Jurnal Teknik Informatika (JUTIF)
Vol. 3, No. 3, Juni 2022, hlm. 753-761

DOI: https://doi.org/10.20884/1.jutif.2022.3.3.345
p-ISSN: 2723-3863
e-ISSN: 2723-3871

LIBRARY SELF SERVICE SYSTEM USING NFC AND 2FA GOOGLE AUTHENTICATOR

Henry David Lie[1], Mychael Maoeretz Engel[*2]

[1,2]Informatika, Fakultas Teknologi Informasi, Universitas Ciputra Surabaya, Indonesia
Email: [1]hdavid@student.ciputra.ac.id, [2]mychael.engel@ciputra.ac.id

(Naskah masuk: 27 Mei 2022, Revisi : 30 Mei 2022, diterbitkan: 28 Juni 2022)

Abstract

The implementation of a self-service system is already used by many libraries, mainly on self-loan books. Self-service generally only uses RFID as a medium for identifying members and borrowed books, but using RFID alone as the head of the identification process may lead to many crimes such as using someone else's member card to borrow books, scam, and so on. This study aims to propose a new business process for self loan books from the library by combining NFC or RFID technology and 2FA (two-factor authentication) to minimize the crimes such as fraudulence, scams, and so on. The results showed that the system or prototype could work and function properly. The process of reading NFC tags and the use of 2F also runs quickly and safely.

Keywords: *android, NFC, RFID, self service, website, 2FA.*

SISTEM PEMINJAMAN MANDIRI PERPUSTAKAAN MENGGUNAKAN *NFC* DAN 2FA *GOOGLE AUTHENTICATOR*

Abstrak

Pemanfaatan sistem *self service* dalam melakukan peminjaman buku telah banyak dilakukan pada berbagai perpustakaan, *self service* tersebut umumnya hanya menggunakan RFID saja sebagai media pengidentifikasi anggota atau peminjam dan buku yang dipinjam, akan tetapi penggunaan RFID saja sebagai ujung tombak proses identifikasi dapat menimbulkan banyak tindak kriminal seperti menggunakan kartu anggota orang lain untuk meminjam buku dan tidak dikembalikan, penipuan, dan lain sebagainya. Penelitian ini bertujuan untuk mengajukan bisnis proses atau suatu rancangan sistem untuk melakukan peminjaman buku pada perpustakaan secara mandiri dengan menggabungkan teknologi NFC atau RFID dan 2FA (two factor authentication) untuk meminimalisir terjadinya tindak kriminal seperti kecurangan, penipuan, dan lain sebagainya pada saat melakukan peminjaman. Hasil penelitian menunjukkan sistem atau *prototype* dapat bekerja dan berfungsi dengan baik. Proses pembacaan NFC tag sampai dengan penggunaan 2FA juga berjalan dengan cepat dan aman.

Kata kunci: *android, NFC, RFID, self service, website, 2FA.*

1. PENDAHULUAN

Berdasarkan data yang diperoleh dari Badan Pusat Statistik (BPS), pada Desember 2019, Indonesia memiliki jumlah mahasiswa aktif sebanyak 7.339.164 [1] dan 4.598 [2] di antaranya berasal dari Universitas Ciputra. Untuk dapat melayani setiap mahasiswa dengan baik Universitas Ciputra telah menggunakan knowledge management system pada perpustakaan dalam menyusun buku - buku sesuai dengan jenis pengetahuan, penulis, dan lain – lain [3]. Selain itu Universitas Ciputra juga telah memanfaatkan teknologi RFID ini untuk melakukan stock opname dan telah terdapat wacana untuk menerapkan sistem peminjaman mandiri hanya saja belum terealisasikan, sedangkan telah banyak perpustakaan lain yang telah memanfaatkan sistem otomatisasi dalam hal peminjaman dan pengembalian buku dan secara berkala mencari solusi baru untuk meningkatkan pelayanan kepada pembaca atau anggota perpustakaan dengan biaya yang rendah dan staf atau pegawai dengan jumlah yang lebih sedikit dengan menerapkan teknologi dan ide baru [4].

Salah satu bentuk pemanfaatan teknologi baru tersebut adalah dengan menggunakan pelayanan mandiri atau self service yang telah berkembang dan mulai memasuki dunia perpustakaan [5]. Bentuk pelayanan mandiri atau self service di klaim sebagai bentuk layanan yang dipilih oleh pengguna karena beberapa alasan seperti kecepatan, lebih nyaman, dan mudah digunakan [6]. Penggunaan teknologi self service telah banyak dilakukan pada

perpustakaan di banyak negara [7]. Penggunaan NFC atau RFID pada sistem tersebut telah umum digunakan karena dinilai menjadi salah satu teknologi yang membantu pustakawan dalam membantu calon peminjam mencari buku, peletakan kembali buku yang dikembalikan, menjadi lebih efektif dan efisien [8][9]. Namun penggunaan NFC yang ada pada id card saja dinilai kurang aman karena dapat menimbulkan penipuan maupun tindak kriminal lainnya, hal tersebut dapat terjadi karena id card yang hilang atau dicuri dapat digunakan untuk melakukan transaksi peminjaman pada sistem perpustakaan [7].

