



INSTITUT TEKNOLOGI BANDUNG

PROGRAM STUDI TEKNIK ELEKTRO

JALAN GANESHA NO. 10 Gedung Labtek V Lantai 2 (022)2508135-36, (022)2500940
BANDUNG 40132

Dokumentasi Produk Tugas Akhir

Lembar Sampul Dokumen

Judul Dokumen

TUGAS AKHIR TEKNIK ELEKTRO:
Sistem Keamanan Mesin ATM menggunakan sidik jari

Jenis Dokumen

DESAIN SISTEM

Catatan: Dokumen ini dikendalikan penyebarannya oleh Prodi Teknik Elektro ITB

Nomor Dokumen

B300-04- TA171801007

Nomor Revisi

Versi 04

Nama File

B300

Tanggal Penerbitan

14 December 2017

Unit Penerbit

Prodi Teknik Elektro - ITB

Jumlah Halaman

110

Data Pemeriksaan dan Persetujuan

Ditulis Oleh	Nama	Christiawan	Jabatan	Mahasiswa
	Tanggal	12 Desember 2017	Tanda Tangan	
	Name	Bayu Aji Sahar N.	Jabatan	Mahasiswa
Diperiksa Oleh	Tanggal	12 Desember 2017	Tanda Tangan	
	Name	Azel Fayyad R.	Jabatan	Mahasiswa
Disetujui Oleh	Tanggal	12 Desember 2017	Tanda Tangan	
	Name	Elvayandri, S.Si, M.T	Jabatan	Dosen Pembimbing
	Name	Elvayandri, S.Si, M.T	Jabatan	Dosen
	Tanggal	12 Desember 2017	Tanda Tangan	
	Name	Dr. Muhammad Amin Sulthoni	Jabatan	Dosen
	Tanggal	12 Desember 2017	Tanda Tangan	

Nomor Dokumen: B300-03-TA1718.01.007 Nomor Revisi: 03 Tanggal: 12/14/2017 Halaman 1 dari 110

© 2017 Prodi Teknik Elektro-ITB. Pengungkapan dan penggunaan seluruh isi dokumen hanya dapat dilakukan atas ijin tertulis Prodi Teknik Elektro - ITB Jalan Ganesha 10 Bandung, 40132 Indonesia.

DAFTAR ISI

DAFTAR ISI.....	2
CATATAN SEJARAH PERBAIKAN DOKUMEN.....	3
1 PENGANTAR	4
1.1 RINGKASAN ISI DOKUMEN	4
1.2 TUJUAN PENULISAN DAN APLIKASI/KEGUNAAN DOKUMEN	4
1.3 REFERENSI	4
1.4 DAFTAR SINGKATAN.....	5
2 KONSEP SISTEM	6
2.1 SISTEM IDEAL	6
2.2 PILIHAN SISTEM	7
2.2.1 <i>Pilihan Desain 1</i>	8
2.2.2 <i>Pilihan Desain 2</i>	13
2.2.3 <i>Pilihan Desain 3</i>	19
2.3 ANALISIS.....	24
2.3.1 <i>Kriteria</i>	24
2.3.2 <i>Analisis konsep</i>	26
2.4 SISTEM YANG AKAN DIKEMBANGKAN	35
2.4.1 <i>Metode pemilihan</i>	35
2.4.2 <i>Konsep sistem terpilih</i>	42
3 DESAIN SISTEM	45
3.1 PEMODELAN FUNGSIONAL SISTEM.....	45
3.1.1 <i>Desain Level 0 Sistem</i>	45
3.1.2 <i>Desain Level 1 Sistem</i>	45
3.1.3 <i>Desain Level 2 Sistem</i>	47
3.1.4 <i>Desain Software</i>	57
3.2 PEMODELAN TINGKAH LAKU SISTEM	60
3.2.1 <i>Behavioral Sistem Utama Mesin ATM</i>	60
3.2.2 <i>Behavioral Input Function</i>	69
3.2.3 <i>Behavioral Fingerprint Function</i>	73
3.2.4 <i>Behavioral Card Function</i>	79
3.2.5 <i>Behavioral Server Function</i>	81
3.2.6 <i>Behavior Display Function</i>	83
3.3 HARDWARE.....	84
3.3.1 <i>Desain Fisik</i>	84
3.3.2 <i>Komponen</i>	84
3.3.3 <i>Rangkaian</i>	91
3.4 GRAPHICAL USER INTERFACE	91
3.5 SIMULASI	93
3.5.1 <i>Algoritma Fingerprint</i>	93
4 LAMPIRAN.....	97

Catatan Sejarah Perbaikan Dokumen

VERSI, TGL, OLEH	PERBAIKAN
1, 25 Novermber 2017, Chrisiawan, Bayu, Azel	<ul style="list-style-type: none">• Cara mengukur kemudahan user secara kuantitatif• Alasan tidak menggunakan kombinasi desain
2, 28 November 2017, Christiawan	Perbaikan Simulasi Algoritma Sidik Jari
2, 28 November 2017, Bayu	<ul style="list-style-type: none">• Penambahan standard yang berlaku dan berpengaruh pada desain• Desain Software Fungsional
2, 28 November 2017, Christiawan	Penambahan tipe variable dan ukuran data setiap fungsi
3, 10 Desember 2017, Azel	<ul style="list-style-type: none">• Gambar-gambar diagram dan flowchart yang samar diperjelas• Penggantian metode analisis decision matrix menggunakan AHP
4, 11 Desember 2017, Azel	<ul style="list-style-type: none">• Penambahan penjelasan skenario penggunaan sistem, registrasi sidik jari, dan proses pengecekan data nasabah di server pada pemilihan desain• Penambahan penjelasan pemenuhan spesifikasi sistem pada tiap desain sistem• Penambahan penjelasan level tegangan dan ukuran data pada bagian dekomposisi fungsional
4, 12 Desember 2017, Bayu	<ul style="list-style-type: none">• Pengaitan Spesifikasi B200 dengan desain pada B300 pada saat pemilihan desain

Proposal Proyek Pengembangan Sistem Keamanan Mesin ATM menggunakan Sidik Jari

1 Pengantar

1.1 Ringkasan Isi Dokumen

Secara umum, dokumen ini berisi tentang perancangan desain Sistem Keamanan Mesin ATM menggunakan Sidik Jari secara keseluruhan yang terdiri dari integrasi antar hardware dan software. Pada dokumen ini, dijelaskan alternative desain keseluruhan yang dapat digunakan untuk merancang produk yang dibandingkan secara fungsionalitas dengan desain sistem ideal yang sudah ada. Kriteria pemilihan dari desain yang ada dibuat berdasarkan tujuan dan spesifikasi sistem yang telah dibuat pada dokumen sebelumnya. Pada dokumen ini, juga terdapat metode pemilihan sistem dengan menggunakan pembobotan.

Dokumen ini juga berisi tentang pemodelan fungsional dan pemodelan behavioral. Pemodelan fungsional sistem berisi tentang fungsi-fungsi yang dipecah dari diagram blok level tinggi sampai dengan diagram blok terendah dengan menggunakan *level design*. Pada bagian ini, juga terdapat beberapa pilihan komponen yang dapat digunakan untuk membentuk sebuah rangkaian akhir sistem. Pemodelan behavioral sistem berisi tentang data flow diagram, flowchart, dan penjelasan algoritma yang digunakan sampai dengan *function call*. Pada bagian ini, juga terdapat GUI (*Graphic User Interface*) yang akan digunakan.

1.2 Tujuan Penulisan dan Aplikasi/Kegunaan Dokumen

Tujuan dari penulisan dokumen ini adalah sebagai berikut:

1. Sebagai dokumen untuk menjelaskan gambaran alternative desain dari proyek Sistem Keamanan Mesin ATM menggunakan Sidik Jari
2. Sebagai justifikasi terhadap desain dan komponen-komponen yang digunakan untuk perancangan Sistem Keamanan Mesin ATM menggunakan Sidik Jari
3. Sebagai landasan dalam mengimplementasikan pembuatan *hardware* dan *software* pada alat yang dibuat.

Dokumen ini dibuat untuk memenuhi prosedur pelaksanaan tugas akhir Teknik Elektro ITB dan ditujukan kepada dosen pembimbing tugas akhir dan tim tugas akhir Program Studi Teknik Elektro ITB sebagai bahan penilaian tugas akhir.

