Sigma Teknika, Vol. 5, No.1 : 100-107
Juni 2022
E-ISSN 2599-0616
P ISSN 2614-5979

PERANCANGAN SISTEM KEAMANAN BRANKAS DENGAN VERIFIKASI PASSWORD DAN SIDIK JARI BERBASIS IOT

Andi Aziz Mahligai[1)], Nur Iksan[2)], Pamor Gunoto[3)], Ismail Yusuf Panessai[4)]
[1,2,3)] Teknik Elektro, Fakultas Teknik, Universitas Riau Kepulauan, Indonesia
[4)] Department of Computing, Faculty of Art, Computing and Creative Industry, Universiti Pendidikan Sultan Idris, Malaysia
E-mail: aazizm.aam@gmail.com [1)], nur.iksan@ft.unrika.ac.id [2)], pamorgunoto@ft.unrika.ac.id[3)], ismailyusuf@fskik.upsi.edu.my[4)]

ABSTRAK

Brankas adalah salah satu sasaran kejahatan tindak pencurian. Dengan kemajuan teknologi saat ini, bagian-bagian tubuh kita dapat dijadikan identitas yang unik sehingga dapat digunakan sebagai sistem keamanan akses. Metode ini cukup baik karena sistem keamanan dapat mengenali langsung ciri-ciri fisik pemilik saat membuka brankas. Dalam hal ini penulis membuat perancangan sistem keamanan brankas dengan verifikasi password dan sidik jari berbasis IoT. Sistem ini menggunakan interlock kombinasi, yaitu fingerprint scanner tidak berfungsi sebelum memasukkan password. Selanjutnya alarm akan berbunyi dan sistem akan mengirimkan notofikasi pesan telegram ke ponsel pemilik brankas jika terjadi kesalahan lebih dari tiga kali saat memasukkan password atau pada saat pemindaian sidik jari, begitu juga saat pintu brankas terbuka dan saat power supply utama brankas terputus untuk menghindari kemungkinan brankas berpindah saat terjadi pencurian. Keypad dan fingerprint scanner sebagai akses pembuka pintu brankas. NodeMcu V3 sebagai media pengiriman data dari sistem mikrokontroler ke ponsel pemilik brankas untuk memberi informasi kepada pemilik brankas jika terjadi upaya pembobolan brankas oleh orang lain. Layar LCD sebagai panduan dalam proses membuka pintu brankas. Dari pembuatan alat ini, diharapkan jika ada seseorang yang ingin membobol brankas akan dengan mudah diketahui dan lebih menjaga keamanan.

Kata kunci : Internet of Things (IoT); keypad; fingerprint scanner; interlock

ABSTRACT

The safe box is one of the targets of theft crimes. With today's technological advances, the parts of our bodies can be used as unique identities so that they can be used as system access. This method is quite good because the security system can immediately recognize the physical characteristics of the owner when opening the safe. In this case the authors make a safe box security system with passwords and fingerprints verification based on IoT. This system uses a combination interlock where the fingerprint scanner cannot perform a fingerprint scan without entering a password. Then the alarm will sound, and the system will send a telegram message notification to the safe owner's cell phone if there is an error more than three times when entering the password or during fingerprint scanning, as well as when the safe door is open and when the safe lose of primary power supply to avoid the possibility of the safe moving when there is a theft. Keypad and fingerprint scanner to open the safe door. NodeMcu V3 as a medium for sending data from the microcontroller system to the safe owner's cell phone to provide information to the safe owner in the event of an attempt to break into the safe by someone else. LCD screen as a guide in the process of opening the safe door. From the manufacture of this tool, it is hoped that if someone who wants to break into a safe will be easily identified and maintain more security.

Keyword : Internet of Things (IoT); keypad; fingerprint scanner; interlock

Sigma Teknika, Vol. 5, No.1 : 100-107
Juni 2022
E-ISSN 2599-0616
P ISSN 2614-5979

1. PENDAHULUAN

Kemajuan teknologi khususnya di bidang sistem keamanan pada pintu brankas akan memberikan manfaat yang sangat besar bagi keamanan barang berharga di dalam brankas itu sendiri. Karena secara praktis teknologi ini akan menjadi konsumsi atau kebutuahan sekunder personal atau orang secara universal, sehingga pengguna atau user dapat lebih mudah melakukan aktifitas di luar tanpa khawatir dengan barang berharga di dalam brankas yang ditinggalkan.

