Implementasi dan Analisis Keamanan Loker Berbasis Sistem Otentifikasi Terpusat

Tugas Akhir

diajukan untuk memenuhi salah satu syarat

memperoleh gelar sarjana

dari Program Studi S1 Teknik Informatika

Fakultas Informatika

Universitas Telkom

1301140308

ILHAM AKBAR MUHAMMAD

Program Studi Sarjana S1 Teknik Informatika

Fakultas Informatika

Universitas Telkom

Bandung

2019

LEMBAR PENGESAHAN

Implementasi dan Analisis Keamanan Loker Berbasis Sistem Otentifikasi Terpusat

Implementation and Analysis of Locker Security Based on Authentication Centric System

NIM : 1301140308

ILHAM AKBAR MUHAMMAD

Tugas akhir ini telah diterima dan disahkan untuk memenuhi sebagian syarat memperoleh gelar pada Program Studi Sarjana S1 Teknik Informatika

Fakultas Informatika

Universitas Telkom

Bandung, < 29 November 2019 >

Menyetujui

Pembimbing I,	Pembimbing II,
Parman Sukarno, S.T., M.Sc., Ph.D.	Rahmat Yasirandi, S.T.,M.T.
NIP: 17770073	NIP: 18910105

Ketua Program Studi
Sarjana S1 Teknik Informatika,

Niken Dwi Wahyu Cahyani, S.T., M.Kom., Ph.D.
NIP: 00750199-1

LEMBAR PERNYATAAN

Dengan ini saya, Ilham Akbar Muhammad, menyatakan sesungguhnya bahwa Tugas Akhir saya dengan judul Implementasi dan Analisis Keamanan Loker Berbasis Sistem Otentifikasi Terpusat beserta dengan seluruh isinya adalah merupakan hasil karya sendiri, dan saya tidak melakukan penjiplakan yang tidak sesuai dengan etika keilmuan yang belaku dalam masyarakat keilmuan. Saya siap menanggung resiko/sanksi yang diberikan jika di kemudian hari ditemukan pelanggaran terhadap etika keilmuan dalam buku TA atau jika ada klaim dari pihak lain terhadap keaslian karya,

Bandung, 29 November 2019

Yang Menyatakan

Ilham Akbar Muhammad

Implementasi dan Analisis Keamanan Loker Berbasis Sistem Otentifikasi Terpusat

Ilham Akbar Muhammad [1], Parman Sukarno[2], Rahmat Yasirandi[3]

[1,2,3]Fakultas Informatika, Universitas Telkom, Bandung
[1]ilhamam@students.telkomuniversity.ac.id,
[2]psukarno@telkomuniversity.ac.id,
[3]batanganhitam@telkomuniversity.ac.id

Abstrak

Loker sebagai ruang penyimpanan memerlukan sistem pengamanan berupa kunci agar bisa dibuka dan ditutup dengan aman. Perkembangan sistem keamanan kunci loker meningkat ke arah penggunaan sandi, perangkat RFID dan yang terakhir sidik jari. Penggunaan sistem keamanan loker dengan sidik jari menggunakan satu pindai (*scanner*) untuk masing-masing loker, membutuhkan banyak alat pindai untuk banyak loker. Sistem ini menjadi tidak efisien, memerlukan banyak sumber energi dan menjadikan loker dengan biaya yang tinggi. Pada penelitian ini diterapkan keamanan loker berbasis sistem otentifikasi terpusat, menggunakan satu pindai untuk banyak loker dengan pengawasan petugas jaga. Ada 2 model permasalahan keamanan loker, yakni: apabila faktor otentifikasi (kunci dan *biometric* sidik jari) dicuri atau diduplikasi dan akan digunakan oleh orang yang tidak berhak (P1); apabila user dengan ID yang tidak terdaftar melakukan otentifikasi pada sistem (P2). Dengan lolosnya melewati beberapa skenario serangan, sistem otentifikasi ini telah terbukti dapat mengatasi permasalahan keamanan. Pengujian *response time* juga dilakukan pada sistem ini, dengan mendapat waktu 1.87 detik lebih lama dari sistem yang ada. Meskipun demikian, selisih waktu ini masih dapat ditoleransi dengan meningkatnya keamanan sistem yang diusulkan. Sehingga sistem yang diusulkan ini, dapat memberikan pengamanan loker yang lebih aman, murah, dan efisien.

Kata kunci : *loker, sidik jari, otentifikasi terpusat.*

Abstract

Locker as a storage room needs a security system such as key for opening and closing the locker safely. Locker security system had been developed and increased to be looks like password, RFID system, and the latest is finger print. The usage of locker security system by finger print with one finger scanner for every locker will need more scanners for more lockers. This system will be not so efficient, need more energy resources and making the locker system will be higher cost. This research will apply locker security based on authentication centric system, using only one finger scanner for many lockers under supervision of the Security personnel. There are two models locker security problem. If authentication factor (key or biometric fingerprint) is being stolen or duplicated and being used by un-authorized person (P1). If user with ID not registered to this system performing an authentication (P2). This system has proven to anticipate security problems. Response time testing had been performed to this system with achievement of 1.87 second more than the other available system. Even though, the time different is still under tolerance with more increment of proposed security system. So, the proposed system could give more locker security, proven safe, cheaper and efficient.

Keywords: locker, finger print, authentication, centric system

1. Pendahuluan

Latar Belakang

Loker penyimpanan umumnya berfungsi untuk menyimpan barang-barang pribadi para penggunanya. Pada lazimnya, loker dilengkapi dengan sebuah kunci pengaman yang konvensional. Akan tetapi, kunci konvensional tersebut mudah hilang dan macet sehingga loker tidak dapat digunakan lagi. Tahap lanjut dari peningkatan sistem keamanan pada loker [1] adalah dengan menggunakan kata sandi sebagai alat otentifikasi, atau menggunakan kartu RFID untuk membuka loker. Sistem ini masih banyak digunakan hingga saat ini, tetapi otentifikasi dengan kata sandi dan RFID masih mempunyai banyak kekurangan, antara lain pengguna mungkin bisa lupa atas kata sandi, atau kata sandi dapat dicoba dicuri (*hacked*) atau dengan mencoba-coba kombinasi kata dan bilangan. Bahkan kartu RFID juga mempunyai kelemahan seperti kartu dapat diduplikasi oleh orang lain untuk membuka akses loker.