Maka dari itu, penelitian sebelumnya untuk menangani hal tersebut peneliti menggunakan penyimpanan gambar peminjam dengan menggunakan kamera pada saat id card di scan dan teridentifikasi oleh sistem [7]. Namun penggunaan metode tersebut masih dapat menimbulkan kasus kejahatan seperti menggunakan foto pemilik kartu, menutupi wajah dan lain - lain [10]. Pada penelitian ini, peneliti akan menggabungkan teknologi NFC seperti pada penelitian sebelumnya sebagai identifikasi buku dan peminjam dengan teknologi 2FA (*two factor authentication*) yang disediakan oleh Google untuk membuat sebuah sistem self service yang lebih aman dan robust serta dapat dikembangkan untuk hal lain di masa yang akan datang. Sistem 2FA yang disediakan oleh Google merupakan suatu sistem OTP (*one time password*) yang tepatnya adalah TOTP (Time-based One-time Password) yang di mana kode OTP yang diberikan akan selalu melakukan sinkronisasi waktu dengan secret yang telah terintegrasi antara server dan sistem 2FA Google sehingga membuat sistem perpustakaan nantinya akan lebih sulit untuk diretas karena pemeriksaan data dan keamanan dilakukan di depan saat akan melakukan transaksi bukan setelah atau dalam melakukan transaksi seperti yang dilakukan oleh penelitian sebelumnya.

Penelitian ini akan menghasilkan sebuah sistem peminjaman mandiri buku pada perpustakaan berbasis web dengan menggunakan NFC sebagai identitas atau pengenal peminjam maupun buku dan 2FA untuk menambahkan lapisan keamanan pada sistem, beserta aplikasi android yang digunakan untuk pengendalian kartu identitas peminjam sekaligus menampilkan data pinjaman.

1.1. *Self Service*

Self service merupakan salah satu cara atau metode penyajian informasi kepada pengguna yang dapat berupa alat maupun aplikasi yang di mana dengan alat tersebut pengguna dapat menyelesaikan suatu transaksi maupun menemukan menemukan informasi yang diinginkan secara mandiri tanpa bantuan pihak lain seperti karyawan toko. Self service juga salah satu metode yang bagus untuk menyajikan suatu informasi secara lebih cepat dengan biaya yang rendah. Self service juga merupakan sistem yang serba guna sehingga dapat diterapkan pada berbagai aspek kehidupan [11].

1.2. Mikrokontroler

Mikrokontroler merupakan suatu komputer yang kompak yang digunakan untuk menjalankan suatu pekerjaan yang spesifik pada suatu sistem tanam, menjalankan perangkat IoT, dan lain sebagainya. Mikrokontroler biasanya mencakup atau terdiri atas prosesor, memori, dan input/output (I/O) port [12].

1.3. *Near Field Communication (NFC)*

Near Field Communication atau NFC merupakan alat komunikasi jarak dekat yang bekerja secara wireless yang berdasar pada teknologi Radio Frequency Identification (RFID) dan kompatibel dengan ISO/IEC 14443. NFC yang telah terhubung antara satu dengan lainnya dapat melanjutkan proses komunikasi dengan menggunakan media komunikasi jarak jauh seperti WiFi atau Bluetooth. NFC bekerja di frekuensi 12.56 MHz dan dapat mengirim data hingga 424 Kbits/s [13].

1.4. *NFC Reader*

NFC reader merupakan komponen atau perangkat aktif dalam suatu transaksi yang menggunakan NFC. Perangkat ini digunakan untuk dapat membaca dan menulis kartu atau tag NFC, berinteraksi dengan NFC pada *smartphone* dan memungkinkan proses komunikasi dari perangkat ke perangkat dapat terjadi [14].

1.5. Jenis *Tag NFC* [15]

- Sticker: *Tag* NFC yang berbentuk stiker dan tersedia dalam banyak bentuk, *tag* jenis ini umum digunakan untuk keperluan inventaris barang.
- Smartcard**:** *Tag* NFC yang berbentuk kartu dan di dalamnya tertanam *chip* NFC, tag jenis ini biasanya digunakan untuk untuk akses kontrol karyawan atau dengan kata lain sebagai id card karyawan, lingkungan sekolah untuk kartu tanda pelajar, keanggotaan organisasi, dan lain sebagainya.
- Gelang: Tag NFC yang diletakkan di dalam gelang hampir sama seperti *id card*. *Tag* jenis ini biasanya sekali pakai dan dapat digunakan kembali. Bahan yang sering digunakan adalah kertas, PVC lunak, dan silikon.

1.6. Tipe Mode Operasi *NFC* [13]

- Mode aktif adalah mode komunikasi NFC dengan kedua alat mengeluarkan atau menghasilkan sinyal radio pada data yang disimpan.

- Mode pasif adalah mode komunikasi NFC di mana hanya salah satu alat saja yang mengeluarkan sinyal radio, sedangkan alat lainnya berfungsi sebagai pembaca dan mengolah data yang diterima.

1.7. Media Komunikasi *NFC* [13]

- *Peer-to-Peer* yang bekerja di mana kedua alat dapat melakukan proses membaca dan menulis data ke alat lainnya.
- *Reader/Writer* dimana hanya salah satu alat yang bekerja sebagai penulis data sedangkan alat lainnya sebagai pembaca.
- *Card Emulation* dimana kedua alat dapat bertukar data di tingkat tautan

1.8. *Relational Database*

Relational Database merupakan salah satu jenis atau tipe dari basis data yang digunakan untuk menyimpan dan menyediakan akses ke data lainnya yang terkait antara satu sama lain. Dalam penggunaannya *relational database* akan memberikan id unik pada setiap baris data yang tersimpan dalam tabelnya, dan setiap baris data atau *record* biasanya mempunyai nilainya sendiri yang dapat memudahkan pembentukan relasi antar data pada tabel lainnya (Orcacle, n.d.). *Relational database* biasanya dikelola dengan menggunakan perangkat lunak untuk dapat melihat data apa saja yang terdapat dalam basis data tersebut. Terdapat banyak perangkat lunak yang dapat digunakan untuk mengolah data pada basis data jenis ini, antara lain Oracle Database, MySQL, PostgreSQL, dan lain sebagainya [16].