Seperti yang kita ketahui bersama, saat ini masih banyak brankas konvesional yang beredar di masyarakat dengan sistem pengamanannya masih menggunakan sistem pengamanan semi otomatis (analog) dan tanpa pembatasan oleh siapa saja dapat membuka brankas tersebut. Sehingga memungkinkan dengan begitu mudah dibobol pencuri.

Berdasarkan masalah ini, lahir ide gagasan untuk merancang sistem keamanan brankas yang dapat dikontrol secara otomatis sebagai solusi dalam mengatasi tindak kriminal tersebut. Penulis mengembangkan sebuah teknik pengamanan dengan mengkombinasikan sidik jari pemilik brankas dengan sebuah kata sandi untuk akses dalam membuka pintu brankas tersebut. Selanjutnya sistem akan memberitahu pemilik brankas melalui pesan telegram jika brankas dicuri karena terputusnya catu daya utama pada brankas tersebut. Hal ini juga berlaku ketika pintu brankas terbuka atau terjadi kesalahan dalam memasukkan kata sandi ataupun ketika pemindaian sidik jari, sebagai notifikasi telah terjadi percobaan pembukaan brankas oleh orang tidak dikenal. Cara ini dianggap aman karena dalam membuka pintu brankas tidak dapat dilakukan oleh siapa pun kecuali mereka yang mengetahui kata sandi dan sidik jarinya sudah didaftarkan saja.

2. TINJAUAN PUSTAKA

Ada beberapa teori yang mendasari substantial pola pikir dari pembuatan alat ini agar mempermudah dalam mengevaluasi segala kendala yang dihadapi dalam tiap-tiap prrosesnya.

2.1 Internet of Things (IoT)

Internet of Things (IoT) dapat dilihat dari gabungan dari dua kata yakni ”Internet” dan ”Things”. Di mana ”Internet” sendiri didefinisikan sebagai sebuah jaringan komputer yang menggunakan protokol-protokol internet (TCP/IP) yang digunakan untuk berkomunikasi dan berbagi informasi dalam lingkup tertentu. Sementara ”Things” dapat diartikan sebagai objek-objek dari dunia fisik yang diambil melalui sensor-sensor yang kemudian dikirim melalui Internet [2] . Dengan kata lain agar sensor yang ditanamkan di berbagai perangkat di sekitar kita dapat terhubung dengan internet yang memungkinkan untuk dapat berkomunikasi dengan tablet, komputer / laptop, dan smartphone serta mempermudah dalam mengumpulkan data untuk dikirimkan ke database atau server. [2]

Gambar 1. Ilustrasi jaringan IoT

2.2 Sistem Biometrik

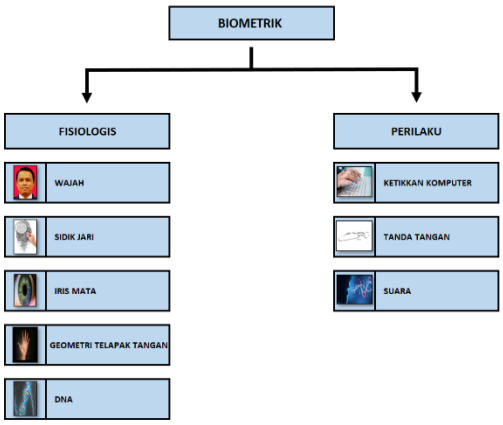
Pada dasarnya sistem biometrik merupakan sebuah sistem pengenalan pola dalam menentukan dan memverifikasi seseorang berdasarkan pada fitur yang berasal dari karakteristik fisiologis atau perilaku tertentu orang tersebut. [3]

Biometrik fisiologis yaitu pengenalan berdasarkan analisa langsung pada bagian tubuh manusia, seperti pengenalan wajah (face recognition), pengenalan sidik jari (fingerprint), pengenalan iris mata (iris recognition), pengenalan tangan (hand geometry), sertan DNA seseorang.