Salah satu pengembangan berikutnya adalah sistem keamanan loker dengan otentifikasi menggunakan sidik jari [2]. Sidik jari (*finger print*) adalah hal yang sangat unik untuk masing-masing personal. Sangat jarang ditemukan kemiripan sidik jari diantara dua personel. Pada saat verifikasi dan otentifikasi, sistem akan membandingkan masukan data sidik jari sebelumnya dari pengguna dan memastikan bahwa loker dibuka oleh pengguna dengan sidik jari yang sama. Bilamana data sidik jari berbeda, maka loker tidak dapat dibuka. Pada penelitian sebelumnya [2][3][4] masih menggunakan satu pindai (*scanner*) otentifikasi sidik jari untuk masing-masing loker, sehingga membutuhkan banyak alat pindai untuk banyak loker. Sistem ini menjadi tidak efisien karena memerlukan banyak sumber energi dan menjadikan loker dengan biaya yang tinggi. Masih memungkinkan pindai loker dapat dirusak oleh orang tidak berhak dikarenakan tidak ada pengawasan langsung.

Berdasarkan permasalahan tersebut, pada penelitan ini penulis membuat *prototype* loker dengan 4 pintu berbasis sidik jari dengan otentifikasi secara terpusat. Sistem ini dibangun dengan tujuan menerapkan sebuah sistem otentifikasi terpusat menjadi lebih murah, efisien, aman dan masih dalam pemantauan penjaga. Faktor-faktor murah, efisien dan aman bisa dicapai dikarenakan hanya memerlukan satu alat pindai untuk semua loker dan ditempatkan dalam pengawasan penjaga. *User* dapat dipantau langsung oleh penjaga dan juga memeperkecil kemungkinan rusaknya alat pindai dan loker oleh orang yang tidak berhak. Batasan masalah pada penelitian ini adalah berfokus pada implementasi loker menggunakan 1 alat pindai untuk 4 solenoid pada setiap pintu loker. Implementasi alat ini juga membutuhkan energi listrik. Keberlangsungan listrik terus menerus pada saat pengujian (tidak ada listrik padam) serta kondisi sidik jari tidak ada cacat permanen yang menganggu proses pendaftaran dan otentifikasi.

Metode Penelitian

Metode penelitian yang dilakukan adalah difokuskan pada implementasi dan analisis sistem otentifikasi terpusat. Terdapat beberapa tahapan yaitu : 1) Studi literatur sistem keamanan loker pada penelitian sebelumnya; 2) Konsultasi dengan dosen pembimbing dalam perencanaan, pembuatan dan penyusunan laporan proposal; 3) Perancangan alat, yaitu implementasi membuat hardware dan software yang dibutuhkan; 4) Pengujian sistem perancangan alat dan analisanya; 5) Pembahasan atas analisis data yang diperoleh; 6) Tahap terakhir – Kesimpulan, akan dituliskan bagaimana hasil perancangan sampai evaluasi memenuhi tujuan yang telah disebutkan di awal.

2. Studi Terkait

Keamanan adalah hal yang sangat menjadi perhatian di akhir-akhir ini. Keamanan pribadi, rumah dan komputer secara dominan melingkupi keseharian manusia, sehingga manusia cenderung berpaling ke teknologi untuk melindunginya. Biometrik telah menjadi salah satu bentuk keamanan yang paling akurat, hemat biaya dan nyaman [3]. Teknologi tahap awal terkait keamanan adalah sistem gembok dan kunci. Protokol keamanan pada metoda ini adalah “satu kunci untuk satu gembok”. Pada awalnya, teknik ini dianggap yang paling aman, tetapi beberapa waktu kemudian terbukti kurang tepat, dikarenakan ada bukti bahwa kunci dapat diduplikasi, sehingga sistem ini dianggap sudah menjadi tidak sepenuhnya aman.

Tahap berikutnya pada penelitian [5] sistem pengamanan pada loker dilakukan dengan menggunakan dobel kata sandi yang berbeda dan menggunakan modem GSM untuk menghubungi pemilik loker. Pemilik akan mengetahui setiap proses yang terjadi pada brankas melalui pesan singkat ke handphone pemilik atau nomor tujuan yang dapat diganti sesuai keinginan. LCD akan menampilkan setiap karakter password dan nomor tujuan. Brankas juga dilengkapi alarm serta LED indikator. Sistem ini ada kekurangan, kata sandi dapat dicuri oleh pengguna lain yang tidak berhak dengan mencoba segala kombinasi kata sandi dan kendala jaringan komunikasi yang *down* akan menjadi masalah.

Sedangkan pada penelitian [6] pengamanan loker menggunakan pengenalan wajah dan One Time Password (OTP) dengan Personnal Identification Number (PIN). Bilamana PIN benar maka kamera yang terhubung dengan loker akan menangkap gambar wajah pengguna dan mencocokkan dengan *database*. Bilamana cocok, maka kata sandi akan dikirimkan ke pengguna. Sistem ini memang sangat aman namun sangat rumit dan berbiaya mahal.

Penelitian yang mirip juga dilakukan [7] dengan menggunakan PIN sebagai sistem keamanan loker. Metoda keamanan yang berbeda dilakukan [8] dengan menggunakan *barcode* dan SMS berbasis mikrokontroler Arduino Uno. SMS digunakan untuk mengirim pesan atas aktivitas yang dilakukan pada loker. Demikian juga penelitian [9] menggunakan kata sandi dan *Radio Frequency Identification* (RFID). Meski penelitian ini dinyatakan murah dan bebas dari kesalahan, namun potensi kendala dalam mengingat kata sandi masih bisa mungkin terjadi. Sedangkan kode data RFID dapat terhapus oleh medan magnet sekitar (dari *handpone*) dan kemungkinan duplikasi kartu RFID untuk membuka akses loker.