1.9. Keamanan

Keamanan atau *security* merupakan tindakan yang dilakukan untuk dapat mencegah terjadinya tindak kejahatan seperti pencurian, spionase, dan lain sebagainya dengan menggunakan benda maupun alat lainnya yang dapat menjadi jaminan ketika tindak kejahatan tersebut terjadi. Keamanan merupakan salah satu hal yang penting untuk dimiliki setiap orang untuk dapat melindungi data maupun diri dari serangan pihak lain [17].

1.9.1 Teknik Otentikasi

- *Single Factor Authentication* (1FA) merupakan sistem pengamanan yang hanya menggunakan 1 metode saja untuk proses pemeriksaan validasi data pengguna saat akan masuk pada sebuah sistem. 1FA banyak ditemukan pada berbagai website komersial yang hanya memerlukan *password* saja untuk dapat masuk pada sistem atau website tersebut [18].
- *Two Factor Authentication* (2FA) merupakan sistem pengamanan yang menggunakan 2 metode otentikasi berbeda untuk dapat memverifikasi data yang dimasukkan. 2FA bergantung pada metode otentikasi pengguna yaitu *password* yang diketahui oleh pengguna dan metode lainnya yang biasanya merupakan token atau OTP atau biometrik seperti sidik jari atau pengenalan wajah [19].
- *Multi Factor Authentication* (MFA) merupakan sistem pengamanan yang membutuhkan lebih dari 1 metode untuk memeriksa valid tidaknya data yang dimasukkan oleh pengguna sebelum dapat menggunakan suatu sistem. Tujuan dari penggunaan MFA adalah membuat sistem keamanan yang berlapis sehingga akan lebih sulit untuk diretas oleh pihak lain, karena jika salah satu metode rusak atau hilang data masih dapat terjaga keamanannya karena peretas memerlukan metode lainnya untuk dapat mengakses data tersebut. Contoh penggunaan MFA adalah menggabungkan password yang diketahui oleh pengguna dengan biometrik yang dimiliki oleh pengguna seperti pengenalan wajah, pemindaian sidik jari, penggunaan OTP dan lain sebagainya [20].

1.9.2 Jenis - Jenis One Time Password [21]

- *OTP (One-time Password)*: OTP merupakan salah satu bentuk *password* atau kata sandi yang hanya berlaku atau dapat digunakan sebanyak satu kali saja, penggunaan OTP sendiri sering ditemukan saat akan masuk pada suatu website dan website tersebut akan meminta rangkaian digit kode yang dikirimkan melalui SMS, Email, dan media lainnya. OTP dibuat menggunakan algoritma seperti SHA-1 yang menggabungkan 2 masukkan data yaitu *seed* dan *moving factor*. *Seed* merupakan suatu nilai rahasia atau (*secret key*) yang dibuat saat pertama kali suatu akun dibuat dan bersifat statis, sedangkan *moving factor* merupakan nilai yang berubah setiap kali pembuatan OTP diperlukan.
- *HOTP (HMAC-based One-time Password)*: HOTP merupakan jenis lain dari OTP yang bekerja secara semi-statis, karena kode yang dibuat bergantung kepada aksi yang dilakukan oleh pengguna. Perbedaan OTP dan HOTP terletak pada proses pembuatan *moving factor*, pada HOTP *moving factor* dibuat secara *incremental* pada nilai yang sebelumnya digunakan, contoh penggunaan HOTP adalah penggunaan Yubiko's Yubikey saat akan masuk pada suatu sistem.
- *TOTP (Time-based One-time Password)*: TOTP merupakan jenis lain dari OTP yang memiliki jangka waktu penggunaan yang lebih singkat. Perbedaan OTP dengan TOTP merupakan bagaimana moving factor dibuat, moving factor pada TOTP dibuat secara terus menerus setiap interval waktu yang ditentukan, normalnya adalah 30 sampai 60 detik, sehingga

pengguna harus menggunakan kode yang muncul pada interval waktu tersebut atau menunggu kode baru dibuat saat interval waktu habis. TOTP merupakan jenis OTP yang lebih baru dibandingkan 2 jenis lainnya yaitu OTP dan HOTP.

2. METODE PENELITIAN

Metode pengembangan perangkat lunak yang akan digunakan pada penelitian ini adalah metode *Software development lifecycle* (*SDLC*) yang menggunakan *Waterfall model* di dalamnya. Pemilihan metode pengembangan perangkat lunak ini didasari dari kecocokan alur kerja metode dengan penelitian ini yang mulai dari proses analisa kebutuhan hingga penyebaran sistem (*deployment*).

2.1. Metode Penelitian

Adapun metode penelitian yang digunakan pada penelitian ini adalah pendekatan kualitatif yang merupakan suatu metode penelitian yang dilakukan dengan tujuan untuk membuat deskripsi tentang suatu keadaan yang sedang terjadi secara fakta dan ada hubungannya dengan masalah yang sedang diteliti.

2.2. Analisa Kebutuhan

Analisa kebutuhan ini bertujuan untuk menyamakan persepsi terhadap sistem yang akan dikembangkan. Persepsi tersebut berupa fitur - fitur yang dibutuhkan atau setidaknya ada agar sistem ini nantinya dapat digunakan pada perpustakaan Universitas Ciputra. Analisa ini didapatkan melalui proses studi literatur dari penelitian terdahulu dan diskusi bersama pengurus perpustakaan Universitas Ciputra.

2.3. Pengumpulan Data

Teknik pengumpulan data yang digunakan selain studi literatur adalah wawancara dengan bapak Yehuda Abiel yang merupakan kepala perpustakaan Universitas Ciputra.

