyek IoT, Telegram digunakan untuk interaksi real-time melalui chatbot, seperti menerima notifikasi status perangkat, mengirim perintah jarak jauh, dan monitoring data sensor dengan memanfaatkan API yang disediakan.

2.3.3 Chatbot Telegram

Chatbot adalah program yang dirancang untuk berinteraksi dengan pengguna melalui percakapan otomatis berbasis teks, juga dikenal sebagai bot. Bot Telegram merupakan program yang berjalan di dalam Telegram dan dibuat oleh pengembang menggunakan API Bot Telegram[17]. Dengan API tersebut, pengembang dapat membuat bot sesuai kebutuhan dan fungsinya.

2.3.4 Telegram Bot API

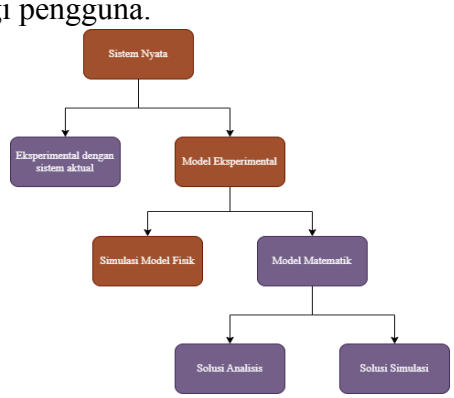
Bot API adalah antarmuka berbasis HTTP yang digunakan pengembang untuk membangun bot Telegram[18], dengan fitur seperti mengirim pesan, menerima pembaruan, mengatur webhook, serta mengelola berbagai konten. Mekanisme kerjanya menggunakan dua metode utama, yaitu long polling (mengambil pembaruan secara berkala dengan getUpdates) dan webhook (server Telegram mengirim pembaruan ke URL yang ditentukan). Integrasi ini memungkinkan bot terhubung dengan sistem eksternal, termasuk IoT, sehingga pengguna dapat melakukan kontrol dan monitoring secara real-time melalui Telegram.

METODE PENELITIAN

3.1 Metodologi Penelitian

Penelitian ini menggunakan metode kuantitatif dengan uji eksperimental melalui pendekatan R&D yang berfokus pada perancangan dan pembuatan purwarupa sistem keamanan brankas. Penelitian dilengkapi metode observasi dan pengujian alat untuk menganalisis kinerja sistem sehingga diperoleh

kesimpulan akhir dan sistem yang efisien bagi pengguna.

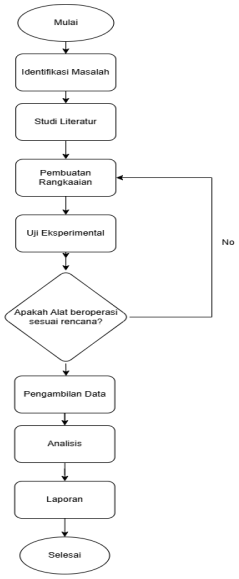


Gambar 3. 1 Metode Penelitian Simulasi

Sumber : Susilo, S., & Abadi, S. (2021). Modeling an Intelligent Agriculture System Simulation Based on Mobile Cloud Internet of Things (IoT). *Lektrokom : Jurnal Ilmiah Teknik Elektro*, *4*(1), 10. https://doi.org/10.33541/lektrokom.v4i1.3378

3.2 Tahapan Penelitian

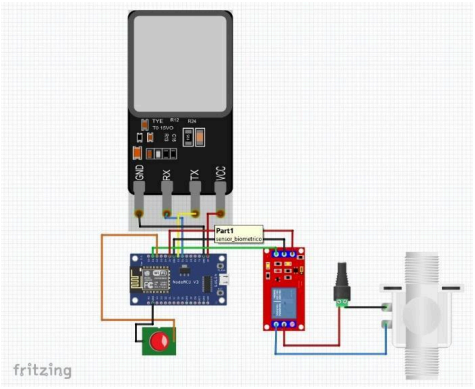
Penelitian ini dilakukan melalui beberapa tahapan, yaitu identifikasi masalah, studi literatur, perancangan dan pembuatan alat, pengembangan program, serta pengujian sistem. Data yang diperoleh dari seluruh tahapan kemudian diolah untuk menghasilkan kesimpulan akhir sesuai alur penelitian.