Teknologi biometrik meliputi sidik jari, suara, geometri tangan, telapak tangan, retina mata, dan pengenalan wajah. Diantara teknologi biometrik yang terdaftar, sidik jari adalah yang paling sering digunakan. Pengembangan sistem keamanan loker berikutnya lebih berkembang dengan menggunakan sidik jari. Pada penelitian [10] sistem keamanan menggunakan kombinasi sidik jari dan menggunakan GSM untuk otentifikasi kepada pemilik loker. Sedangkan pada penelitian [3] sistem kemanan dengan pengenalan sidik jari sebagai kunci pembuka loker. Namun penelitian ini masih terbatas menggunakan satu pindai untuk satu loker. Pada penelitian [11], untuk tuntutan sistem keamanan loker yang lebih tinggi, maka digunakan kombinasi RFID, sidik jari, kata sandi dan GSM. Namun konsekuensinya membuat sistem kemanan ini menjadi lebih rumit dan berbiaya mahal. Beberapa perkembangan penggunaan sistem keamanan loker tersebut diatas, dapat dilihat pada Tabel 1.

Tabel 1. Perkembangan Sistem Keamanan Loker

No.	Paper	Faktor Otentifikasi	Penerapan
1	[5]	Kata Sandi /*Password*	Brankas penyimpanan di rumah
2	[6]	*Facial Recognition* dan *One Time Passsword* (OTP)	*Locker*
3	[7]	*Pin-Number Lock*	*Electronic digital lock*
4	[8]	*Barcode* dan SMS	Gudang barang (*storage*) penyimpanan di Pabrik
5	[9]	*Keypad* dan RFID	*Locker*
6	[10]	ARM7, GSM, dan *fingerprint*	*Bank Locker*
7	[3]	Sidik jari / *Finger print*	Perkantoran, Gudang Penyimpanan
8	[11]	RFID, *Finger print*, *Password*	*Locker* di bank, kantor, dan rumah

Sistem yang diusulkan pada penelitian ini adalah menerapkan sistem otentikasi menggunakan data biometrik melalui sidik jari. Pada beberapa penelitian [3], [10], [11], [12], sidik jari telah digunakan sebagai faktor otentifikasi untuk membuka pintu masuk, dengan berbagai tambahan variasi kombinasi otentifikasi lainnya. Penerapan yang dilakukan pada penelitian ini adalah dengan menggunakan otentifikasi terpusat melalui satu unit pindai untuk beberapa loker, di bawah pengawasan petugas jaga loker. Sehingga lebih aman dan efeisien dan memperkecil rusaknya alat pindai dan loker oleh orang yang tidak berhak.

3. Sistem yang Dibangun

Perancangan Masalah

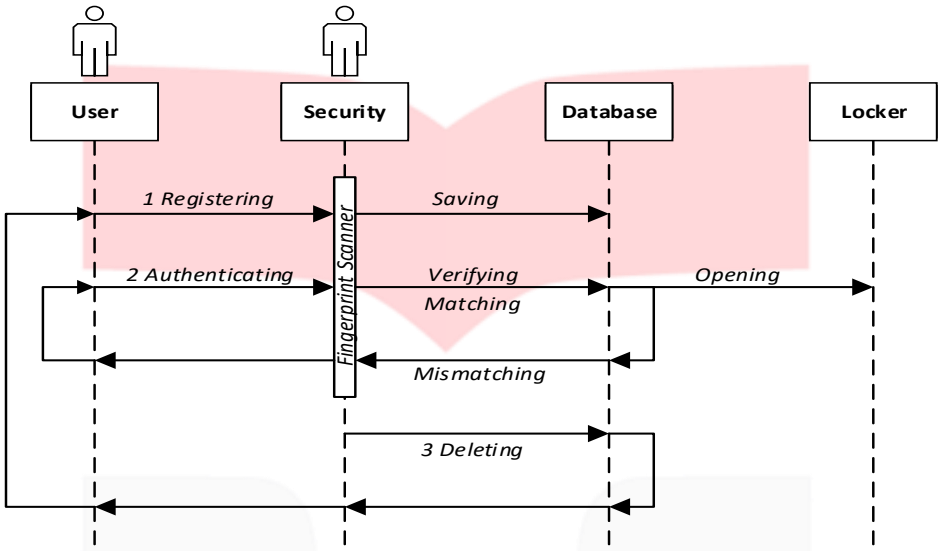
Sistem yang diusulkan dirancang untuk menjawab permasalahan keamanan loker sebagai berikut:

- P1: Apabila faktor otentifikasi (kunci dan *biometric* sidik jari) dicuri atau diduplikasi (*cloning*), pintu loker bisa dibuka oleh orang lain.
- P2: Apabila pintu loker dibuka dengan *biometric* sidik jari yang tidak terdaftar.

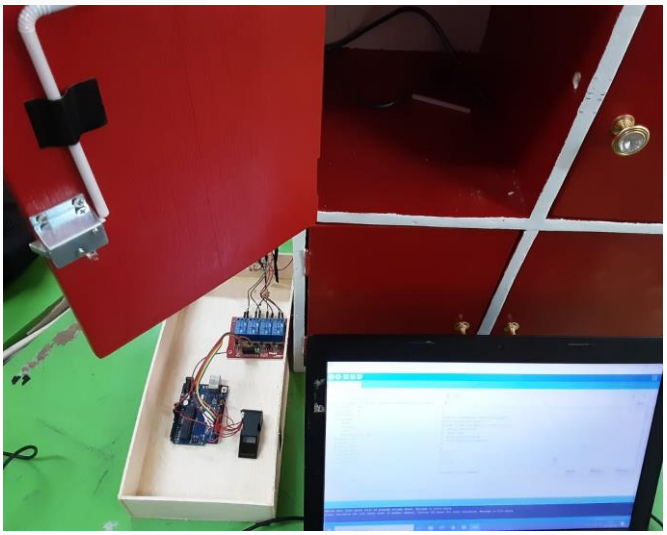
Untuk membuktikan sistem yang diusulkan dapat mengatasi permasalahan keamanan di atas, maka dibuat dua skenario *attacker* pada bagian prosedur pengujian.