1.3 Referensi

- [1] Moses, Hillary D. *Fundamentals of Fingerprint Analysis*. CRC Press (2015)
- [2] Ford, Raplh M. and Coulston, Chris S. *Design for Electrical and Computer Engineers*. McGraw-Hill (2008)
- [3] More, Prachi and Shriram Markande. *Design and Implementation of Anti-theft Module for ATM Machine*. Institute of Electrical and Electronics Engineers (IEEE)

- [4] Gabriel, Iwasokun, Muda Josiah Lange, dkk. *Experimental Study of Thumbprint-Based Authentication Framework for ATM Machines*. Science and Information Conference, London, UK – (2014)
- [5] Shamdasani, Jaydeep and Prof. Pravin Mate. *ATM Client Authentication System Using Biometric Identifier & OTP*. International Journal of Engineering Trends and Technology (IJETT) – Volume 11 Number 5 – (2014)
- [6] Lakshmi, Sampada and Chandra Babu. *Fingerprint and RFID Based Biometric ATM Authentication System*. International Journal of Innovative Technologies – ISSN 2321-8665 Vol.04, Issue.16, pp :3154-3156 (2016)
- [7] Gafurov, Davrondzhon and Patrick Bours. *Impact of Finger Type in Fingerprint Authentication*. Norwegian Information Security Lab – ISSN 1865-0929. DOI 10.1007/978-3-642-17610-4_1

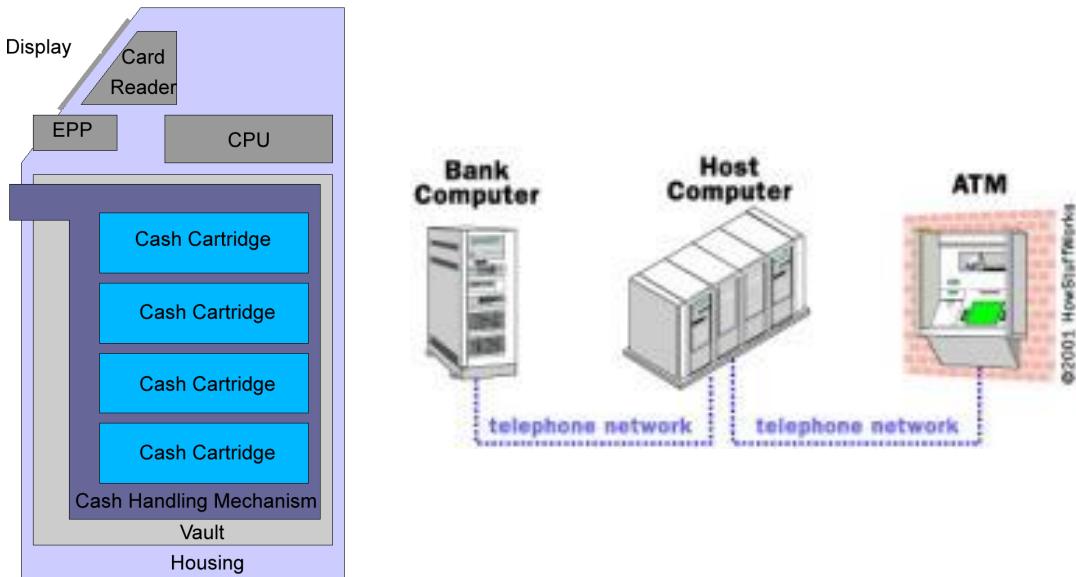
1.4 Daftar Singkatan

SINGKATAN	ARTI
ATM	Anjungan Tunai Mandiri (<i>Automated Teller Machine</i>)
PIN	<i>Personal Identification Number</i>
LED	<i>Light Emitting Diode</i>
GSM	<i>Global System for Mobile Communication</i>
SMS	<i>Short Message Service</i>
OTP	<i>One-Time Password</i>
COWS	<i>Criteria-Option-Weight-Scale</i>
TFT	<i>Thin Film Transistor</i>
LCD	<i>Liquid Crystal Display</i>
APDU	<i>Application Protocol Data Unit</i>
SQL	<i>Structured Query Language</i>

2 Konsep Sistem

2.1 Sistem Ideal

Mesin ATM ideal memiliki bentuk fisik yang cukup besar, diantaranya karena memiliki banyak komponen-komponen fisik seperti brankas uang, printer resi transaksi, dan lainnya. Sistem komputer dari mesin ATM sendiri biasanya terpusat, dengan menggunakan sebuah komputer utama yang mengatur seluruh operasinya.



Gambar 1 Sistem dan Jaringan ATM yang ada.

Berikut adalah bagian komponen yang biasanya terdapat pada mesin ATM:

- CPU utama
- *Magnetic stripe reader* atau *chip card reader*
- PIN pad dengan EEP (*Encrypting PIN Pad*)
- *Cryptoprocessor*
- Display monitor
- Tombol kendali menu
- *Record printer*
- Brankas
- Kerangka mesin
- Sensor

Mesin ATM tempo dulu biasanya menggunakan mikrokontroler khusus dengan arsitektur tersendiri sebagai CPU utamanya. Namun mesin ATM yang lebih modern telah menggunakan arsitektur menyerupai *Personal Computer* dengan *Operating System* karena kebutuhan komputasi yang lebih tinggi dan harga komputer dengan arsitektur demikian yang lebih murah.

Tergantung jenis kartu yang dibacanya (magnetic stripe atau chip), maka mesin ATM akan memiliki card reader yang sesuai pula. Pada keypad juga terpasang blok enkripsi agar kode PIN dari pengguna selalu aman, dalam arti PIN pengguna bahkan tidak pernah diketahui

oleh mesin ATM ini sendiri pada programnya. Cryptoprocessor juga berfungsi untuk melakukan proses enkripsi-dekripsi dengan key management untuk melakukan proses enkripsi-dekripsi lainnya. Lalu tombol kendali menu adalah tombol pada sekitar area layar mesin ATM yang digunakan untuk memilih menu yang ada, mesin ATM terbaru biasanya telah memiliki touchscreen yang menggantikan fungsi tombol ini.

Output dari mesin ATM diantaranya adalah berupa tampilan di layar monitornya. Pada mesin ATM ini juga terdapat *record printer*, yaitu perangkat yang berfungsi untuk mencetak tanda bukti sah transaksi dengan mesin ATM. Lalu brankas digunakan untuk menyimpan lembaran uang, pada proses penarikan tunai, lembaran uang ini akan dikeluarkan dari brankas tersebut dengan mekanisme yang ada dengan jumlah yang tepat.

Semua komponen tersebut dilingkupi oleh kerangka mesin yang kuat, dan tertanam dengan kokoh di tanah (untuk model freestanding). Karena mesin ATM selalu memiliki stok uang yang besar, keamanan uang tersebut merupakan bagian terpenting. Oleh karena itu semua komponen yang ada selalu diintegrasikan di dalam kerangka mesinnya. Komponen-komponen yang berada di luar seperti keypad dan card reader merupakan bagian terlemah, sehingga banyak dimanfaatkan untuk kejahatan, namun pada dasarnya komponen-komponen ini masih terpasang dengan kuat pada mesin ATM, dan bentuk kejahatan pada fisik mesin ATM adalah berupa pemasangan perangkat baru, karena memang membongkar mesin ATM bukanlah hal yang dapat dilakukan. Dan untuk lebih memperketat keamanan ini, mesin ATM juga dilengkap berbagai sensor, seperti sensor termal, magnetik, dan lainnya. Sensor ini berfungsi untuk mendeteksi bila ada kerusakan fisik pada mesin ATM yang dapat membahayakan mesin ATM tersebut.

Jaringan ATM harus memiliki koneksi terhubung, dan berkomunikasi melalui sebuah host processor (pusat proses). Pusat proses yang disertai oleh Internet service provider (ISP) yg berfungsi sebagai jalur gateway untuk menuju keberbagai macam jaringan ATM dan menjadikan berfungsi bagi si pemegang kartu ATM. Pada umumnya, pusat proses yang mendukung dapat melalui Leased-line atau jalur kontrak (sewa) maupun mesin dial-up (telepon). Mesin Leased-line terhubung langsung pada pusat proses melalui empat kabel (four-wire), point-to-point, dedicated telephone line (pilihan jalur telepon). Dial-up ATMs terhubung ke pusat proses melalui sambungan telepon normal menggunakan modem dan sambungan nomor bebas pulsa, atau melalui penyedia layanan internet yang menggunakan akses nomor local. Leased-line ATMs disarankan untuk digunakan pada lokasi yang padat karena kemampuan kerja thru-put yg cukup berat, dan dial-up ATMs disarankan untuk digunakan pada toko atau lokasi yang tidak ramai dimana penggunaan hanya sekedar mengambil uang. Biaya yang diperlukan untuk sebuah mesin ATM dial-up kurang dari setengahnya mesin ATM leased-line. Biaya operasi mesin ATM dial-up juga hanya sebagian kecil dari biaya operasi mesin ATM leased-line.

Pusat proses mungkin dapat dimiliki oleh sebuah bank atau instansi keuangan, atau mungkin juga dimiliki oleh penyedia layanan internet yg berdiri sendiri. Jika dimiliki bank, biasanya hanya mendukung mesin ATM bank itu sendiri, dimana hanya proses tunggal yang tersedia bagi pemilik toko atau tempat usaha.