Sedangkan pada biometrik perilaku (behaviour) pengenalan didasarkan pada analisa secara tidak langsung pada pengukuran

Sigma Teknika, Vol. 5, No.1 : 100-107
Juni 2022
E-ISSN 2599-0616
P ISSN 2614-5979

karakteristik anggota tubuh manuasia, yaitu data yang diambil dari suatu kebiasaan atau berasal dari tindakan seseorang. Seperti pengetikan pada komputer, tanda tangan, dan suara seseorang. Oleh karena itu proses verifikasi pada biometrik perilaku bisa berlangsung lebih lama dibandingkan dengan biometrik fisiologis. [4]



Gambar 2. Bagan teknologi biometrik

Ada dua terminologi pada biometrik yaitu pendaftaran dan identifikasi. pendaftaran adalah proses verifikasi pada sistem biometrik dalam menentukan identitas seseorang untuk ditambahkan dalam database, sedangkan identifikasi adalah membandingkan seseorang dengan identitas yang ada dalam database untuk memastikan orang tersebut tidak terdaftar sebelumnya.

2.3 Modul NodeMCU V3

Modul NodeMcu V3 adalah sebuah platform Iot yang bersifat opensource terdiri System on a Chip (SoC) nirkabel integrasi tinggi, dirancang untuk perancang platform seluler yang memiliki ruang dan daya terbatas, serta dapat digunakan untuk menghosting aplikasi atau untuk memindahkan fungsi jaringan Wi-Fi dari prosesor aplikasi lain. Modul kecil ini memungkinkan Micro Controller Unit (MCU) untuk terhubung ke jaringan WiFi dan membuat koneksi TCP / IP penuh dan mikrokontroler [5].

Gambar 3. Modul NodeMCU V3

Modul NodeMcu V3 diperkenalkan oleh pabrikan Espressif Systems. Modul ini adalah versi 3 dan didasarkan pada ESP-12E (Modul WiFi berbasis ESP8266). Beberapa pin GPIO di papan memungkinkan kita untuk menghubungkan papan dengan periferal lain dan mampu menghasilkan komunikasi serial PWM, I2C, SPI, dan UART.

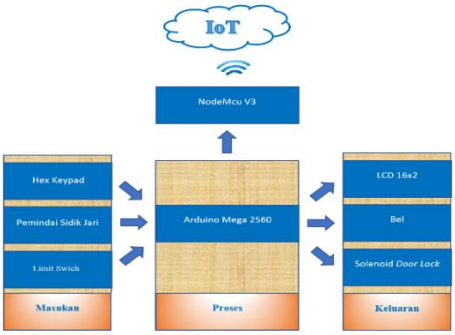
Antarmuka modul ini dibagi menjadi dua bagian termasuk Firmware dan Hardware dimana yang pertama berjalan pada ESP8266 Wi-Fi SoC dan yang lebih baru didasarkan pada modul ESP-12. Konverter USB ke UART pada modul mempermudah kita dalam mengubah data USB menjadi data UART yang terutama memahami bahasa komunikasi serial. Modul ini dilengkapi LED status yang berkedip sebagai isyarat status terkini dari modul jika berjalan dengan benar saat dihubungkan dengan komputer.

Modul ini membutuhkan daya sekitar 3.3v dengan memiliki tiga mode wifi yaitu Station, Access Point dan Both (Keduanya). Dengan menambahkan library ESP8266 / CTBot pada board manager kita dapat dengan mudah memprogram dengan basic program arduino.

3. PERANCANGAN

Perancangan sistem merupakan suatu proses serangkaian uji coba alat untuk mencapai tujuan dari dilakukannya penelitian ini. Dalam kesatuan sistem pengaman brankas ini, dibagi menjadi tiga blok yaitu masukan, proses, dan keluaran. Blok masukan menerima sinyal masukan dari sensor yang kemudian akan diteruskan ke blok pemrosesan, dimana pada blok ini semua data dari blok masukan akan dianalisa oleh suatu program yang telah disematkan di dalam chip mikrokontroler yaitu Arduino Mega 2560 sebagai kepala pikiran yang akan mengontrol seluruh eksekusi sesuai dengan perintah permrograman. Pada blok keluaran sistem penguncian brankas terjadi sebelum solenoid door lock aktif karena kondisi awalnya Normally Close (NC).