Perancangan Sistem

Pada Gambar 1 di bawah adalah diagram sekuensial sistem keamanan loker otentifikasi terpusat yang diajukan. Sistem ini berada dibawah pengawasan petugas jaga yang mengawasi *user* menggunakan pindai sidik jari. Ada tiga tahapan yang akan dilakukan, pertama, *user* melakukan registrasi menggunakan pindai sidik jari agar sistem dapat menyimpan data *biometric user*. Kedua, *user* dapat melakukan otentifikasi pada sistem. Apabila data *user* telah tersimpan, sistem akan memverifikasi *user* dan pintu loker dapat terbuka. Apabila sistem tidak dapat memverifikasi maka *user* kembali ke tahap otentifikasi. Tahap ke tiga petugas jaga secara berkala menghapus data *user* pada sistem sehingga loker dapat digunakan oleh *user* lainnya pada kesempatan berikutnya. *Prototype* loker dengan sistem yang diusulkan ditampilkan pada Gambar 2.



Gambar 1. Diagram sekuensial sistem yang diusulkan [12]

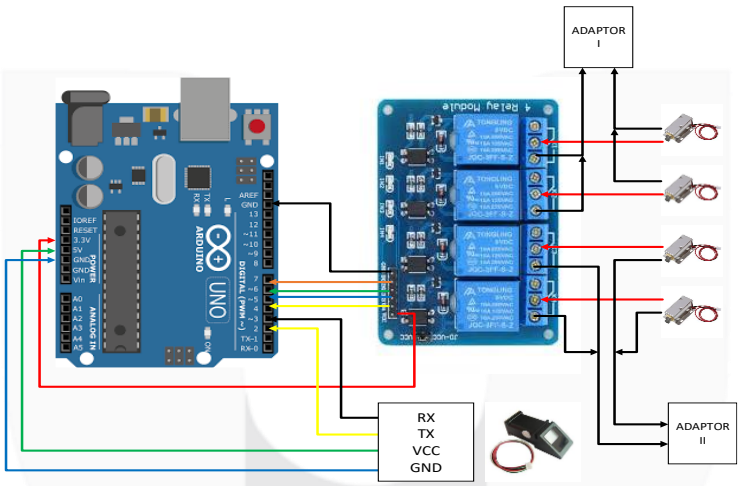


Gambar 2. *Prototype* loker berbasis sidik jari dengan sistem yang diusulkan

Perancangan Teknis dan Mekanis

Perancangan teknis dan mekanis dari sistem yang diusulkan membutuhkan perangkat keras dan perangkat lunak dilihat pada gambar 3 sebagai berikut :

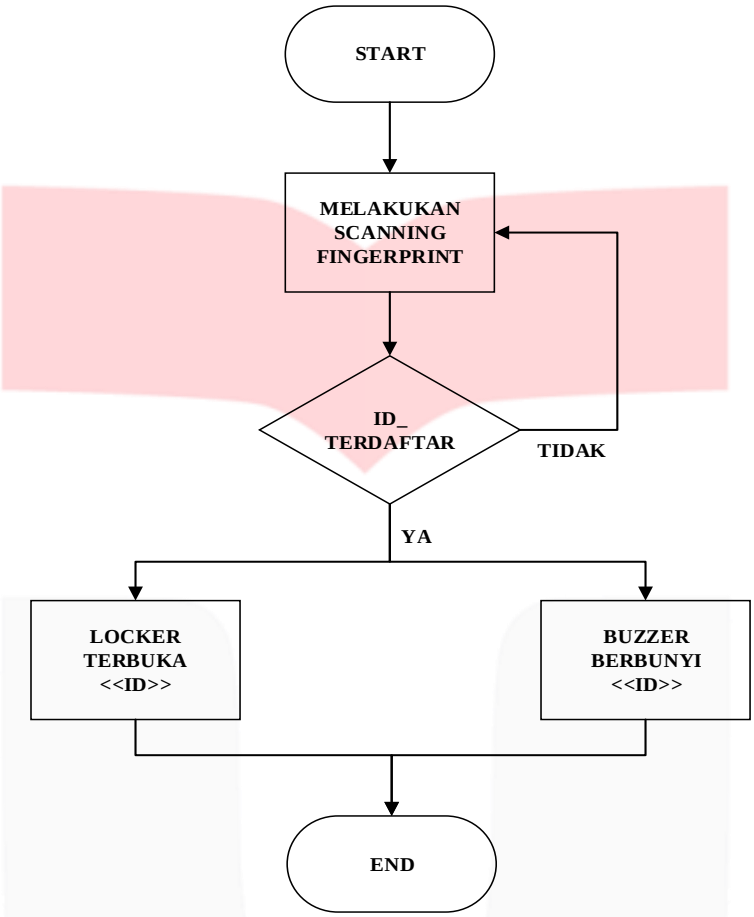
- Sensor sidik jari adalah modul yang terdiri atas sensor optik yang terpasang pada papan sirkuit. Sensor optik akan memindai sidik jari dan mikrokontroler dan perangkat lunak menyediakan fungsi otomatis untuk memproses sidik jari yang telah dipindai. Sensor ini mempunyai tingkat sensivitas tinggi meski pindai dalam keadaan basah atau kering. Fingerprint yang digunakan adalah fingerprint module fpm 10a. Akurasi fingerprint diketahui berdasarkan *False Accepted Rate* **(FAR)** dan *False Rejected Rate* **(FRR)**. Hasil pengujian yang dilakukan adafruit menunjukkan FAR sebesar <0,001% dan FRR sebesar <1,0% [13].
- *Solenoid door lock* adalah alat elektronik yang digunakan untuk menutup dan membuka loker. *Solenoid* ini akan bekerja bilamana diberikan tegangan. Pada kondisi normal, *solenoid* dengan kondisi tuas terkunci. Bilamana diberikan tegangan, maka tuas pada solenoid akan membuka. Pada penelitian ini digunakan solenoid dengan daya 6 volt.
- *Relay* yang berfungsi untuk melakukan perubahan (*switching*) pada perangkat AC maupun DC yang membutuhkan arus dan tegangan yang besar.
- Arduino Uno adalah *board* berbasis mikrokontroler pada ATMega 328, berfungsi untuk mengontrol masukan data dari pindai sidik jari serta *output* pada *solenoid*. Pada Arduino terdapat kontrol *Input/Output* (I/O) dengan beberapa pin untuk koneksi ke perangkat pindai sidik jari, data relay, dan lain-lain.
- *Personal Computer* (PC) digunakan untuk menjalankan perangkat lunak Arduino Uno, dimana perangkat lunak yang digunakan untuk membuat program adalah Arduino IDE, dengan bahasa program yang digunakan adalah bahasa C yang dapat meng-upload langsung ke mikrokontroler.