2.2 Pilihan Sistem

Sistem Keamanan Mesin ATM menggunakan sidik jari terdiri dari dua bagian yaitu hardware dan software. Masing-masing bagian mempunyai alternative desain yang dapat dikembangkan lebih lanjut. Desain hardware lebih fokus kepada pilihan arsitektur sistem, dimana terdapat keterhubungan antar subsistem dan komponen input-output serta metode penyimpanan datanya. Perbedaan ketiga desain hardware terletak pada metode

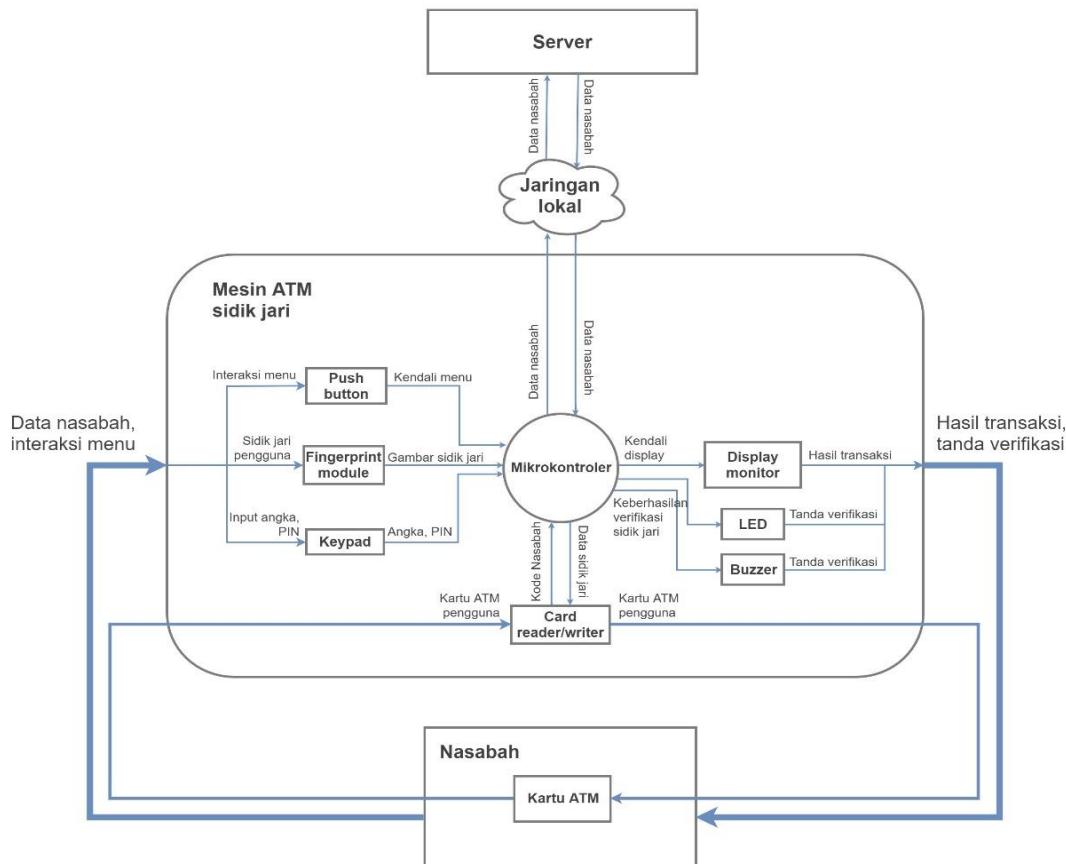
penyimpanan data sidik jari nasabah dan metode penambah sistem keamanannya. Desain software lebih fokus kepada algoritma yang digunakan untuk mengenali dan mencocokkan sidik jari yang terdapat pada *database*.

2.2.1 Pilihan Desain 1

- Arsitektur Sistem

Pada sistem ini, nasabah memasukkan input berupa kartu ATM dengan chip yang menyimpan kode nasabahnya dan data sidik jari. Setelah itu, data yang terdapat pada kartu ATM akan dibaca menggunakan card reader dan diverifikasi oleh mikrokontroler apakah sesuai dan betul merupakan nasabah bank yang bersangkutan dengan verifikasi data yang terdapat pada database server. Lalu proses verifikasi akan dilakukan dengan verifikasi PIN dan sidik jari. Input pin dilakukan seperti biasa menggunakan keypad yang tersedia. Input sidik jari diberikan user melalui *fingerprint module*, data yang diterima oleh fingerprint module akan diekstraksi oleh algoritma sidik jari pada mikrokontroler, lalu data sidik jari tersebut akan dibandingkan dengan data yang tersimpan di kartu ATMnya. Pada proses pengambilan input sidik jari pengguna, LED dan buzzer akan digunakan untuk menandakan bahwa proses pengambilan gambar sidik jari telah selesai dan pengguna dapat dilepas dari sensornya.

Setelah berhasil melakukan verifikasi sidik jari, menu ATM akan dapat diakses oleh pengguna. Pilihan menu akan dilakukan dengan push button yang ada seperti pada atm biasa. Lalu untuk setiap transaksi yang dilakukan, mikrokontroler akan melakukan komunikasi dengan server, karena proses-proses transaksi bank dilakukan oleh server. Lalu setiap proses transaksi yang dilakukan akan ditampilkan hasilnya di tampilan monitor.



Gambar 1 Pilihan Arsitektur Sistem Pertama

Desain sistem pertama ini masih menggunakan sistem PIN untuk verifikasi tambahan selain sidik jari. Hal ini ditujukan karena pengguna akan lebih terbiasa dengan metode verifikasi PIN dibanding metode lain. Proses input dari keypad akan dilakukan seperti keypad pada umumnya, dengan melakukan scanning keypad, yaitu misalnya dengan memberikan tegangan rendah pada pin kolom keypad, dan membaca nilai tegangan pada pin baris, bila ditemukan nilai tegangan rendah, maka tombol keypad koordinat tersebut sedang ditekan. Keypad yang kami gunakan pada desain ini tidak memiliki blok enkripsi-dekripsi seperti pada mesin ATM ideal karena terlalu sulit untuk diimplementasi. Verifikasi PIN akan terintegrasi dengan data nasabah yang tersimpan pada chip atau server.

Pada desain sistem pertama ini, kami memilih untuk menggunakan teknik desentralisasi, yaitu menyimpan data sidik jari di kartu ATM chip nasabah sehingga autentifikasi sidik jari hanya perlu mencocokkan dengan data yang ada pada kartu saja. Tingkat keamanan kartu ATM dengan chip cukup baik, sehingga data sidik jari dapat tersimpan dengan aman (aman dari *skimming*). Seandainya pencurian data kartu ATM cukup maju untuk dapat mencuri data dari kartu tersebut pun, data sidik jari sangat sulit untuk direkonstruksi ulang sehingga keamanan akun nasabah masih terjaga. Dengan tidak menyimpan data sidik jari pada database server, beban bandwidth jaringan yang digunakan untuk pertukaran data sidik jari antara mesin ATM dengan server akan berkurang. Data yang ada pada server hanya sebatas kode nasabah dan PIN untuk dicocokkan dengan yang terdapat pada chip kartu. Dengan beban jaringan yang lebih ringan, akan lebih banyak jumlah mesin ATM yang dapat dioperasikan dalam waktu bersamaan.

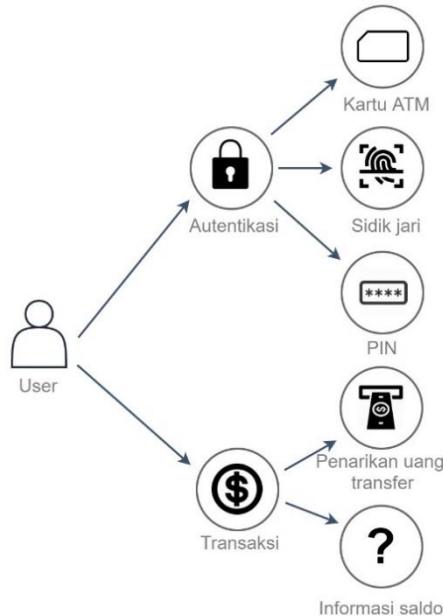
Berikut adalah daftar pemenuhan spesifikasi desain ini yang telah dijelaskan pada dokumen B200

Spesifikasi	Detail	Pemenuhan oleh desain 1
Sistem dilengkapi dengan sistem keamanan berlapis	Minimal 2 buah autentifikasi digunakan untuk melakukan transaksi	Dipenuhi oleh keberadaan kartu ATM, verifikasi PIN, dan sidik jari
Sistem memiliki tempat penyimpanan yang dapat digunakan untuk menyimpan ada rekening nasabah dan sidik jari	Sistem dapat menyimpan data 13.500 nasabah per bulannya dengan 4 buah sidik jari setiap nasabahnya	Dipenuhi oleh penyimpanan data nasabah di server dan sidik jari di kartu ATM sehingga tidak memiliki batas penyimpanan
Sistem tidak memakan waktu yang lama untuk melakukan transaksi	Lama waktu transaksi maksimal 2 menit	Dapat dipenuhi karena pencarian sidik jari dilakukan 1:4 yang hanya memakan waktu beberapa milisekon dan input PIN hanya akan memakan waktu beberapa detik
Menu ATM dapat digunakan untuk beberapa transaksi perbankan	Sistem dapat digunakan untuk melakukan 2 buah transaksi, yakni cek saldo dan penarikan tunai	Dipenuhi karena tersedia kedua fungsi transaksi tersebut