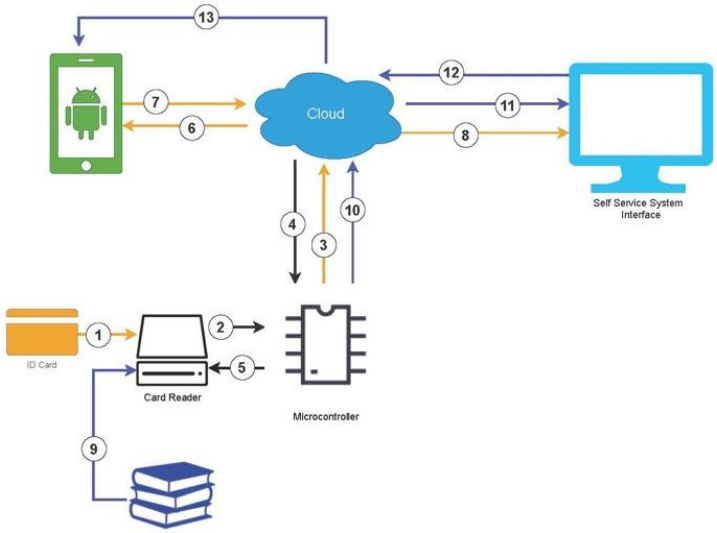
2.4. Hasil Analisa

Berdasarkan hasil yang telah didapatkan setelah melakukan wawancara. Terdapat beberapa fitur – fitur yang diharapkan ada dalam suatu sistem peminjaman buku secara mandiri. Fitur – fitur tersebut antara lain:

- Dapat membaca NFC maupun QRCode.
- Terdapat sekuritas tambahan selain kartu anggota.
- Terdapat pemberitahuan jika suatu transaksi peminjaman selesai dilakukan.
- Terdapat fitur untuk dapat memperpanjang buku secara otomatis melalui aplikasi android.
- Terdapat fitur yang dapat mengendxzalikan validitas kartu anggota.

2.5. Desain Arsitektur Sistem

Berikut ini adalah desain arsiketur dari sistem peminjaman mandiri yang akan menggambarkan garis besar jalan kerja sistem:



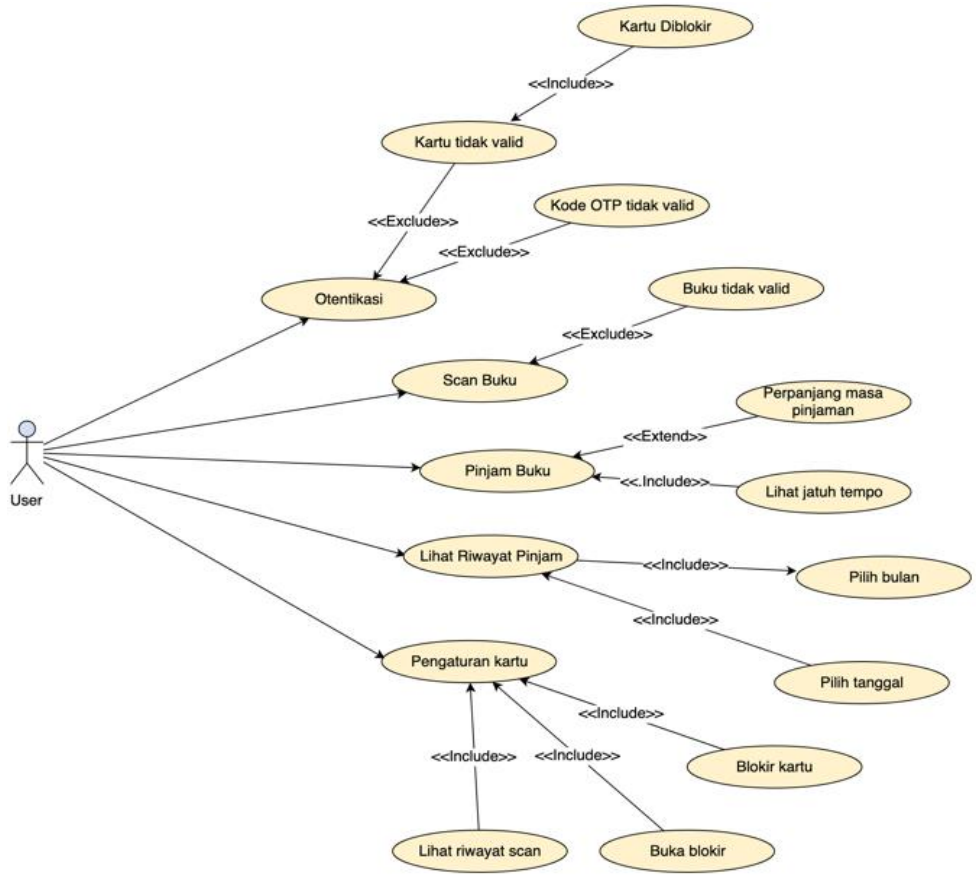
Gambar 1. Desain Arsitektur Sistem

Pengguna melakukan scan id card pada NFC reader (langkah 1), kemudian data pada kartu tersebut akan dikirimkan ke mikrokontroler (langkah 2), di mikrokontroler data tersebut akan dikirimkan ke server untuk diperiksa kredibilitasnya atau validasi data pada kartu tersebut (langkah 3), kemudian server akan mengembalikan response apakah kartu tersebut valid atau tidak (langkah 4), kemudian mikrokontroler yang menerima umpan balik dari server tersebut akan menyalakan memicu sensor yang menandakan bahwa kartu yang di scan valid atau tidak (langkah 5). Pada server kartu yang valid akan memicu server untuk meminta kode unik dari aplikasi 2FA untuk dapat mengakses sistem self

service (langkah 6 dan 7). Setelah sistem mendapatkan kode yang benar dari aplikasi 2FA, sistem akan membukakan akses untuk pengguna agar dapat menggunakan sistem self service (langkah 8). Sistem kemudian akan meminta pengguna untuk melakukan scan buku yang ingin dipinjam (langkah 9). Sama halnya seperti proses scan kartu, sistem akan secara otomatis memeriksa apakah buku yang di scan valid dan akan memberi pengguna notifikasi melalui sensor dan tampilan pada sistem (langkah 2, 10, 4, 5, 11). Pengguna kemudian melakukan konfirmasi peminjaman pada sistem (langkah 12), lalu setelah semua proses selesai pengguna akan mendapatkan notifikasi pada aplikasi bahwa peminjaman telah sukses dilakukan (langkah 13).