Gambar 3. Perancangan teknis sistem yang diusulkan

Prosedur Pengujian

Pada Gambar 4 di bawah ini adalah diagram skematis alur pengujian sistem yang diusulkan. Pertama, *user* harus melakukan pindai sidik jari. Hasil pindai akan disimpan dalam database. Jika ID *user* sudah terdaftar, maka loker akan terbuka. Bilamana ID *user* belum terdaftar, maka pintu loker tidak akan terbuka dan harus memulai ke tahap awal. Selanjutnya, loker terbuka dan buzzer berbunyi.



Gambar 4. Diagram skematis alur pengujian alat

Sebelum pengujian dilakukan ditetapkan kondisi awal yang harus dipenuhi oleh kedua sistem. Kondisi awal yang harus dipenuhi yaitu :

1. Adanya keberlangsungan sumber listrik untuk sistem yang diusulkan
2. Sistem yang diusulkan harus mempunyai ID *user* terdaftar
3. Kedua sistem harus mempunyai pintu loker yang dapat terbuka jika otentifikasi berhasil

Pada tahap pengujian dilakukan 2 prosedur pengujian pada sistem yang ada dan sistem yang diusulkan. **Pertama** adalah prosedur pengujian perbandingan keamanan sistem, dan **kedua** adalah prosedur pengujian *response time* otentifikasi sistem. Perbandingan sistem yang digunakan untuk *testing* dapat dilihat pada Tabel 2. Kunci konvensional dipilih sebagai faktor otentifikasi sistem yang ada, karena umumnya kunci masih digunakan di lingkungan kampus seperti perpustakaan, laboratorium dsb.

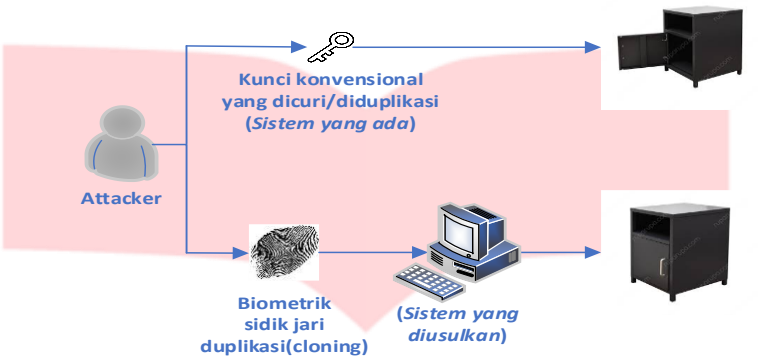
Tabel 2. Perbandingan sistem otentifikasi keamanan loker

No.	Sistem	Faktor Otentifikasi
1	Sistem yang ada	Kunci
3	Sistem yang diusulkan	Biometrik Sidik Jari

Prosedur pengujian keamanan sistem

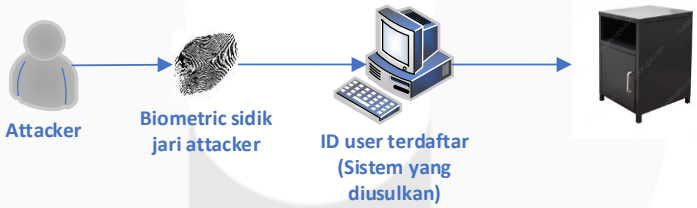
Tujuan dari pengujian ini adalah untuk mengetahui sistem otentifikasi yang diusulkan dengan *biometric* sidik jari lebih aman dibandingkan sistem otentifikasi yang sudah ada. Untuk mendapatkan perbandingan keamanan kedua sistem, dibuat skenario yang dapat terjadi pada otentifikasi loker adalah sebagai berikut :

a. *Attacker* menggunakan faktor otentifikasi (kunci dan biometrik sidik jari) yang dicuri atau diduplikasi (*cloning*) untuk membuka loker. Pada sistem yang sudah ada, *attacker* dapat dengan mudah membuka pintu loker. Sedangkan pada sistem yang diusulkan, sistem akan melakukan verifikasi terlebih dahulu. Sehingga hasil yang diharapkan adalah otentifikasi akan gagal dan *attacker* tidak dapat membuka pintu loker. Hasil pengujian ini untuk membuktikan apakah permasalah 1 (P1) dapat diatasi. Skema pengujian dapat dilihat pada Gambar 5.



Gambar 5. Skema pengujian 1 [12]

b. Pada sistem yang diusulkan, *attacker* melakukan otentifikasi *biometic* sidik jari dengan ID tidak terdaftar. Sistem akan melakukan verifikasi terhadap ID user. Sehingga hasil yang diharapkan adalah otentifikasi gagal dan *attacker* tidak dapat membuka pintu loker. Hasil pengujian ini untuk membuktikan apakah permasalah 2 (P2) dapat diatasi. Skema pengujian dapat dilihat pada Gambar 6.