Mampu bekerja dengan kondisi yang ada di Indonesia	Sistem mampu beroperasi cukup dengan infrastruktur jaringan bank tersebut, iklim tropis, dan ditenagai oleh tegangan 220 AC	Dipenuhi karena sistem ini hanya membutuhkan jaringan bank; komponen yang dapat beroperasi pada iklim tropis Indonesia; dan dapat ditenagai oleh 220 AC
User interaction dapat dimengerti dan praktis oleh semua nasabah	User interaction menggunakan bahasa indonesia, lokasi tombol yang sesuai dengan interface, dan dimiliki oleh semua user	Dipenuhi karena kedua jenis transaksi tersebut akan disediakan oleh sistem ini
Mampu mengenali pola dan karakteristik sidik jari	Sistem mampu mengenali 2 buah Crossing Number (termination dan bifurcation) yang merupakan karakteristik minutiae sidik jari	Dipenuhi karena menggunakan metode minutiae matching untuk sidik jarinya

- Interaksi dengan Pengguna

Pada desain sistem pertama, interaksi user dapat digambarkan dengan diagram berikut



Gambar 2 Diagram Interaksi Sistem dengan User

Interaksi user terhadap sistem terjadi dalam 2 tahap yaitu pada proses autentikasi dan proses transaksi. Proses autentikasi pada dasarnya sama seperti pada ATM biasa, namun pada bagian verifikasi user, sistem juga akan meminta input sidik jari dari pengguna seperti yang telah dijelaskan sebelumnya. Kemudian, untuk keperluan pengujian, kami menambahkan fitur registrasi sidik jari agar dapat melakukan registrasi sidik jari tanpa sistem terpisah, pilihan ini akan ditemui bila nabasah belum memiliki data sidik jari pada kartu ATMnya.

Pada proses autentifikasi, selain memberikan input sidik jari, sistem juga akan meminta user untuk meletakkan kartu ATM pada card reader dan input PIN untuk verifikasi tambahan. Tampilan penerimaan input PIN adalah seperti berikut



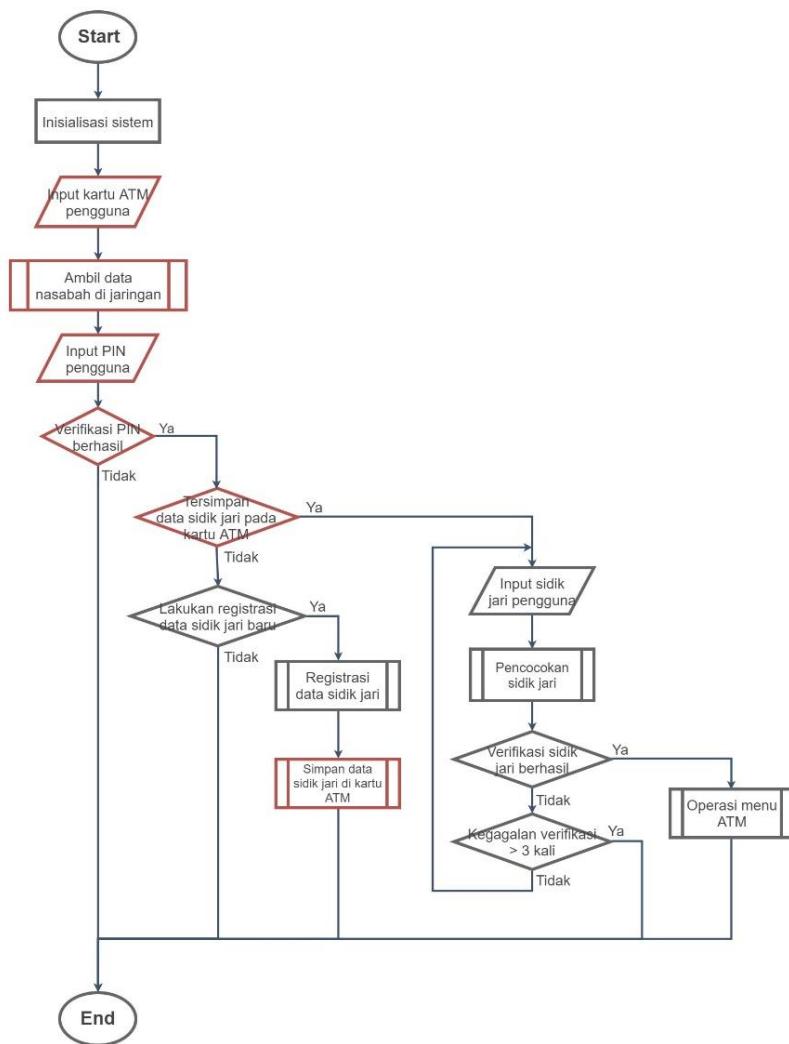
Gambar 3 User Interface Input PIN

Interaksi user lainnya adalah melakukan transaksi biasa seperti mengecek saldo, dan melakukan penarikan uang. User dapat menggunakan tombol untuk memilih menu transaksi dan juga menekan keypad angka untuk mengambil atau mentrasnfer jumlah uang yang diinginkan. Seluruh proses ini tentunya ditampilkan pada layar monitor.

Untuk sistem kami, proses registrasi sidik jari seharusnya dilakukan di bank, karena memerlukan arahan dari staf bank untuk mendapat pembacaan sidik jari yang tepat, juga untuk alasan keamanan. Namun kami memberikan mode registrasi pada mesin ini karena untuk keperluan demo tugas akhir dan pengujian sistem dengan mudah. Ketika melakukan registrasi, pengguna akan dituntun untuk menempelkan jarinya, lalu diulangi sekali lagi, bila kedua input sesuai maka registrasi sidik jari berhasil. Sidik jari yang diregistrasi kami tentukan adalah jempol dan telunjuk untuk kedua tangan.

- Algoritma Sistem

Berikut adalah flowchart dari program mesin ATM yang kami rancang untuk desain pertama secara umum



Gambar 4 Flowchart Sistem Desain Pertama

Pada sistem ini, pertama akan dilakukan inisialisasi sistem yang diperlukan. Lalu program akan menunggu untuk menerima kartu ATM, ketika kartu ATM terbaca, akan dicek terlebih dahulu apakah data nasabah terdapat pada jaringan server.

Proses pengecekan dilakukan dengan melakukan komunikasi ke server database, dan melakukan query untuk id nasabah yang tertera pada kartu ATM tersebut. Bila respon server mengatakan data tersebut benar ada di database maka pengguna valid.

Setelah itu, sistem akan meminta input PIN pengguna. Jika PIN benar, maka sistem akan mengecek apakah telah tersimpan data sidik jari pada kartu ATM tersebut. Bila belum, program akan meminta persetujuan pengguna untuk melakukan registrasi sidik jari, yaitu sidik jari telunjuk dan jempol masing-masing 2x, bila tidak diinginkan maka program akan dihentikan. Bila ingin melakukan registrasi, maka pengguna akan melalui serangkaian proses penerimaan input sidik jari. Jika benar maka data sidik jari akan disimpan pada kartu ATM. Dan program akan kembali ke awal untuk mengecek keberadaan data sidik jari pada kartu ATM.

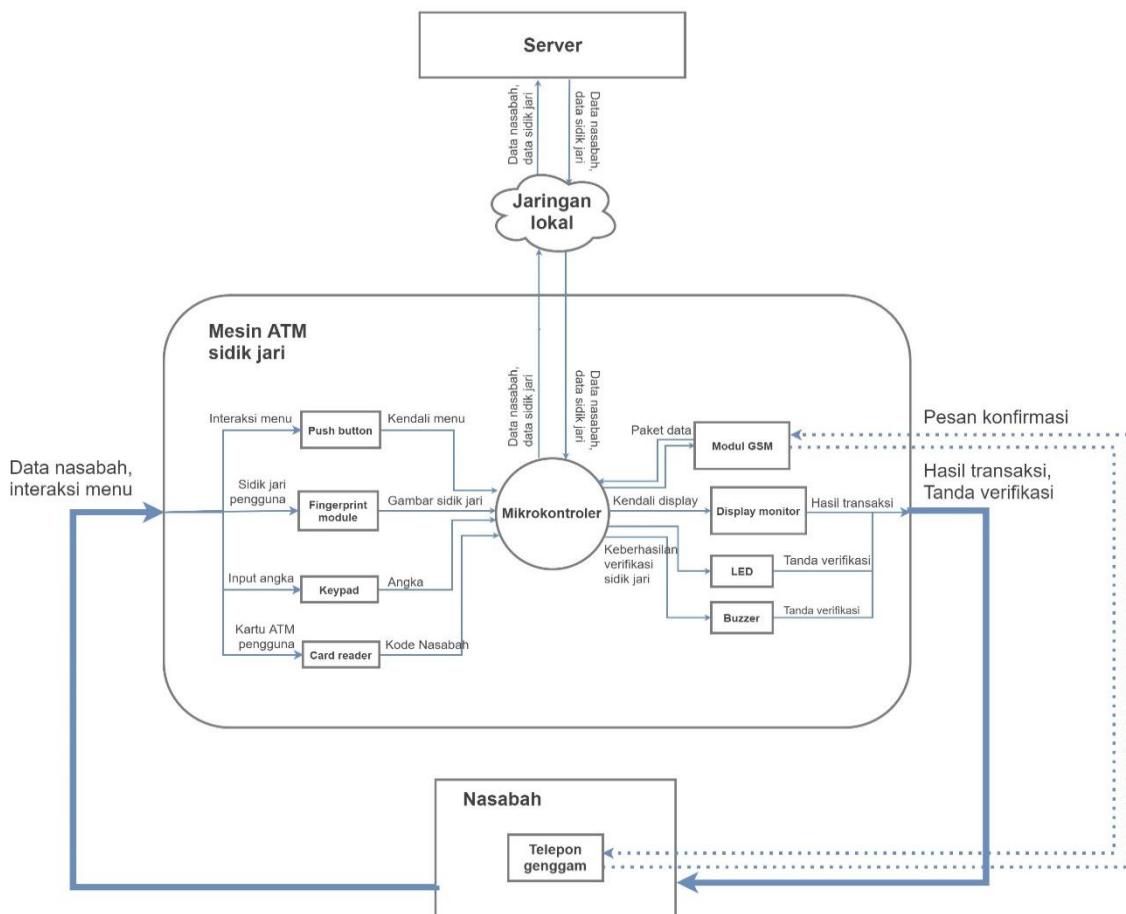
Bila ditemukan data sidik jari pada kartu ATM, maka sistem akan meminta sidik jari pengguna. Proses Pencocokan sidik jari dilakukan oleh mikrokontroler. Jika verifikasi sidik jari gagal lebih dari 3 kali, maka sistem akan berakhir. Jika tidak, maka sistem akan meminta memasukkan sidik jari kembali. Ketika telah diverifikasi benar, maka pengguna dapat