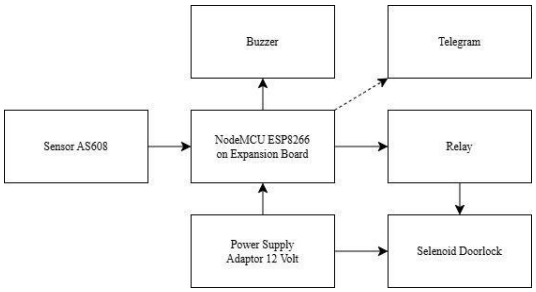
Gambar 3. 2 Alur Tahapan Penelitian

3.3 Perancangan Sistem dan Cara Kerja sistem

Saat sistem dijalankan, NodeMCU ESP8266 terhubung ke jaringan WiFi dan mengirim notifikasi ke Telegram bahwa sistem brankas aktif dan siap digunakan. Pengguna kemudian melakukan pemindaian sidik jari menggunakan sensor AS608. Jika sidik jari terdaftar, sistem mengaktifkan buzzer singkat, membuka solenoid melalui relay selama 3 detik, dan mengirim notifikasi pembukaan brankas ke Telegram. Jika sidik jari tidak terdaftar, buzzer berbunyi lebih lama, solenoid tidak aktif, dan Telegram mengirim pesan "Akses Ditolak".



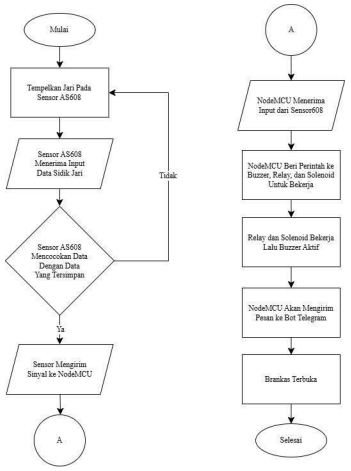
Gambar 3. 3 Rangkaian pada Fritzing



Gambar 3. 4 Blok Diagram

Pengguna dapat mengecek status sistem dengan mengirim perintah /status pada bot Telegram untuk memastikan sistem dalam kondisi normal. Untuk menambahkan sidik jari baru, pengguna mengirim perintah /enroll dengan ID tertentu, lalu mengikuti instruksi dari bot

hingga proses pendaftaran berhasil. Setelah sidik jari terdaftar, sistem akan membuka brankas secara otomatis dan mengirim notifikasi melalui Telegram.



Gambar 3. 5 Alur Kerja Sistem

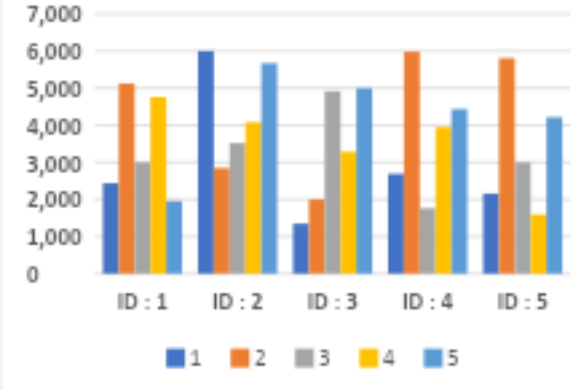
HASIL DAN PEMBAHASAN

4.1 Pengujian Fungsional Sistem

4.1.1 Pengujian Pada Saat Kondisi Sidik Jari Terdaftar

Pengujian ini dilakukan untuk mengetahui berapa lama sensor sidik jari AS608 untuk memindai sidik jari. Adapun yang diuji pada pengujiann ini yaitu Relay, Buzzer, dan Respons Time pada saat jari menmpel pada sidik jari. Sample yang pakai adalah sidik jari Jonathan M. Christiano (Penulis)

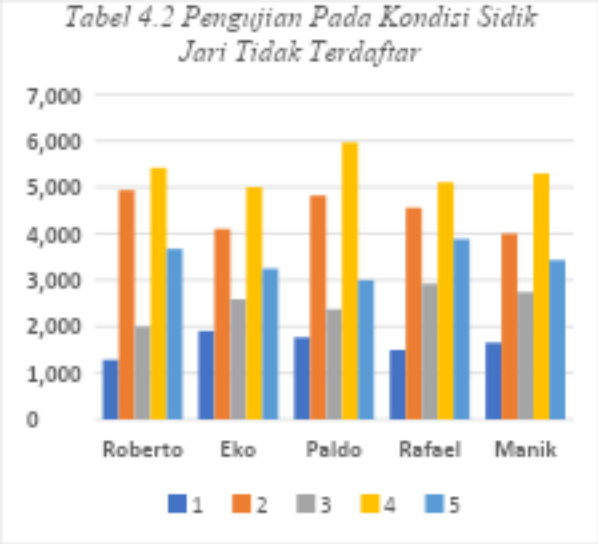
Tabel 4.1 Pengujian Pada Kondisi Sidik Jari Terdaftar