Gambar 6. Skema pengujian 2 [12]

Prosedur pengujian *response time* sistem

Tujuan dari pengujian ini adalah untuk mengetahui *response time* otentifikasi sistem yang diusulkan masih dalam batasan toleransi. Pengujian ini dilakukan dengan membandingkan kedua sistem. Pada sistem yang sudah ada, pengujian dilakukan dengan mengukur waktu mulai *user* memutar kunci hingga pintu loker terbuka. Sedangkan pada sistem yang diusulkan adalah dengan mengukur waktu mulai *user* melakukan pindai sidik jari hingga pintu loker dengan kunci *solenoid* terbuka. Pengujian ini dilakukan oleh 10 *user* dimana setiap *user* melakukan otentifikasi berulang sebanyak 10 kali. Jadi total pengujian yang dilakukan adalah 100 kali pada masing-masing sistem.

4. Evaluasi

Pada bagian ini adalah hasil pengujian dan analisa dari kedua prosedur yang telah dijelaskan pada bagian sebelumnya.

4.1 Hasil Pengujian dan Analisis Keamanan Sistem

Hasil pengujian perbandingan keamanan sistem menggunakan skenario pertama dapat dilihat pada Tabel 3. Pada sistem yang ada, *attacker* dapat dengan mudah membuka pintu loker. Sedangkan pada sistem yang diusulkan, *attacker* gagal membuka pintu loker. Pada skenario kedua, *attacker* gagal membuka pintu loker dengan ID tidak terdaftar.

Tabel 3. Hasil pengujian perbandingan sistem keamanan loker

No.	Skenario	*Existing System*	*Propose System*
1	Skenario 1	*Attacker* berhasil membuka pintu loker	*Attacker* gagal membuka pintu loker

Hasil analisa dari pengujian skenario pertama adalah sebagai berikut. Pada sistem yang ada apabila kunci telah dicuri atau diduplikasi, berarti faktor otentifikasi telah berada di tangan *attacker*. Sistem yang ada tidak mempunyai kontrol untuk memverifikasi user. Sehingga *attacker* dengan mudah menggunakan kunci yang dicuri atau diduplikasi untuk membuka pintu loker. Sedangkan pada sistem yang diusulkan, *attacker* tidak dapat membuka pintu loker dikarenakan *biometric* sidik jari seseorang tidak dapat dicuri atau sulit diduplikasi (*cloning*) karena melekat pada tubuh manusia. Alat pindai sidik jari juga sulit dimanipulasi dengan cara manual seperti membuat sidik jari palsu dengan lilin (*Play-Doh*), silicon atau bahan lainnya. Keamanan sistem ini juga bertambah dengan adanya kontrol petugas jaga yang mengawasi *user* ketika melakukan otentifikasi. Hal ini membuktikan permasalahan 1 dapat teratasi dengan menggunakan sistem yang diusulkan.

Hasil analisa dari pengujian skenario kedua adalah apabila *attacker* melakukan otentifikasi, maka sistem akan melakukan verifikasi ID *user*. Jika ID *user* tidak terdaftar maka sistem akan gagal melakukan otentifikasi dan pintu loker tidak dapat terbuka. Pada sistem ini ada beberapa tahapan yang harus dilakukan. Pertama, *user* melakukan registrasi menggunakan pindai sidik jari agar sistem dapat menyimpan data *biometric user*. Kedua, *user* dapat melakukan otentifikasi pada sistem. Apabila data *user* telah tersimpan, sistem akan memverifikasi *user* dan pintu loker dapat terbuka. Hal ini membuktikan permasalahan 2 dapat teratasi dengan menggunakan sistem yang diusulkan.

Setelah melakukan pengujian dengan dua skenario dapat dibuktikan sistem yang diusulkan lebih aman dari tindakan pencurian atau duplikasi otentifikasi. Sistem ini juga dapat memverifikasi *user* dan adanya petugas jaga dapat menghindari otentifikasi dari orang yang tidak berhak.

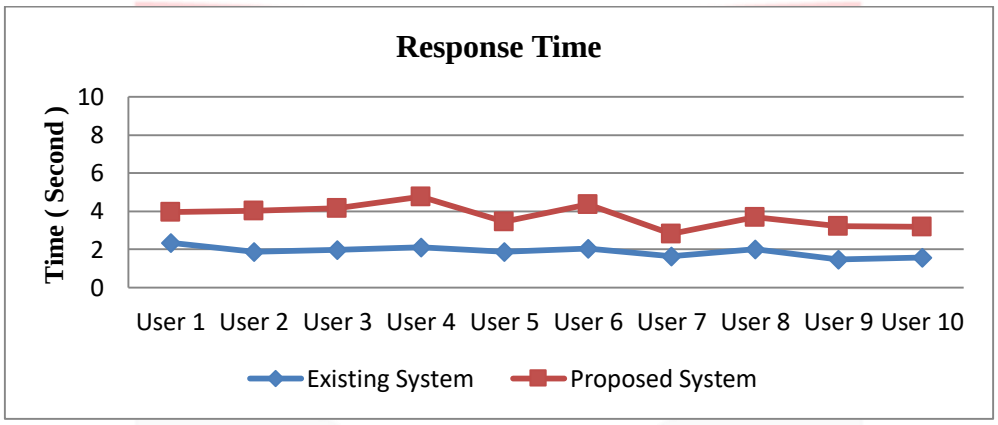
4.2 Hasil Pengujian dan Analisis *Response Time* Sistem

Pada Tabel 4 adalah hasil pengujian *response time* otentifikasi pada kedua sistem. *Response time* pada sistem yang telah ada *(existing system*) mendapat waktu untuk membuka loker rata-rata sebesar 1.90 detik. Sedangkan *response time* pada sistem yang diusulkan *(proposed system*) memerlukan waktu membuka loker rata-rata sebesar 3.77 detik. Terdapat selisih waktu 1.87 detik dari kedua sistem.