Sigma Teknika, Vol. 5, No.1 : 100-107
Juni 2022
E-ISSN 2599-0616
P ISSN 2614-5979

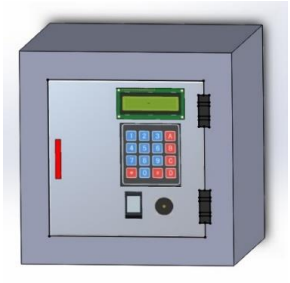


Gambar 4. Blok diagram sistem pengaman brankas

Pada Gambar 4 Hex Keypad berfungsi sebagai masukan ke Arduino Mega 2560 untuk memberi akses agar Pemindai Sidik Jari aktif. Selanjutnya Pemindai Sidik Jari melakukan pencocokan data dari hasil pemindaian dengan data yang telah tersimpan pada program Arduino Mega 2560, dan mengirimkan logika atau status data tersebut ke Arduino Mega 2560. NodeMcu V3 berfungsi sebagai media konektifitas antara perangkat keras dengan internet sebagai media informasi. Internet of Things (IoT) merupakan jalur komunikasi perangkat keras dengan aplikasi mobile (telegram bot) pada jaringan internet yang konektifitasnuya terhubung secara terus-menerus. LCD sebagai penampil status berjalannya tahapan proses pada sistem. Solenoid door lock aktif ketika menerima perintah dari Arduino Mega 2560 berupa tegangan listrik. Kemudian bel memberikan isyarat dengan berdering apabila terjadi kesalahan proses atau ketika solenoid door lock aktif.

3.1 Perancangan Perangkat Keras

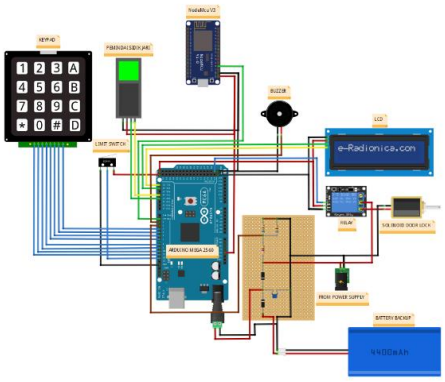
Teknik perancangan perangkat keras meliputi desain alat yaitu prototipe brankas lengkap dengan dimensional dan tata letak tiap komponen. Tujuannya adalah untuk mengetahui gambaran secara umum tentang sistem yang akan dibangun guna memenuhi kebutuhan pada tahapan analisis nantinya.



Gambar 5. Desain alat

3.2 Perancangan Pengkawatan (Elektronika)

Rancangan pengkawatan ialah skema yang digunakan dalam menggambarkan konfigurasi intalasi rangkaian kelistrikan pada tiap komponen secara detail. Skema ini digunakan untuk mempermudah kita memahami dari pemetaan sistem kelistrikan pada penelitian ini seperti gambar berikut.