2.6. *Use Case Diagram*

Berikut ini merupakan use case diagram dari sistem peminjaman madiri yang akan menggambarkan garis besar fitur – fitur utama yang akan ada dalam aplikasi atau sistem peminjaman mandiri:



Gambar 2. *Use Case Diagram Sistem Peminjaman Mandiri*

Pada bagan di Gambar 2. di atas dapat terlihat proses apa saja yang dapat dilakukan oleh pengguna atau peminjam buku. Pengguna dapat melakukan proses otentikasi sebelum meminjam sebuah buku melalui website, melakukan pemindaian buku melalui website, melakukan proses peminjaman melalui website, melihat riwayat pinjam menggunakan aplikasi android, dan mengendalikan kartu anggota melalui aplikasi android.

3. HASIL DAN PEMBAHASAN

3.1. Implementasi Fitur

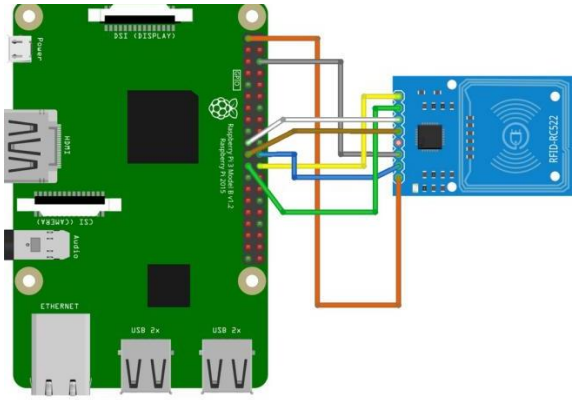
Pada aplikasi website terdapat empat user interface utama yang akan digunakan oleh pengguna, interface tersebut terdiri dari halaman masuk ke aplikasi atau login, halaman untuk memasukkan kode 2FA, halaman dasbor yang, dan halaman pinjaman terkonfirmasi. Selain empat interface atau antarmuka tersebut terdapat satu lagi antarmuka yang akan digunakan oleh pengguna saat pertama kali melakukan proses peminjaman, yaitu halaman aktivasi 2FA.

Pada aplikasi android terdapat empat user interface utama yang akan digunakan oleh pengguna, interface tersebut terdiri dari halaman masuk ke aplikasi atau login, halaman pinjaman aktif, halaman riwayat pinjaman, halaman detil pinjaman, halaman pengaturan akun, dan halaman riwayat tap kartu anggota. Aplikasi android ini sendiri hanya sebagai pelengkap dari keseluruhan sistem peminjaman mandiri, karena itu penampilan dari setiap user interface tidak dibuat sedemikian bagusnya. User interface pada aplikasi android ini

dibuat secara sederhana dan menampilkan informasi – informasi inti yang diperlukan oleh aplikasi. Aplikasi android pada penelitian ini akan menggunakan MVVM Architecture (Model-View-ViewModel).

3.2. Implementasi Perangkat IoT

Koneksi kabel yang menghubungkan antara sensor dengan Raspberry Pi dapat dilihat pada Gambar 3, sedangkan untuk detail *pin* dengan warna kabel dijabarkan pada Tabel 1 di bawah ini.



Gambar 3. Koneksi Kabel Sensor dengan Raspberry Pi

Tabel 1. Detail Koneksi Kabel

Warna kabel	Pin sensor	Pin raspberry Pi
Oranye	Pin 3.3V	Pin 1 / 3v3
Abu-Abu	Pin GND	Pin 6 / GND / Ground
Putih	Pin MOSI	Pin 19 / MOSI
Coklat	Pin MISO	Pin 21 / MISO
Hijau	Pin SICK	Pin 23 / SCLK
Biru	Pin RST	Pin 22
Kuning	Pin SDA	Pin 24

3.3. Implementasi Firebase

Pada pembuatan sistem peminjaman mandiri ini dibutuhkan pembaharuan data secara real-time antara perangkat IoT, aplikasi website, dan sistem backend. Pada Firebase digunakan sebagai perantara atau penghubung, dalam sistem ini Firebase juga digunakan untuk mengirimkan pesan notifikasi ke aplikasi android saat sebuat transaksi peminjaman baru dibuat. Layanan Firebase yang digunakan pada system ini antara lain adalah *Firebase Realtime Database*, dan *Firebase Cloud Messaging.*

3.4. Implementasi Basis Data

Pada penelitian ini basis data utama yang digunakan oleh sistem adalah basis data relasional yaitu *MySQL*. Basis data ini digunakan untuk menyimpan daftar buku yang dimiliki oleh perpustakaan, data pengguna perpustakaan, dan data transaksi peminjaman buku.

4. HASIL PENGUJIAN

Pada bagian ini menjelaskan hasil pengujian yang telah dilakukan pada sistem peminjaman mandiri yang meliputi aplikasi website, perangkat IoT dan aplikasi android. Hasil pengujian selanjutnya di analisis untuk mengetahui apakah sistem yang dirancang dapat berjalan dengan baik. Pengujian yang dilakukan dalam penelitian ini adalah pengujian terhadap penerapan teknologi NFC dan Implementasi 2FA pada perangkat IoT dan aplikasi website.