4.1.2 Pengujian Pada Kondisi Sidik Jari Tidak Terdaftar

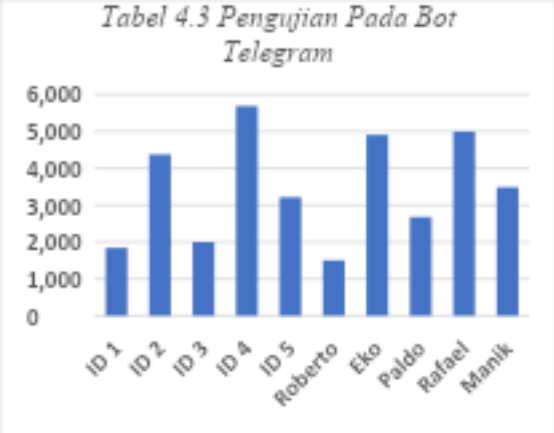
Pengujian ini dilakukan dengan tujuan membuktikan bahwa pada saat kondisi sidik jari yang tidak terdaftar sistem akan menolak dan pintu brankas tidak terbuka. Aspek yang diuji masih sama dengan pengujian sebelumnya dan respons time juga pada saat sidik jari tertempel pada sensor. Sample yang digunakan yaitu sidik jari Roberto, Eko, Paldo, Rafael, dan Manik.

Tabel 4.2 Pengujian Pada Kondisi Sidik Jari Tidak Terdaftar



4.1.3 Pengujian Pada Chat Bot Telegram

Pengujian ini dilakukan bertujuan untuk mengetahui lama waktu pesan terkirim di chat bot Telegram pada saat pemindaian sidik jari. Pengujian ini bertujuan untuk mengetahui tingkat efektifitas pemberitahuan pada Telegram. Aspek yang dipakai dalam pengujian ini adalah status dan respons time. Sample yang digunakan masih sama, sidik jari yang terdaftar dan satu sample sidik jari tidak terdaftar.



4.2 Pengolahan Data

Hasil pengujian menunjukkan bahwa sensor AS608 berhasil memindai sidik jari terdaftar dengan tingkat keberhasilan 100%, ditandai dengan aktifnya relay, buzzer, dan terbukanya brankas pada seluruh percobaan. Sistem memiliki waktu respons rata-rata 3,662 detik yang menunjukkan kinerja cukup responsif untuk penggunaan nyata.

Pengujian pada sidik jari tidak terdaftar menunjukkan bahwa sensor AS608 mampu membedakan sidik jari dengan baik dan seluruh percobaan berhasil menolak akses tanpa mengaktifkan relay maupun solenoid. Sistem memiliki waktu respons rata-rata 3,538 detik dalam proses pencocokan sidik jari.

Pengujian chatbot Telegram menunjukkan bahwa sistem mampu mengirim notifikasi pada kondisi sidik jari terdaftar maupun tidak terdaftar, dengan waktu respons rata-rata sebesar 3,470 detik.

SIMPULAN DAN SARAN

5.1 Simpulan

Penelitian ini berhasil merancang dan mengimplementasikan purwarupa sistem keamanan brankas berbasis biometrik menggunakan NodeMCU ESP8266, sensor sidik jari AS608, relay, dan solenoid door lock yang mampu mengenali identitas pengguna dengan akurasi 100% pada seluruh pengujian. Integrasi dengan API Telegram juga berhasil direalisasikan sehingga sistem dapat mengirimkan notifikasi status akses, baik berhasil maupun gagal, beserta identitas pengguna dengan rata-rata waktu respons 3,470 detik. Selain itu, sistem menunjukkan rata-rata waktu respons pengenalan sidik jari sebesar 3,600 detik, sehingga mampu meningkatkan keamanan brankas melalui autentikasi biometrik serta pemberian informasi secara cepat kepada pemilik. Hasil penelitian menunjukkan bahwa sistem telah memenuhi tujuan penelitian, yaitu merancang, mengintegrasikan, dan mengevaluasi kinerja sistem keamanan berbasis biometrik secara efektif.