Gambar 6. Skematik diagram pengkawatan sistem

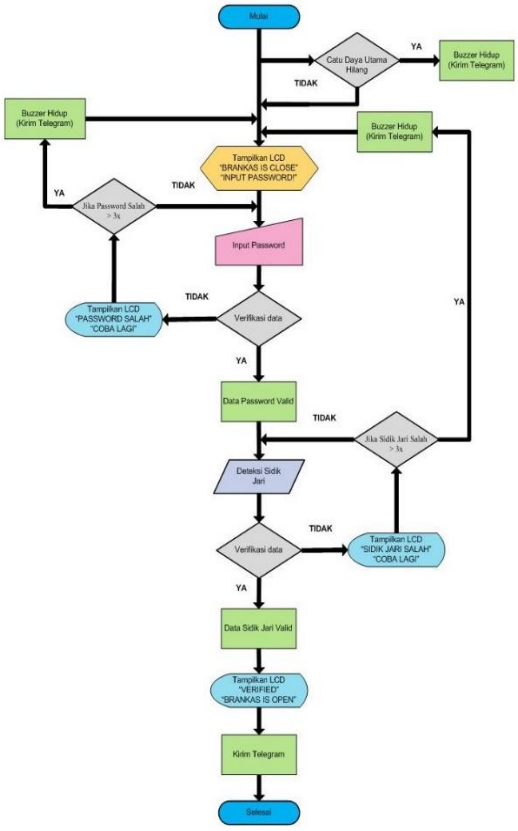
Tabel 1. Konfigurasi pin Arduino

Pin	Fungsi
1	Data tranmiter ke nodeMCU
2	VCC bel
3	Reading lose primary power supply
4 – 11	Koneksi keypad
12	Reading status limit switch
18 – 19	Mengirim dan menerima data dari fingerprint
20 – 21	Koneksi SDA & SCL pada modul I2C
53	Trigger relay

3.3 Perancangan Perangkat Lunak

Sigma Teknika, Vol. 5, No.1 : 100-107
Juni 2022
E-ISSN 2599-0616
P ISSN 2614-5979

Rancangan perangkat lunak bertujuan untuk merepresentasikan abstrak atau deskripsi suatu desain sistem ke dalam sistem perangkat lunak (pemrograman). Pada perancangan ini ada beberapa tahapan pemrograman mulai dari pembacaan program tiap komponen kemudian diproses oleh sebuah kontroler untuk menghasilkan eksekusi perintah tertentu. Sketsa perintah kerja pada sistem ini dapat digambarkan dengan alur diagram sebagai berikut:

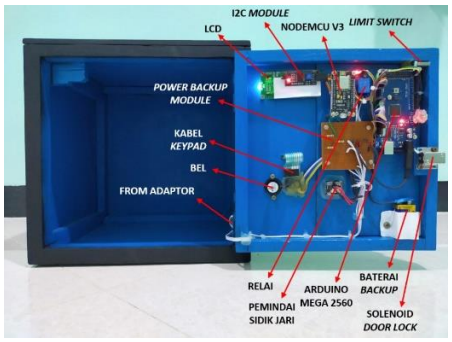


Gambar 7. Diagram alir sistem

4. HASIL DAN PEMBAHASAN

Bentuk fisik alat yaitu realisasi dari desain perancangan sistem yang terdiri dari beberapa komponen yang telah dirakit menjadi satu kesatuan dalam sebuah prototipe brankas yang terbuat dari papan plywood.

Gambar 8. Tampilan alat dari depan



Gambar 9. Tampilan alat bagian dalam

4.1 Hasil Pengujian Alat

Pengujian dan pengambilan data dilakukan untuk mengetahui sejauh mana kinerja tiap sub sistem yang saling berinteraksi sesuai dengan fungsinya masing-masing, serta mendapatkan data rujukan yang pasti untuk dilakukan analisa.

4.1.1 Pengujian Papan Ketik

Pembacaan data pada papan ketik dilakukan untuk mengetahui apakah tombol papan ketik yang ditekan menghasilkan keluaran yang sesuai. Pengujian ini dilakukan secara visual dengan membandingkan tombol yang ditekan pada papan ketik dengan tampilan LCD. Melaui pemrosesan mikrokontroler data masukan dari papan ketik akan diolah sehingga menghasilkan data keluaran yang sesuai pada tampilan pada LCD. Data hasil pembacaan adalah sebagai berikut:

Tabel 2. Hasil pengujian papan ketik

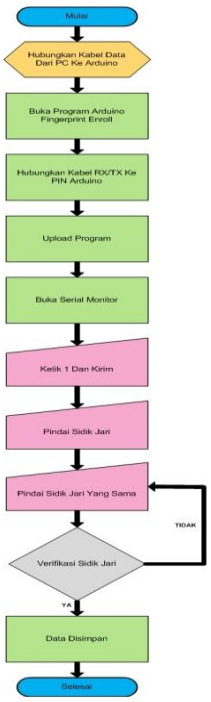
Tombol yang ditekan	Karakter yang muncuk di layar
Tekan 1	“1”
Tekan 2	“2”
Tekan 3	“3”