masuk ke menu transaksi ATM dan menggunakan pilihan transaksi yang ada. Setelah seluruh transaksi selesai dilakukan, maka sistem akan berakhir dan kembali ke proses awal untuk user atau nasabah berikutnya.

2.2.2 Pilihan Desain 2

- Arsitektur Sistem

Pada arsitektur ini, data berasal dari nasabah yang pertama-tama memasukkan input berupa kartu ATM dan *scanning* sidik jari pada *fingerprint module*. Pola sidik jari dan ID kartu yang terbaca akan diolah dengan menggunakan mikrokontroler lalu dicocokkan dengan data nasabah termasuk sidik jari yang terdapat pada database server melalui jaringan lokal. Untuk menandakan user mengangkat jarinya, mikrokontroler akan memberikan perintah pada LED dan Buzzer untuk mengeluarkan output berupa suara dan nyala LED. Keberhasilan verifikasi ditunjukkan oleh display monitor. Setelah terautentifikasi, terjadi pertukaran informasi dua arah antara mikrokontroler, modul GSM, dan telepon genggam nasabah. Pesan konfirmasi akan dikirimkan ke telepon genggam nasabah dari Modul GSM dan nasabah akan mengirimkan balik pesan konfirmasi berupa SMS 4 digit kode OTP yang menandakan bahwa benar nasabah yang bersangkutan sedang melakukan transaksi ke mikrokontroler. Setelah semuanya terverifikasi, mikrokontroler akan melanjutkan proses untuk menerima input kembali berupa pilihan transaksi dari push-button dan jumlah transaksi dari keypad dan mengolah serta menampilkan outputnya pada display monitor. Oleh karena semua proses diatur oleh satu buah mikrokontroler, dibutuhkan mikrokontroler 32 bit agar proses pengolahan berjalan dengan cepat demi kenyamanan nasabah.



Gambar 5 Pilihan Arsitektur Sistem Kedua

Desain Sistem Kedua menggunakan Modul GSM sebagai keamanan tingkat selanjutnya dan Server sebagai tempat penyimpanan seluruh data nasabah. Modul Global System Mobile (GSM) merupakan peralatan yang didesain agar dapat digunakan untuk aplikasi komunikasi dari mesin ke mesin atau dari manusia ke mesin. Modul GSM itu sendiri dapat terintegrasi dengan mikrokontroler. Dalam aplikasi yang dibuat, mikrokontroler yang bertugas mengirimkan perintah kepada modul GSM berupa AT command melalui RS232 sebagai komponen penghubung (communication links). Modul GSM merupakan bagian dari pusat kendali yang berfungsi sebagai transceiver. Modul GSM mempunyai fungsi yang sama dengan sebuah telepon seluler yaitu mampu melakukan fungsi pengiriman dan penerimaan SMS. Di dalam kebanyakan handphone dan GSM modem terdapat suatu komponen wireless modem/engine yang dapat diperintah antara lain untuk mengirim suatu pesan SMS dengan protokol tertentu. Standar perintah tersebut dikenal sebagai AT-Command, sedangkan protokolnya disebut sebagai PDU (Protokol Data Unit). Melalui AT-Command dan PDU inilah kita dapat membuat komputer/mikrokontroler mengirim/menerima SMS secara otomatis berdasarkan program yang dibuat.

Desain Sistem Kedua juga akan menggunakan sentralisasi, yaitu Database Server sebagai tempat penyimpanan data nasabah termasuk data sidik jari. Database server adalah sebuah program komputer yang menyediakan layanan pengelolaan basis data dan melayani komputer atau program aplikasi basis data yang menggunakan model klien/server. Jenis database server yang digunakan adalah In-memory Databases. Database di memori terutama bergantung pada memori utama untuk penyimpanan data komputer. Ini berbeda dengan sistem manajemen database yang menggunakan disk berbasis mekanisme penyimpanan. Database memori utama lebih cepat daripada dioptimalkan disk database sejak Optimasi algoritma internal menjadi lebih sederhana dan lebih sedikit CPU mengeksekusi instruksi. Mengakses data dalam menyediakan memori lebih cepat dan lebih dapat diprediksi kinerja dari disk. Sistem manajemen basis data (SMBD) pada umumnya menyediakan fungsi-fungsi server basis data, dan beberapa SMBD (seperti halnya MySQL atau Microsoft SQL Server) sangat bergantung kepada model klien-server untuk mengakses basis datanya. Data kecil sidik jari yang dikirimkan dari hasil pemrosesan mikrokontoler melalui jaringan local, disimpan sebagai template dalam database pada server yang sesuai dengan kode atau ID nasabah masing-masing. Manfaat dari menggunakan database server adalah bahwa banyak pengguna dapat mengakses database sidik jari ini pada waktu yang sama. Ini adalah cara yang efisien untuk menyediakan layanan kepada banyak orang semua pada waktu yang sama. Selain itu, manfaat lain menggunakan database server adalah keamanan.

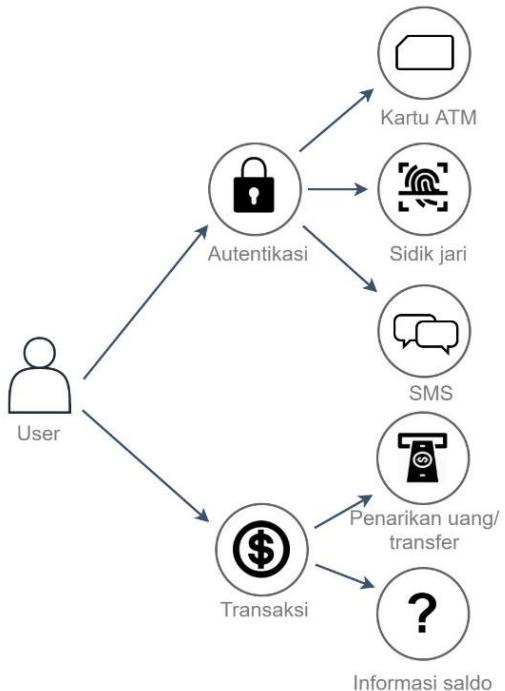
Berikut adalah daftar pemenuhan spesifikasi desain ini yang telah dijelaskan pada dokumen B200

Spesifikasi	Detail	Pemenuhan oleh desain 2
Sistem dilengkapi dengan sistem keamanan berlapis	Minimal 2 buah autentifikasi digunakan untuk melakukan transaksi	Dipenuhi oleh keberadaan kartu ATM, verifikasi SMS, dan sidik jari
Sistem memiliki tempat penyimpanan yang dapat digunakan untuk menyimpan ada rekening nasabah dan sidik jari	Sistem dapat menyimpan data 13.500 nasabah per bulannya dengan 4 buah sidik jari setiap nasabahnya	Dipenuhi oleh penyimpanan data nasabah dan sidik jari di server sehingga tidak memiliki batas penyimpanan

Sistem tidak memakan waktu yang lama untuk melakukan transaksi	Lama waktu transaksi maksimal 2 menit	Dapat dipenuhi namun relatif lebih sulit karena walaupun pencarian sidik jari dilakukan juga 1:4 yang hanya memakan waktu beberapa milisekon, proses verifikasi SMS akan memperlama waktu verifikasi pengguna
Menu ATM dapat digunakan untuk beberapa transaksi perbankan	Sistem dapat digunakan untuk melakukan 2 buah transaksi, yakni cek saldo dan penarikan tunai	Dipenuhi karena tersedia kedua fungsi transaksi tersebut
Mampu bekerja dengan kondisi yang ada di Indonesia	Sistem mampu beroperasi cukup dengan infrastruktur jaringan bank tersebut, iklim tropis, dan ditenagai oleh tegangan 220 AC	Dapat dipenuhi namun relatif lebih sulit karena verifikasi SMS dengan modul GSM membutuhkan infrastruktur jaringan GSM, yang sudah tersedia cukup umum di Indonesia namun belum merata di seluruh lokasi di Indonesia; komponen dapat beroperasi di iklim tropis Indonesia; dan sistem ini dapat ditenagai oleh 220 AC
User interaction dapat dimengerti dan praktis oleh semua nasabah	User interaction menggunakan bahasa indonesia, lokasi tombol yang sesuai dengan interface, dan dimiliki oleh semua user	Dipenuhi karena kedua jenis transaksi tersebut akan disediakan oleh sistem ini
Mampu mengenali pola dan karakteristik sidik jari	Sistem mampu mengenali 2 buah Crossing Number (termination dan bifurcation) yang merupakan karakteristik minutiae sidik jari	Dipenuhi karena menggunakan metode minutiae matching untuk sidik jarinya