5.2 Saran

Pengembangan penelitian selanjutnya disarankan dengan menambahkan fitur delete ID dan sistem blokir otomatis untuk meningkatkan keamanan, mengintegrasikan metode autentikasi tambahan seperti face recognition, menambahkan push button sebagai solusi saat terjadi kegagalan pemindaian sidik jari berulang, serta meningkatkan kualitas konektivitas sistem agar lebih stabil dan andal.

DAFTAR PUSTAKA

[1] Mahesa, A. T., Rahmawan, H., Rinharsah, A., & Arifin, S. (2019). Sistem Keamanan Brankas Berbasis Kartu Rfid E-Ktp. *Jurnal Teknologi dan Manajemen Informatika*, *5*(1).

[2] Arafat, A. (2016). Sistem pengamanan pintu rumah berbasis Internet Of Things (IoT) dengan ESP8266. *Technologia: Jurnal Ilmiah*, *7*(4).

[3] Irawan, Y., Wahyuni, R., Rahmawati, D., & Saputra, H. T. (2022). Sistem keamanan smart brankas menggunakan fingerprint android. *JSR: Jaringan Sistem Informasi Robotik*, *6*(1), 14-19.

[4] Rabbani, F., Resab, M. K., & Wicaksono, R. (2019). Sistem Pengamanan Brankas Berbasis GPS Tracking & IoT (Internet of Things). *Autocracy: Jurnal Otomasi, Kendali, dan Aplikasi Industri*, *6*(01), 36-42.

[5] Muthohir, M., & Prayogi, S. (2021). Prototype Sistem Keamanan Brankas Menggunakan Teknologi RFID Berbasis Arduino Uno. *Jurnal Manajemen Informatika & Teknologi*, *1*(2), 97-106.

[6] https://id.wikipedia.org/wiki/Brankas

[7] https://jogjacagar.jogjaprov.go.id/detail/3772/brankas-b-di-bangsal-sewokoprojo

[8] Mahligai, A. A., Iksan, N., Gunoto, P., & Panessai, I. Y. (2022). Perancangan Sistem Keamanan Brankas dengan Verifikasi Password dan Sidik Jari Berbasis IOT. *Sigma Teknika*, *5*(1), 100-107.

[9] Ramadhan, H. I., & Supriyanto, R. (2024). Prototype sistem keamanan brankas berbasis sensor sidik jari. *Jurnal Ilmiah KOMPUTASI*, 23(1), 131–138.

[10] Muttaqin, Yuswardi, Parewe, A. M. A. K., Ashari, I. F., Nurzaenab, Munsarif, M., Wahyuddin, S., Pasnur, Rahmah, S. A., Defiariany, Gustiana, Z., Fadhillah, Y., Sinambela, M., Hakim, L., Yanto, G., Syahrani, A., & Siregar, M. N. H. (2023). *Pengantar sistem cerdas*. Yayasan Kita Menulis. ISBN 978-623-342-758-6.

[11] Alrawili, R., AlQahtani, A. A. S., & Khan, M. K. (2024). *Comprehensive survey: Biometric user authentication—Application, evaluation, and discussion*. Preprint manuscript submitted for publication.

[12] A. K. Jain, A. Ross and S. Prabhakar, "An introduction to biometric recognition," in IEEE Transactions on Circuits and Systems for Video Technology, vol. 14, no. 1, pp. 4-20, Jan. 2004, doi: 10.1109/TCSVT.2003.818349.
keywords: {Biometrics;Character recognition;Fingerprint recognition;Robustness;Privacy;Humans;Law enforcement;Databases;Co

mputer science;Pattern recognition},

[13] Yu, Y., Niu, Q., Li, X., Xue, J., Liu, W., & Lin, D. (2023). A review of fingerprint sensors: Mechanism, characteristics, and applications. *Micromachines*, *14*(6), 1253.

[14] Mantik, H. (2022). Revolusi industri 4.0: Internet of things, implementasi pada berbagai sektor berbasis teknologi informasi (bagian 1). *Jurnal Sistem Informasi (JSI)*, *9*(2), 41-48.

[15] (2024). Arduino.cc. https://docs.arduino.cc/software/ide-v1/tutorials/Environment/

[16] Telegram FAQ. (2021). Telegram. https://telegram.org/faq#q-apa-itu-telegram-apa-yang-saya-lakukan-di-sini

[17] Telegram. (n.d.). *How do I create a bot?* In *Telegram FAQ*. Retrieved February 27, 2026, from

[18] Telegram. (n.d.). *Telegram APIs*. Retrieved February 27, 2026, from