Sigma Teknika, Vol. 5, No.1 : 100-107
Juni 2022
E-ISSN 2599-0616
P ISSN 2614-5979

Tekan A	“A”
Tekan 4	“4”
Tekan 5	“5”
Tekan 6	“6”
Tekan B	“B”
Tekan 7	“7”
Tekan 8	“8”
Tekan 9	“9”
Tekan C	“C”
Tekan *	“*”
Tekan 0	“0”
Tekan #	“#”
Tekan D	“D”

4.1.2 Pengujian Sensor Pemindai Sidik Jari

Pengujian sensor pemindai sidik jari dilakukan untuk mengetahui kemampuan sensor mengenali sidik jari yang sudah didaftarkan. Pada pengujian ini lima jari tangan kanan didaftarkan sebagai data yang dikenali oleh sensor dan lima jari tangan sebelah kiri tidak didaftarkan sebagai pembanding pembacaan sensor sidik jari. Adapun alur proses pendaftaran sidik jari dapat digambarkan pada alur diagram berikut.



Gambar 10. Diagram alir *enroll* sidik jari

Setelah dilakukan proses pendaftaran sidik jari, maka diperoleh data pengujian sebagai berikut:

Tabel 3. Hasil pengujian sensor sidik jari

Sidik jari	Status pada EEPROM	Respon	Data serial monitor
Ibu jari kanan	Disimpan	Valid	Found a print match
Jari telunjuk kanan	Disimpan	Valid	Found a print match
Jari tengah kanan	Disimpan	Valid	Found a print match
Jari manis kanan	Disimpan	Valid	Found a print match
Jari kelingking kanan	Disimpan	Valid	Found a print match
Ibu jari kiri	Tidak disimpan	Tidak valid	Did not find a match
Jari telunjuk kiri	Tidak disimpan	Tidak valid	Did not find a match
Jari tengah kiri	Tidak disimpan	Tidak valid	Did not find a match
Jari manis kiri	Tidak disimpan	Tidak valid	Did not find a match
Jari kelingking kiri	Tidak disimpan	Tidak valid	Did not find a match

4.1.3 Pengiriman Data dari NodeMcu ke Telegram

Pengujian dilakukan untuk mengetahui apakah data dari NodeMcu dapat dikirim ke telegram sebagai notifikasi bagi pengguna. Pengujian dilakukan dengan membuat penamaan baru (newbot) pada aplikasi telegram melalui akun @BotFather, dan juga IDBot sebagai alamat tujuan komunikasi. Setelah kode Application Programming Interface (API) berupa token serta IDBot diunggah pada Modul NodeMcu, kemudian catu daya utama dilepas serta percobaan memasukan data password dan sidik jari yang tidak terdaftar pada sistem. Data hasil pengujian

Sigma Teknika, Vol. 5, No.1 : 100-107
Juni 2022
E-ISSN 2599-0616
P ISSN 2614-5979

secara visual dapat dilihat pada gambar dibawah ini:

Gambar 11. Tampilan layer bot Telegram

4.1.4 Pengujian Keseluruhan Sistem

Pada tahapan ini uji coba dilakukan, setelah semua perakitan dan pengemasan hardware serta proses verifikasi dan unggahan program selesai. Adapun proses pengujian dapat dilihat pada tabel berikut:

Tabel 4. Hasil pengujian kinerja sistem

Deskripsi	Pemindai sidik jari	Tampilan LCD	Tampilan Bot Telegram	Bel	Solenoid door lock
Disconnect Adaptor	Tidak merespon	"BRANKAS IS CLOSE – INPUT PASSWORD"	"LOSE PRIMARY POWER SUPPLY"	Berbunyi tanpa henti	Tidak aktif
Input password salah	Tidak merespon	SIDIK JARI SALAH – 1X COBA LAGI	-	Diam	Tidak aktif
Input password salah >3 kali	Tidak merespon	"BRANKAS IS CLOSE – INPUT PASSWORD"	"WRONG PASSWORD"	Berbunyi 5 detik	Tidak aktif
Input password benar	Merespon	"DATA DITERIMA – SCAN SIDIK JARI"	-	Diam	Tidak aktif
Pindai sidik jari salah	Merespon	"SIDIK JARI SALAH – 1X COBA LAGI"	-	Diam	Tidak aktif
Pindai sidik jari salah >3 kali	Merespon	"BRANKAS IS CLOSE – INPUT PASSWORD"	"WRONG FINGER SCANNED"	Berbunyi 5 detik	Tidak aktif
Pindai sidik jari salah benar	Merespon	"VERIFIED" – "BRANKAS IS OPEN"	"OPENED SAFE BOX"	Diam	Aktif

Gambar 11. Tampilan layar LCD pada Alat

Sigma Teknika, Vol. 5, No.1 : 100-107
Juni 2022
E-ISSN 2599-0616
P ISSN 2614-5979

5. KESIMPULAN DAN SARAN

5.1 Kesimpulan

Kesimpulan menggambarkan jawaban dari hipotesis dan/atau tujuan penelitian atau temuan ilmiah yang diperoleh. Kesimpulan bukan berisi perulangan dari hasil dan pembahasan, tetapi lebih kepada ringkasan hasil temuan seperti yang diharapkan di tujuan atau hipotesis.

Berdasarkan rumusan masalah dan setelah melakukan analisa terhadap hasil dari pengujian pada perancangan alat ini, maka dapat diambil kesimpulan sebagai berikut:

a. Dalam hal membuka pintu brankas, perancangan ini berhasil menggunakan verifikasi dua langkah yaitu sistem interlock antara password dengan sidik jari.

b. Upaya yang dapat dilakukan dalam mengawasi brankas dari jarak jauh adalah menggabungkan sistem IoT sebagai media informasi untuk mengetahui kondisi keadaan brankas saat itu.

5.2 Saran

Perancangan alat ini masih jauh dari kata sempurna dan perlu pengembangan lebih lanjut, untuk itu penulis menyarankan beberapa hal sebagai berikut:

a. Selain adanya notifikasi pesan telegram serta alarm, sebaiknya diperlukan tambahan GPS tracker untuk agar pemilik brankas dapat mengetahui keberadaan brankas jika terjadi tindak pencurian.

b. Dalam memaksimalkan tingkat keamanan perlu adanya komunikasi dua arah antara sistem keamanan brankas dengan user melalui telegram serta sebaiknya sistem merekam setiap orang yang telah mengakses brankas tersebut.

DAFTAR PUSTAKA

[1] Didit, E, P. (2014). Sistem Keamanan Berlapis Untuk Lemari Brankas Dengan Menggunakan 3 Kombinasi Password. Skripsi. Program Sarjana. Sekolah Tinggi Manajemen Informatika dan Komputer AMIKOM Yogyakarta. Yogyakarta.

[2] Fitri, H. (2019). Tren Masif Internet of Things (IoT) di Perpustakaan. Skripsi. Program Sarjana. Universitas Internasional Batam. Batam.

[3] Prabhakar, S & Pankanti, S & Jain A.K. (2003). Biometric Recognition: Security and Privacy Concerns. IEEE Security and Privacy, 99(2), 33-42. https://www.researchgate.net/publication/3437477BiometricRecognation SecurityandPrivacyConcerns. Diakses tanggal 25 September 2020.

[4] I Nyoman, S & I Gede, S, W & Ade, S, W. (2016). Rancang Bangun Sistem Keamanan Brankas Menggunakan Kombinasi Password Dan Sidik Jari Berbasis Mikrokontroler Atmega328. http://ojs.pnb.ac.id/index.php/matrix/article/view/64. Diakses tanggal 25 September 2020.

[5] Ali, A, D & Mohamed, F. (2018). NodeMcu V3 for Fast IoT Application Development. Https://www.researchgate.net/publication/328265730. Diakses tanggal 25 September 2020.