- Interaksi dengan Pengguna

Pada desain sistem kedua, terdapat beberapa interaksi sistem dengan pengguna yang sebenarnya sudah tergambar pada arsitektur sistem kedua di poin sebelumnya. Secara spesifik, interaksi dapat digambarkan dengan diagram berikut



Gambar 6 Diagram Interaksi Sistem dengan User

Interaksi sistem dengan user terjadi ketika user ingin melakukan transaksi bank. User dapat menggunakan tombol untuk memilih menu transaksi dan juga menekan keypad angka untuk mengambil atau mentrasnfer jumlah uang yang diinginkan. Seluruh proses ini tentunya ditampilkan pada layar monitor.

Interaksi utama sebenarnya terjadi pada proses autentifikasi nasabah setelah memasukkan kartu ATM dan sebelum memilih jenis transaksi yang akan dilakukan, yaitu autentifikasi sidik jari dan autentifikasi SMS melalui nomor telepon genggam nasabah. Pertama, data pada kartu ATM diverifikasi terlebih dahulu dengan data nasabah pada server. Autentifikasi sidik jari dilakukan dengan cara user meletakkan jenis jari yang digunakan pada saat registrasi pada modul fingerprint mencocokkan kesamaan pola sidik jari dengan yang ada pada database. User akan mengetahui kapan harus mengangkat jarinya kembali dengan notifikasi suara dari buzzer dan nyala lampu dari LED. Keberhasilan autentifikasi akan ditunjukkan pada display monitor. Jika tidak berhasil, maka user perlu mengulang lagi proses autentifikasinya.

Autentifikasi SMS dilakukan dengan cara modul GSM mengirimkan user interface kepada user dalam bentuk SMS ke nomor telepon genggam user yang sudah terdaftar. Modul GSM akan mengirimkan pesan verifikasi apakah benar orang yang melakukan transaksi adalah user pemilik kartu ATMnya sendiri. Autentifikasi tidak hanya terjadi pada saat transaksi saja, tetapi juga terjadi pada saat registrasi sidik jari dengan tujuan agar sidik jari yang terdaftar adalah user pemilik kartu ATM. Setelah user mengetikkan dan mengirimkan 4 kode OTP, modul SIM akan menerima kode tersebut lalu dilakukan pengecekan. Jika autentifikasi benar, maka user sudah terbukti benar sehingga user dapat melakukan transaksi sesuai dengan keinginannya. Agar lebih jelas interaksi yang terjadi, dapat dilihat contoh gambaran user interface pada telepon genggam di bawah ini

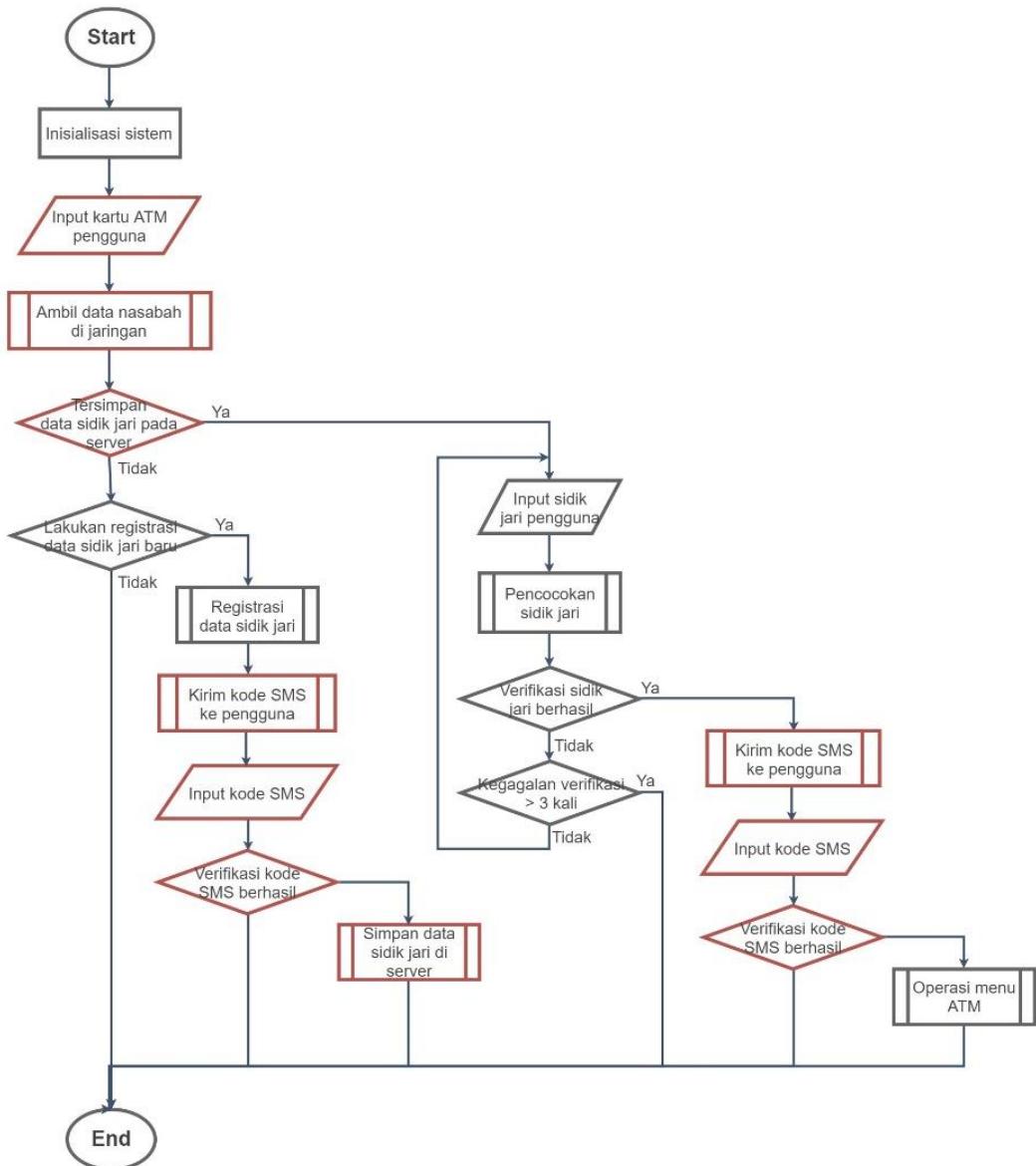


Gambar 7 User Interface SMS

Untuk desain 2 ini, sama seperti desain 1, proses registrasi sidik jari seharusnya dilakukan di bank. Untuk alasan yang juga seperti pada desain 1. Dan sidik jari yang diregistrasi kami tentukan juga adalah jempol dan telunjuk untuk kedua tangan.

- **Algoritma Sistem**

Algoritma sistem dapat dilihat dari aliran data secara keseluruhan data dan kemungkinan yang dapat terjadi pada setiap subsistem. Keseluruhan subsistem akan diatur oleh mikrokontroler sebagai pengolah data dan kontrol. Algoritma sistem desain kedua adalah



Gambar 8 Flowchart Desain Sistem Kedua

Algoritma sistem ini dimulai dari inisialisasi sistem. Inisialisasi ini berupa persiapan modul fingerprint, menyalakan power secara keseluruhan, dan mempersiapkan user interface pertama. Setelah sistem sudah menyala secara keseluruhan, user pertama-tama akan memasukkan kartu ATM miliknya. Kartu ATM tersebut lalu akan diverifikasi dengan data nasabah yang ada pada server bank.

Proses pengecekan dilakukan dengan melakukan komunikasi ke server database, dan melakukan query untuk id nasabah yang tertera pada kartu ATM tersebut. Bila respon server mengatakan data tersebut benar ada di database maka pengguna valid. Selanjutnya akan dicek lebih lanjut dengan subfungsi apakah sidik jari nasabah sudah ter-registrasi dan tersimpan pada database tersebut.

Apabila belum terdapat data sidik jari, sistem akan masuk ke tahap registrasi, dimana user akan mendaftarkan sidik jari dengan jari jempol dan telunjuk masing-masing sebanyak 2 kali. Data sidik jari tersebut akan diolah terlebih dahulu menjadi fitur untuk *matching*. User juga akan diverifikasi terlebih dahulu dengan SMS apakah benar akan melakukan registrasi

sidik jari. Baru setelah itu data dikirim ke server dan disimpan di database sesuai dengan kode atau ID nasabah dan setelah itu sistem akan kembali mengecek database server.