4.1. Pengujian *Alpha*

Pengujian *alphe* dilakukan untuk mengetahui dan menemukan *bug* atau permasalahan yang muncul saat aplikasi digunakan, dan untuk mengetahui kekurangan yang dari aplikasi yang perlu diperbaiki maupun dikembangkan lebih jauh. Pada penelitian ini pengujian aplikasi yang digunakan adalah pengujian *Alpha* dan *Beta*.

Pengujian a*lpha* merupakan bentuk pengujian yang dilakukan oleh pembuat aplikasi maupun orang – orang yang terlibat dalam pembuatan aplikasi. Pengujian *alpha* di tujukan untuk mencari dan membenarkan kesalahan atau *bug* yang ditemukan sebelum aplikasi di rilis pada pengguna eksternal. Pada penelitian ini pengujian *alpha* yang digunakan yaitu pengujian *white box* dan *black box* [22].

4.1.1. Pengujian *White Box*

Pengujian *white box* merupakan salah satu metode pengujian yang digunakan untuk menguji struktur internal dari sebuah aplikasi. Pengujian ini bertujuan untuk mencari kejanggalan pada sebuah sistem aplikasi [23].

Pengujian *white box* pada penelitian ini menangani kesulitan pembuatan fitur *login* atau masuk secara otomatis kedalam aplikasi website dengan melakukan *tap* kartu anggota pada perangkat *IoT*. Beberapa metode telah di uji coba untuk mewujudkan agar fitur ini dapat bekerja dengan baik, yaitu implementasi *websocket* dan implementasi *firebase.* Pada akhir pengujian implementasi *firebase* digunakan dalam mewujudkan kinerja dari fitur ini, karena salah satu layanan yang disediakan oleh *firebase* yaitu *real-time database* dirasa cukup efektif.

4.1.2. Pengujian *Black Box*

Pengujian *black box* merupakan salah satu metode pengujian yang digunakan untuk menguji perilaku dari aplikasi atau sistem hanya berdasarkan apa yang di masukkan dan yang dikeluarkan (*input* dan *output*) saja tanpa mengetahui struktur internal dari aplikasi atau sistem tersebut atau bisa dikatakan pengujian terhadap jalannya *user interface* yang telah di rancang dan di implementasikan [24].

Hasil pengujian *black box pada* aplikasi website dapat dilihat pada Tabel 2, sedangkan hasil pengujian *black box* pada aplikasi *android* dapat dililhat pada Tabel 3 di bawah ini.

Tabel 2. Hasil Pengujian *Black Box* Aplikasi *Website*

Fungsi Aplikasi	**Kondisi**	**Aksi yang diharapkan**	**Aksi yang terjadi**	**Status**
Masuk ke aplikasi (pertama kali dan gagal)	Melakukan tap pada perangkat IoT	Menampilkan pesan ketika kartu yang digunakan salah atau bermasalah.	Menampilkan pesan ketika kartu yang digunakan salah atau bermasalah.	Valid
Masuk ke aplikasi (pertama kali dan berhasil)	Meminta pengguna mengaktifkan 2FA	Dapat menampilkan tombol untuk mengaktifkan 2FA.	Dapat menampilkan tombol untuk mengaktifkan 2FA.	Valid
Mengaktifkan 2FA	Meminta konfirmasi passsword	Dapat menampilkan QR Code dan Recovery codes setelah konfirmasi password.	Dapat menampilkan QR Code dan Recovery codes setelah konfirmasi password.	Valid
Masuk ke aplikasi (bukan pertama kali dan gagal)	Meminta pengguna memasukkan kode 2FA	Dapat meminta pengguna melakukan tap kembali jika kode yang dimasukkan tidak valid	Dapat meminta pengguna melakukan tap kembali jika kode yang dimasukkan tidak valid	Valid
Masuk ke aplikasi (bukan pertama kali dan berhasil)	Meminta pengguna memasukkan kode 2FA	Dapat menampilkan halaman dasbor jika kode yang dimasukkan valid.	Dapat menampilkan halaman dasbor jika kode yang dimasukkan valid.	Valid
Menonaktif-kan tombol pinjam dan menampilkan pesan jika terdapat pinjaman aktif pada halaman dasbor	Memeriksa apakah pengguna memiliki pinjaman aktif	Dapat menonaktif-kan tombol pinjam dan menampilkan pesan terdapat pinjaman aktif	Dapat menonaktif-kan tombol pinjam dan menampilkan pesan terdapat pinjaman aktif	Valid
Menampilkan daftar buku pada halaman dasbor	Membaca data daftar buku yang telah di *tap* oleh pengguna	Dapat menampilkan daftar buku dalam bentuk tabel	Dapat menampilkan daftar buku dalam bentuk tabel	Valid
Membuat transaksi pinjam baru	Mengirim email dan notifikasi ke aplikasi android saat pinjaman terbuat	Dapat menampilkan halaman pinjaman baru terkonfirmasi dan mengirimkan email serta notifikasi ke aplikasi android	Dapat menampilkan halaman pinjaman baru terkonfirmasi dan mengirimkan email serta notifikasi ke aplikasi android	Valid