Tabel 4. Hasil pengujian perbandingan *response time (second)* sistem keamanan loker

	Existing System	Proposed System
User 1	2.35	3.96
User 2	1.89	4.03
User 3	1.97	4.18
User 4	2.11	4.77
User 5	1.89	3.46
User 6	2.05	4.36
User 7	1.66	2.81
User 8	2.02	3.7
User 9	1.47	3.24
User 10	1.57	3.2
Rata-rata	1.90	3.77

Pada Gambar 7 di bawah ini, dapat dilihat grafik *response time* otentifikasi. Pada sistem yang telah ada, mempunyai waktu lebih cepat dibandingkan sistem yang diusulkan. Sistem yang ada lebih mudah digunakan untuk membuka loker. Sedangkan pada sistem yang diusulkan dengan tingkat keamanan yang semakin baik, membutuhkan waktu untuk membaca sidik jari dan verifikasi *user* di database. Selain itu *response time* dapat dipengaruhi oleh sensitifitas alat pindai dan keadaan jari yang digunakan *user* untuk otentifikasi. Untuk mendapat *response time* yang optimal maka alat pindai harus dijaga kebersihannya dari kotoran bekas sidik jari yang menempel, keringat dan sensor tidak boleh terkena cahaya langsung. Sensor juga sulit mendeteksi jari yang kotor, basah, terlalu kering, terkelupas/luka dan tertutup tinta. Hal ini dapat diatasi dengan cara ketika tahap registrasi, *user* dapat mendaftarkan beberapa sidik jari (misal jempol, telunjuk, jari tengah atau jari manis). Sistem akan menyimpan beberapa data *biometric* sidik jari *user*, yang dapat digunakan untuk otentifikasi dan verifikasi bilamana ada kegagalan salah satu identifikasi data sidik jari data *user*.



Gambar 7. Grafik perbandingan *response time* sistem keamanan loker

5. Kesimpulan

Sistem keamanan loker yang diusulkan ini telah terbukti dapat mengatasi beberapa skenario pengujian keamanannya. *Biometric* sidik jari dipilih sebagai faktor otentifikasi sistem ini karena lebih aman, mudah dan murah. Otentifikasi terpusat pada sistem ini menjadi lebih aman karena menggunakan satu alat pindai untuk beberapa loker dibawah pengawasan petugas jaga. Meskipun ada perbedaan respon waktu antara sistem yang ada (konvensional) dengan system yang diusulkan (biometric sidik jari), namun selisih waktu ini masih dapat diterima. Untuk penelitian lebih lanjut, apabila letak alat pindai sidik jari untuk otentifikasi jauh dari posisi loker, disarankan menggunakan fasilitas WIFI menggantikan rangkaian kabel yang menghubungkan pindai sidik jari, mikrokontroler dengan solenoid yang dipasang pada loker.

Daftar Pustaka

[1] A. Aditya Shankar, P.R.K. Sastry, A. L. Vishnu Ram, A. Vamsidhar, *Finger Print Based Door Locking System*, International Journal Of Engineering And Computer Science ISSN:2319-7242, Volume 4, Issue 3, Page No. 10810-10814, March 2015
[2] Ajinkya Kawale, *Fingerprint based locking system*, International Journal of Scientific & Engineering Research ISSN 2229-5518, Volume 4, Issue 5, May 2013
[3]Y. L. Lay, H. J. Yang, C. H. Tsai, *Biometric Locker System*, Proceedings of the World Congress on Engineering and Computer Science 2011 Vol I WCECS 2011, San Francisco, USA, 19-21 October 2011
[4] Dinesh Bhatia, *A smart door access system using finger print biometric system*, Int. J. Medical Engineering and Informatics, Vol. 6, No. 3, 2014
[5] Ivan C. Melalolin, *Rancang Bangun Brankas Pengaman Otomatis Berbasis Mikrokontroler AT89S52*, Telekontran, Vol. 1, No. 1, Januari 2013
[6]N. Anusha, A. Darshan Sai and B. Srikar, *Locker Security System Using Facial Recognition and One Time Password (OTP)*, IEEE WiSPNET 2017
[7] Yogaratnam Nagaratnam, Wai Kit Wong, *Miniature Digital Pin-Number Lock*, Second International Conference on Computer Research and Development, 2010
[8] Prabowo H, *Pembuatan Prototipe Sistem Keamanan Pintu Gudang Penyimpanan Menggunakan Barcode dan SMS berbasis Mikrokontroler Arduino Uno*, Universitas Negeri Yogyakarta, 2017
[9]Salma Mohammed and Abdul Hakim Alkeelani, *Locker Security System Using Keypad and RFID*, IEEE/ICCSRE 2019
[10]Pooja Ausekar, Shraddha Kshirsagar, Puja Lawate, Prof. Mr. Sujit A. Inamdar, *Design and implementation of fingerprint based bank locker system using ARM7 and GSM*, International Research Journal of Engineering and Technology (IRJET), Volume: 05 Issue: 03, March 2018
[11] Raghu Ram.Gangi, Subhramanya Sarma.Gollapudi, Locker *opening and closing system using RFID, Finger print, Password and GSM*, International Journal of Emerging Trends & Technology in Computer Science (IJETTCS), Volume 2, Issue 2, March – April 2013
[12] Isa Mulia Insan, Parman Sukarno, Rahmat Yasirandi, *Multi-Factor Authentication Menggunakan Smart Card dan Fingerprint (Studi Kasus: Gerbang Parkir)*, Universitas Telkom, Juni 2019
[13] Ada, Lady. Adafruit. 2019. Adafruit Optical Fingerprint Sensor. [online] dapat dilihat pada : https://cdn-learn.adafruit.com/downloads/pdf/adafruit-optical-fingerprint-sensor.pdf