Apabila sudah terdapat data sidik jari, sistem akan masuk ke tahap autentifikasi, dimana sensor akan mendeteksi sidik jari user yang telah ter-registrasi. Mikrokontroler akan melakukan *image processing* untuk fungsi *fingerprint matching* dengan mengekstraksi data sidik jari lalu dicocokkan dengan yang tersimpan pada database. Jika tidak sesuai dengan yang tersimpan pada database, sistem akan meminta user untuk mengulang verifikasi sidik jari sampai dengan 3 kali. Namun, jika sudah sesuai, sistem akan masuk ke tahap autentifikasi kedua dengan mengirim kode OTP kepada *mobile phone user* melalui SMS. Sistem kemudian akan mengecek kesamaan kode yang dikirimkan oleh user melalui SMS juga. Jika kode berbeda, maka sistem akan mengirimkan notifikasi kembali bahwa kode yang dimasukkan tidak sesuai dan sistem berakhir. Namun, jika kode sama, sistem akan memberi tahu mikrokontroler untuk melanjutkan proses berikutnya yaitu ke subfungsi operasi menu ATM. Pada subfungsi ini, sistem akan menerima transaksi yang diinginkan oleh user. Setelah seluruh transaksi selesai dilakukan, maka sistem akan berakhir dan kembali ke proses awal untuk user atau nasabah berikutnya.

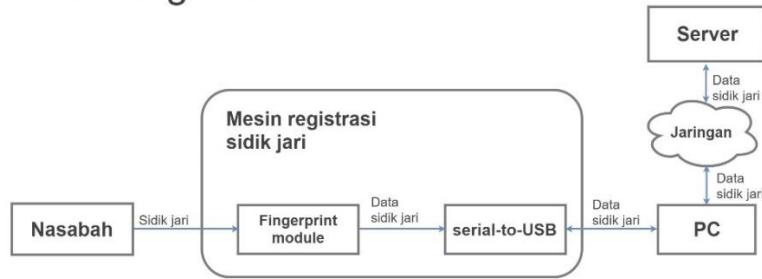
2.2.3 Pilihan Desain 3

- Arsitektur Sistem

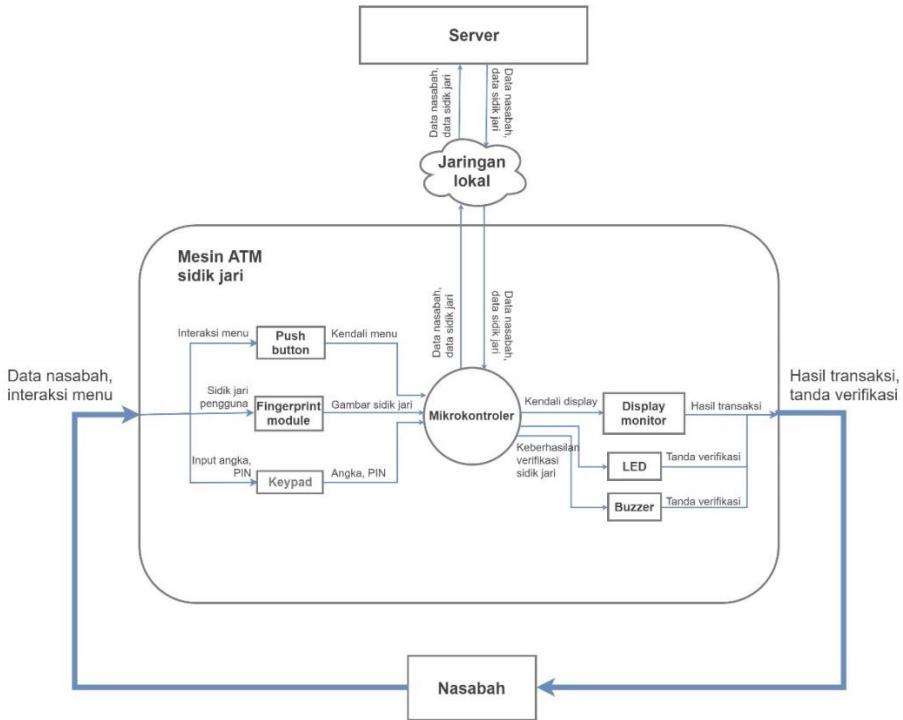
Desain Sistem Ketiga dirancang *cardless* atau tidak memerlukan kartu untuk melakukan transaksi pada mesin ATM dan juga data sidik jari tersimpan dalam memori local dalam jangka waktu tertentu. Oleh karena itu, dibutuhkan dua sistem yang berbeda, yaitu sistem untuk registrasi dan sistem untuk pemakaian. Registrasi sidik jari tidak dapat dilakukan pada mesin ATM secara langsung dengan alasan keamanan dan tidak adanya pengecekan data nasabah terlebih dahulu. Hal tersebut menyebabkan registrasi harus dilakukan pada sistem berbeda khususnya pada bank, dimana nasabah hanya perlu membawa dokumen-dokumen data nasabah yang dapat berupa buku tabungan atau nomor rekening atau bukti lainnya. Sensor fingerprint pada mesin registrasi akan menerima input sidik jari dari user yang kemudian dikomunikaskan ke PC melalui sambungan serial-to-USB. PC akan memproses data sidik jari sehingga diperlukan software tambahan, lalu dikirimkan ke server melalui suatu jaringan untuk disimpan pada database. Database server ini akan sama dengan database server yang ada pada mesin ATM.

Sistem untuk pemakaian berupa mesin ATM itu sendiri yang berisi komponen yang sama dengan desain sebelumnya hanya saja tidak terdapat *card reader*. Fingerprint Module akan menerima input sidik jari user. Mikrokontroler akan memproses sidik jari hasil output dari modul fingerprint untuk kemudian dicocokkan dengan yang terdapat pada memori local mesin ATM. Untuk menandakan user mengangkat jarinya, mikrokontroler akan memberikan perintah pada LED dan Buzzer untuk mengeluarkan output berupa suara dan nyala LED. Keberhasilan verifikasi ditunjukkan oleh display monitor. Jika belum ada sidik jari yang terkait, maka sistem melakukan pencocokan sidik jari yang sesuai dengan data pada server dan jika ditemukan, data tersebut akan disimpan dalam memori local mesin ATM selama setengah bulan untuk mempercepat verifikasi sidik jari user ketika akan melakukan proses transaksi berikutnya dalam jangka waktu tersebut. Setelah data sidik jari benar, maka keypad akan membaca tekanan user untuk memasukkan PIN yang akan dicocokkan kembali oleh mikrokontroler terhadap server. Setelah semuanya terverifikasi, mikrokontroler akan melanjutkan proses untuk menerima input kembali berupa pilihan transaksi dari push-button dan jumlah transaksi dari keypad dan mengolah serta menampilkan outputnya pada display monitor.

Sistem Registrasi



Sistem Pemakaian



Gambar 9 Pilihan Arsitektur Sistem Ketiga

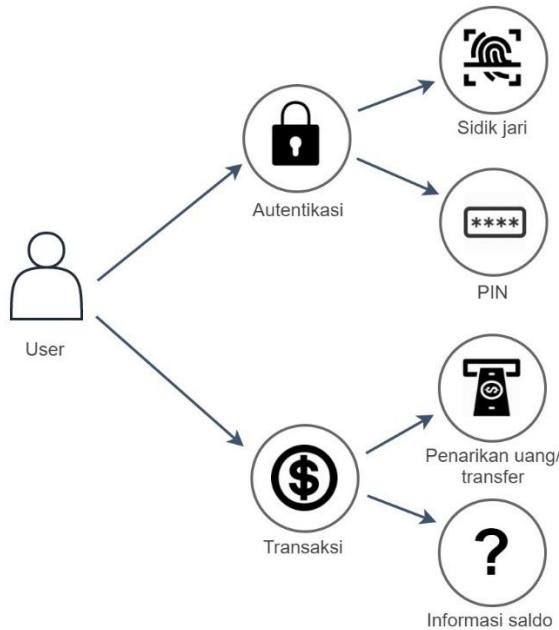
Berikut adalah daftar pemenuhan spesifikasi desain ini yang telah dijelaskan pada dokumen B200