Tabel 3. Hasil Pengujian *Black Box* Aplikasi *Android*

Fungsi Aplikasi	**Kondisi**	**Aksi yang diharapkan**	**Aksi yang terjadi**	**Status**
Splashscreen	Menampilkan logo aplikasi dan memeriksa data pada *sharedpreference*	Dapat menampilkan logo selama 2 detik, dan berpindah ke halaman login jika data kosong atau ke halaman pinjaman aktif.	Dapat menampilkan logo selama 2 detik, dan berpindah ke halaman login jika data kosong atau ke halaman pinjaman aktif.	Valid
Masuk / Login Aplikasi	Email dan password benar, serta mendapatkan akses token	Sukses masuk ke aplikasi dan berpindah ke halaman pinjaman aktif	Sukses masuk ke aplikasi dan berpindah ke halaman pinjaman aktif	Valid
Halaman pinjaman aktif	Menampilkan data yang di terima dari sistem *backend*	Dapat menampilkan data dalam *recyclerview*	Dapat menampilkan data dalam *recyclerview*	Valid
Halaman riwayat pinjaman	Menampilkan data yang di terima dari sistem *backend*	Dapat menampilkan data dalam *recyclerview*	Dapat menampilkan data dalam *recyclerview*	Valid
Halaman detil pinjaman	Menampilkan data pinjaman secara lebih rinci	Dapat menampilkan daftar buku yang dipinjam dalam recyclerview	Dapat menampilkan daftar buku yang dipinjam dalam recyclerview	Valid
Halaman akun	Menampilkan data pribadi pengguna	Dapat menampilkan nama, nim pengguna	Dapat menampilkan nama, nim pengguna	Valid
Memblokir dan buka blokir kartu	Melakukan permintaan ke sistem *backend* untuk memblokir atau membuka blokir kartu	Dapat menampilkan pesan dari *backend* dalam sebuah *toast.*	Dapat menampilkan pesan dari *backend* dalam sebuah *toast.*	Valid
Halaman riwayat tap	Menampilkan data yang di terima dari sistem *backend*	Dapat menampilkan data dalam *recyclerview*	Dapat menampilkan data dalam *recyclerview*	Valid

Berdasarkan tabel pengujian *black box* pada aplikasi *website* dan *android* di atas, hasil pengujian menunjukkan bahwa aplikasi *website* dan aplikasi *android* dapat berjalan dengan baik. Hal tersebut

dapat dilihat dari kasus uji coba yang berjalan sesuai dengan aksi yang diharapkan.

4.2. Pengujian *Beta*

Pengujian *beta* adalah rangkaian pengujian yang dilakukan terhadap calon pengguna yang tidak terlibat dalam proses pembuatan sistem. Pada penelitian ini jenis pengujian *beta* yang dilakukan adalah *Closeted beta testing* dengan melibatkan orang – orang tertentu saja dalam pengujiannya [25].

Dalam penelitian ini *closeted beta testing* dilakukan dengan melakukan wawancara dan pengujian sistem bersama bapak Yehuda Abiel yang merupakan kepala perpustakaan Universitas Ciputra. Wawancara tersebut dilakukan untuk menguji dan mendapatkan masukkan serta saran terhadap sistem yang telah dirancang dan dibangun.

Berdasarkan hasil wawancara dengan bapak Abiel, beliau merespon dengan baik dan mengatakan bahwa aplikasi atau sistem ini sudah bagus dan bisa digunakan. Penggunaan kartu anggota dan keamanan tambahan 2FA juga dapat membantu memperketat keamanan jika terdapat hal – hal yang tidak diharapkan, karena menurut bapak Abiel sistem peminjaman mandiri memerlukan tingkat sekuritas yang cukup ketat dalam penggunaannya nanti. Bapak Abiel juga merespon dengan positif pada pemeriksaan sistem ini, karena jika ada orang yang menggunakan kartu lain dan tidak terdaftar maka orang tersebut tidak bisa masuk ke dalam aplikasi. Di samping sistem yang sudah cukup baik bapak Abiel memberikan beberapa masukkan agar sistem ini dapat berkembang lebih baik lagi, masukkan atau saran tersebut antara lain:

- Memberikan mekanisme atau fitur untuk melakukan perpanjangan buku.
- Menerapkan mekanisme menghitung kuota buku untuk dipinjam.
- Memberikan fitur rekomendasi terhadap buku – buku yang terkait dengan buku yang sedang dipinjam.
- Dapat mengganti penggunaan kartu anggota dengan *QR Code*.

5. KESIMPULAN

Berdasarkan hasil desain, implementasi, pengujian dan proses yang telah dilakukan pada bab – bab sebelumnya, dapat disimpulkan bahwa tugas akhir ini telah mampu menjawab penerapan rancang bangun sistem peminjaman mandiri di perpustakaan menggunakan NFC dan 2FA Google Authenticator dengan jabaran:

Sistem telah berhasil menerapkan teknologi NFC yang digunakan sebagai tanda pengenal seorang peminjam dan buku pada perpustakaan. Dalam penggunaannya peminjam diminta untuk melakukan tap kartu anggota pada perangkat IoT yang tersedia. Pada proses tersebut data pada kartu akan diperiksa validitasnya. Setelah itu pengguna akan diminta untuk memasukkan kode 2FA yang di buat oleh aplikasi Google Authenticator atau mengaktifkan fitur 2FA jika belum aktif pada akun yang digunakan. Setelah itu pengguna dapat melakukan tap buku dan membuat transaksi peminjaman baru.

Setelah transaksi pinjam terkonfirmasi dan pengguna telah menerima notifikasi melalui email dan pada aplikasi android, sistem ini telah berjalan dengan baik sesuai dengan skema atau arsitektur sistem yang telah dirancang.

Sekuritas pada sistem ini juga telah dapat berjalan sesuai dengan harapan dan tujuan penelitian dalam menjawab permasalahan terkait sekuritas yang kurang pada penelitian sebelumnya.