Lampiran

Tabel 5. Hasil pengujian *response time existing system*

	User1	**User2**	**User3**	**User4**	**User5**	**User6**	**User7**	**User8**	**User9**	**User10**
1	1.91	2.45	1.82	1.68	2.12	2.54	1.5	1.56	1.55	1.31
2	1.82	1.95	1.78	1.94	2.24	1.7	1.18	2.18	1.7	1.43
3	2.21	1.76	1.97	1.75	2.41	2.55	1.32	2.54	1.18	1.42
4	3.39	1.91	1.93	2.77	1.98	1.7	1.85	1.57	1.31	1.25
5	3.87	2.11	2.34	2.01	1.83	2.29	2.1	2.44	1.5	1.98
6	2.18	1.87	2.64	2.87	1.47	2.43	2.03	2.37	1.5	1.99
7	2.45	1.65	1.85	2.21	1.63	1.5	1.51	1.54	1.92	1.24
8	1.78	1.52	1.54	1.92	1.43	2.35	2.03	1.94	1.34	1.58
9	2.14	1.99	1.88	1.59	1.97	1.51	1.71	2.31	1.54	1.48
10	1.76	1.66	1.93	2.31	1.82	1.93	1.37	1.74	1.12	1.98
Jumlah	23.51	18.87	19.68	21.05	18.90	20.50	16.60	20.19	14.66	15.66
Rata-rata	2.35	1.89	1.97	2.11	1.89	2.05	1.66	2.02	1.47	1.57

Tabel 6. Hasil pengujian *response time purpose system*

	User1	User2	User3	User4	User5	User6	User7	User8	User9	User10
1	2.82	2.56	3.68	3.15	2.14	4.46	3.08	2.76	4.03	2.83
2	5.1	3.88	5.32	3.54	3.54	2.02	2.81	5.16	3.76	2.77
3	2.72	3.45	2.24	5.81	4.53	5.82	3.59	3.7	2.83	3.57
4	3.45	5.12	5.43	4.01	4.11	5.1	2.76	3.83	3.44	4.51
5	5.26	4.43	5.82	4.76	2.92	5.49	3.15	2.77	2.7	3.45
6	5.25	2.34	3.67	5.56	5.35	3.2	2.09	3.83	4.07	2.64
7	2.45	3.83	2.65	5.49	2.43	3.47	2.15	2.82	2.64	3.38
8	3.92	5.65	4.54	5.12	2.75	3.59	2.03	3.64	2.9	3.5
9	5.93	3.28	3.17	4.58	3.27	5.41	2.9	3.94	2.64	2.71
10	2.66	5.75	5.23	5.67	3.54	5.08	3.58	4.57	3.38	2.64
Jumlah	39.56	40.29	41.75	47.69	34.58	43.64	28.14	37.02	32.39	32.00
Rata-rata	3.96	4.03	4.18	4.77	3.46	4.36	2.81	3.70	3.24	3.20

Tabel 7. Hasil perhitungan data *response time* yang *acceptable* dengan *Standard Deviasi*

	Existing System	Proposed System
User 1	2.35	3.96
User 2	1.89	4.03
User 3	1.97	4.18
User 4	2.11	4.77
User 5	1.89	3.46
User 6	2.05	4.36
User 7	1.66	2.81
User 8	2.02	3.7
User 9	1.47	3.24
User 10	1.57	3.2
Rata-rata (mean)	1.90	3.77
STANDARD DEVIASI	**0.26**	**0.60**
mean ± SD		
mean + SD	**2.15**	**4.37**
mean - SD	**1.64**	**3.17**

Standard Deviasi (STDDEV)

Standard deviasi adalah nilai statistik yang dimanfaatkan untuk menentukan bagaimana sebaran data dalam sampel pengujian, serta seberapa dekat suatu data ke rata rata (mean) nilai sampel pengujian. Merupakan cerminan dari rata rata penyimpangan data dari mean (rata-rata). Standard deviasi dapat menggambarkan seberapa jauh bervariasinya data.

Pada pengujian *response time* untuk *existing system* data pengujian yang masih dapat diterima (*acceptable*) adalah antara 1.64 sd 2.15 *second.* Sedangkan untuk *proposed system* adalah antara 3.17 sd 4.37 *second.*

Tabel 8. Hasil perhitungan *Accuracy Proposed System* dengan *Confusion Matrix*

ID	Kondisi	Loker	Frekuensi	Kondisi	Loker	Frekuensi	Kondisi	Loker	Frekuensi	Kondisi	Loker	Frekuensi
A	TP	1	1	TN	3.4	2	TN	2.4	2	TN	2.3	2
	TN	2,3,4	3	FP	2	1	FP	3	1	FP	4	1
				FN	1	1	FN	1	1	FN	1	1
B	TN	3.4	2	TP	2	1	TN	1.4	2	TN	1.3	2
	FP	1	1	TN	1,3,4	3	FP	3	1	FP	4	1
	FN	2	1				FN	2	1	FN	2	1
C	TN	2.4	2	TN	1.4	2	TP	3	1	TN	1.2	2
	FP	1	1	FP	2	1	TN	1,2,4	3	FP	4	1
	FN	3	1	FN	3	1				FN	3	1
D	TN	2.3	2	TN	1.3	2	TN	1.2	2	TP	4	1
	FP	1	1	FP	2	1	FP	3	1	TN	1,2,3	3
	FN	4	1	FN	4	1	FN	4	1			

Keterangan :
TP = Keadaan/prediksi **(POSITIVE)** no. loker terbuka, memang benar **(TRUE)** no. loker terbuka sesuai dengan ID & no.loker yang terdaftar.
TN = Keadaan/prediksi **(NEGATIVE)** no. loker tertutup, memang benar **(TRUE)** no. loker tertutup sesuai dengan ID & no.loker yang tidak terdaftar.
FP = Keadaan/prediksi **(POSITIVE)** dimana no. loker terbuka, tetapi prediksi salah **(FALSE)** no. loker yang terbuka tidak sesuai dengan ID & no.loker yang terdaftar.
FN = Keadaan/prediksi **(NEGATIVE)** dimana no. loker tertutup, tetapi prediksi salah **(FALSE)** no. loker yang tertutup tidak sesuai dengan ID & no.loker yang terdaftar.

Tabel 9. *Accuracy Proposed System*

Rumus Accuracy	**(TP+TN)/(TP+TN+FP+FN)×100%**
Benar = 100%	**(1+3)/(1+3+0+0)×100%=100%**
Salah = 50%	**(0+2)/(0+2+1+1)×100%=50%**