Sistem ini juga sudah dapat menjawab kebutuhan dasar dari sebuah sistem peminjaman mandiri yang mudah untuk digunakan dan aman, namun tetap memerlukan beberapa penyesuaian lebih lanjut ketika akan digunakan nantinya.

Adapula saran perluasan terhadap sistem untuk pengembangan penelitian ke depan, antara lain, membuat metode 2FA sendiri yang tidak menggunakan aplikasi pihak ketiga seperti Google Authenticator, menambahkan fitur rekomendasi buku lain saat pengguna telah meminjam suatu buku pada aplikasi android, menambahkan fitur untuk melakukan perpanjangan buku yang sedang dipinjam melalui aplikasi android dan membuat mekanisme maupun fitur untuk mengembalikan buku yang sedang dipinjam.

DAFTAR PUSTAKA

[1] Badan Pusat Statistik (BPS), "Jumlah Mahasiswa Aktif Indonesia Tahun 2019," 2019. https://www.bps.go.id/indikator/indikator/view_data_pub/0000/api_pub/82/da_04/1 (accessed May. 18, 2021).

[2] Kemdikbud, "PDDikti - Pangkalan Data Pendidikan Tinggi," 2019. https://pddikti.kemdikbud.go.id/data_pt/NjhGODA5NDItMkIzRC00MDRCLTk0QjktRDc3NjUxODJDQzlG (accessed May. 18, 2021).

[3] N. Karna, I. Supriana, and N. Maulidevi, "Implementation of e-learning based on knowledge management system for Indonesian academic institution," in 2016 1st International Conference on Information Technology, Information Systems and Electrical Engineering (ICITISEE), 2016.

[4] K. Wing, "Use of self-service holds in Maine public libraries," Publ. Libr. Q., vol. 38, no. 1, pp. 1–18, 2018.

[5] R. Sigwald, "Self-service customer service models in libraries," J. Libr. Adm., vol. 56, no. 4, pp. 453–478, 2016.

[6] M. Kasavana, "Emergent service delivery

technologies," Journal of International Management Studies, vol. 5, no. 2, pp. 159–167, 2010.

[7] N. Karna, D. Pratama, and M. Ramzani, "Self service system for library automation : Case study at telkom university open library," in 2019 International Conference on Information and Communications Technology (ICOIACT), 2019.

[8] C. Hu and I. Harris, "RFID in the library: Economic, social and environmental perspectives," in 2016 Third International Conference on Digital Information Processing, Data Mining, and Wireless Communications (DIPDMWC), 2016.

[9] I. Markakis, T. Samaras, A. C. Polycarpou, and J. N. Sahalos, "An RFID-enabled library management system using low-SAR smart bookshelves," in 2013 International Conference on Electromagnetics in Advanced Applications (ICEAA), 2013.

[10] T. S. Huang and K. Aizawa, "Image processing: some challenging problems," Proc. Natl. Acad. Sci. U. S. A., vol. 90, no. 21, pp. 9766–9769, 1993.

[11] Salesforce, "What exactly is self-service?," 2021. https://www.salesforce.com/products/service-cloud/what-is-self-service/. (accessed May. 18, 2021).

[12] B. Lutkevich, "What is a Microcontroller and How Does it Work?," 2019. https://internetofthingsagenda.techtarget.com/definition/microcontroller. (accessed May. 18, 2021).

[13] J. Gautam, Y. Kumar, and A. Gupta, "Existing scenario of near field communication in transport sector," in 2014 International Conference on Signal Processing and Integrated Networks (SPIN), 2014.

[14] Nxp, "NFC Readers," 2020. https://www.nxp.com/products/rfid-nfc/nfc-hf/nfc-readers:NFC-READER. (accessed May. 18, 2021).

[15] Serialio, "Common types of NFC tags," 2020. https://www.serialio.com/support/learn-rfid/common-types-nfc-tags. (accessed May. 18, 2021).

[16] Trustradius, "Relational Databases," 2019. https://www.trustradius.com/relational-databases. (accessed May. 18, 2021).

[17] D. J. Brooks, "What is security: Definition through knowledge categorization," Secur. J., vol. 23, no. 3, pp. 225–239, 2010.

[18] T. Contributor, "Single-Factor Authentication (SFA)," 2015. https://searchsecurity.techtarget.com/definition/single-factor-authentication-SFA. (accessed: May. 18, 2021).

[19] L. Rosencrance, P. Loshin, and M. Cobb, "What is two-factor authentication (2FA) and how does it work?," 2020. https://searchsecurity.techtarget.com/definition/two-factor-authentication. (accessed May. 18, 2021).

[20] M. E. Shacklett and T. Contributor, "Multifactor Authentication (MFA)," 2021. https://searchsecurity.techtarget.com/definition/multifactor-authentication-MFA. (accessed May. 18, 2021).

[21] Onelogion, "OTP, TOTP, HOTP: What's the Difference?," 2020. https://www.onelogin.com/learn/otp-totp-hotp. (accessed May. 18, 2021).

[22] A. S. Oktriwina, "Alpha Testing: Definisi, Cara dan Keuntungannya untuk Aplikasi," 2019. https://glints.com/id/lowongan/alpha-testing/. (accessed May. 19, 2021).

[23] G. N. Arviana, "White box testing: Definisi dan berbagai tekniknya," 2020. https://glints.com/id/lowongan/white-box-testing-adalah/. (accessed May. 19, 2021).

[24] N. Rahmalia, "Black box testing, uji software penting bagi developer," 2020. https://glints.com/id/lowongan/black-box-testing/. (accessed May. 19, 2021).

[25] A. S. Oktriwina, "Beta Testing: Pengertian dan Cara Melakukannya," 2020. https://glints.com/id/lowongan/beta-testing-adalah/. (accessed May. 19, 2021).