Spesifikasi	Detail	Pemenuhan oleh desain 3
Sistem dilengkapi dengan sistem keamanan berlapis	Minimal 2 buah autentifikasi digunakan untuk melakukan transaksi	Dipenuhi oleh keberadaan verifikasi PIN dan sidik jari
Sistem memiliki tempat penyimpanan yang dapat digunakan untuk menyimpan ada rekening nasabah dan sidik jari	Sistem dapat menyimpan data 13.500 nasabah per bulannya dengan 4 buah sidik jari setiap nasabahnya	Dipenuhi oleh penyimpanan data nasabah di server, dan sidik jari di server juga memori lokal, sehingga batas penyimpanan hanya diatur oleh ukuran memori lokal yang menyimpan data tersebut yang dapat

diseduikan dengan kebutuhannya		
Sistem tidak memakan waktu yang lama untuk melakukan transaksi	Lama waktu transaksi maksimal 2 menit	Dapat dipenuhi namun sangat sulit karena pencarian sidik jari yang dilakukan 1:12600 bila merujuk spesifikasi no. 2 yang akan memakan waktu beberapa puluh detik, proses verifikasi PIN akan cukup cepat yaitu hanya beberapa detik.
Menu ATM dapat digunakan untuk beberapa transaksi perbankan	Sistem dapat digunakan untuk melakukan 2 buah transaksi, yakni cek saldo dan penarikan tunai	Dipenuhi karena tersedia kedua fungsi transaksi tersebut
Mampu bekerja dengan kondisi yang ada di Indonesia	Sistem mampu beroperasi cukup dengan infrastruktur jaringan bank tersebut, iklim tropis, dan ditenagai oleh tegangan 220 AC	Dipenuhi karena sistem ini hanya membutuhkan jaringan bank; komponen dapat beroperasi pada iklim tropis Indonesia; dan sistem dapat ditenagai oleh 220 AC
User interaction dapat dimengerti dan praktis oleh semua nasabah	User interaction menggunakan bahasa indonesia, lokasi tombol yang sesuai dengan interface, dan dimiliki oleh semua user	Dipenuhi karena kedua jenis transaksi tersebut akan disediakan oleh sistem ini
Mampu mengenali pola dan karakteristik sidik jari	Sistem mampu mengenali 2 buah Crossing Number (termination dan bifurcation) yang merupakan karakteristik minutiae sidik jari	Dipenuhi karena menggunakan metode minutiae matching untuk sidik jarinya

- Interaksi dengan Pengguna

Pada desain sistem ketiga, secara spesifik interaksi yang dapat dilakukan user digambarkan dengan diagram berikut



Gambar 10 Diagram Interaksi Sistem dengan User

Interaksi user pada sistem ketiga dibagi dua menjadi autentikasi dan transaksi. Pada autentikasi, user hanya memberikan data sidik jari dan PIN sebelum melakukan transaksi untuk menyatakan bahwa data user tersebut valid dan ada pada server bank yang bersangkutan. Input sidik jari dilakukan dengan meletakkan jari yang digunakan user saat registrasi pada fingerprint module lalu dan input PIN dilakukan dengan menekan tombol keypad yang ada. Keberhasilan autentifikasi akan ditampilkan pada user interface monitor.

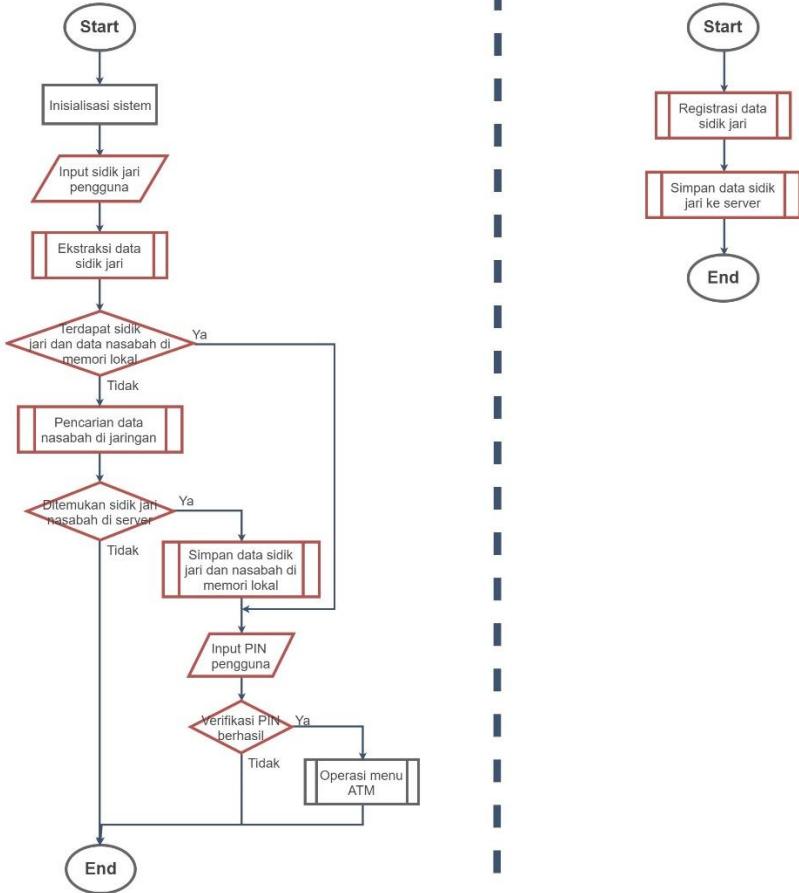
Pada saat transaksi, user dapat menarik uang dalam jumlah tertentu, atau hanya untuk cek informasi saldo saja. User interface yang ditampilkan kurang lebih sama dengan mesin ATM pada umumnya.

Untuk desain 3 ini, sama seperti desain 1, proses registrasi sidik jari seharusnya dilakukan di bank. Untuk alasan yang juga seperti pada desain 1. Namun secara eksplisit kamu buat kedua alat terpisah karena *Cardless ATM* ini tidak memiliki cara sama sekali untuk melakukan registrasi karena tidak ada cara verifikasi pengguna, disebabkan tidak adanya input kartu ATM. Sehingga untuk keperluan tugas akhir untuk demo alat kami akan perlu membuat alat spesifik untuk proses registrasi. Dan sidik jari yang diregistrasi kami tentukan juga adalah jempol dan telunjuk untuk kedua tangan.

- Algoritma Sistem

Terdapat dua buah algoritma pada desain sistem ketiga karena memang terdapat dua buah sistem yang berbeda sehingga cara kerjanya pun juga berbeda tetapi berhubungan. Algoritma desain sistem ketiga adalah sebagai berikut

Sistem Pemakaian | Sistem Registrasi



Gambar 11 Flowchart Sistem Desain Ketiga

Algoritma Sistem Registrasi cukup sederhana karena semua sudah diatur dalam subsistem tersendiri. Sistem ini diawali dengan registrasi sidik jari masing-masing jari sebanyak 2 kali, dimana di dalamnya terdapat teknik pengolahan ekstraksi fitur sidik jari user. Setelah itu, data sidik jari tersebut akan disimpan ke dalam server yang sama dengan server yang digunakan untuk pengecekan pada mesin ATM.

Algoritma Sistem Pemakaian diawali dengan user melakukan *scanning* sidik jari pada sensor yang tersedia pada mesin ATM. Kemudian, data tersebut akan diolah ekstraksi yang sama pada saat registrasi sehingga data tersebut dapat dicocokkan. Sistem akan mengecek apakah data sidik jari tersimpan dalam memori lokal mesin ATM. Jika tidak ada, maka sistem akan melakukan pencarian pola sidik jari yang sesuai atau sama dengan yang terdapat pada server database. Oleh karena itu, user yang akan menggunakan mesin ATM ini harus mendaftarkan sidik jarinya terlebih dahulu pada sistem registrasi (bank).

Proses pengecekan dilakukan dengan melakukan komunikasi ke server database, dan melakukan query untuk id nasabah yang tertera pada kartu ATM tersebut. Bila respon server mengatakan data tersebut benar ada di database maka pengguna valid. Selanjutnya akan dicek lebih lanjut dengan subfungsi apakah sidik jari nasabah sudah ter-registrasi dan tersimpan pada database tersebut.

Jika ditemukan, maka data sidik jari tersebut akan disimpan dalam memori lokal dalam jangka waktu tertentu untuk mempercepat pencarian sehingga sistem tidak perlu lagi untuk mencari data sidik jari melalui jaringan server. Jika memang dari awal data sidik jari sudah tersimpan di memori lokal, maka sistem akan langsung masuk ke tahap autentifikasi berikutnya, yaitu meminta input PIN dan jika PIN terverifikasi, operasi menu ATM akan terbuka, dimana di dalamnya terdapat menu transaksi yang dapat dipilih oleh user atau menu keluar jika ingin menyudahi atau membatalkan transaksi.

2.3 Analisis

2.3.1 Kriteria

Dalam pertimbangan desain, ada beberapa hal yang menjadi kriteria dalam mendesain sebuah sistem keamanan sidik jari pada mesin ATM. Berikut ini adalah kriteria yang menjadi dasar penilaian dalam menetapkan desain yang tepat pada sistem keamanan sidik jari pada mesin ATM.

- Keamanan

Keamanan menjadi salah satu kriteria yang patut dipertimbangkan dalam pemilihan desain pada mesin ATM. Bila meninjau pada B200, keamanan menjadi salah satu aspek yang menjadi poin penting di bagian spesifikasi. Oleh karena itu, keamanan menjadi kriteria yang dipakai dalam pemilihan desain.

Dalam kriteria ini, dengan mempertimbangkan faktor keamanan akan membuat kualitas dari desain mesin ATM menjadi semakin baik. Pada dasarnya, keamanan pada mesin ATM merupakan salah satu aspek yang harus dipenuhi pada setiap desain mesin ATM. Ketika kita membahas sistem keamanan pada mesin ATM, maka pokok bahasan tersebut akan berkaitan dengan sistem keamanan utama yang dipakai pada mesin serta dikombinasikan dengan sistem keamanan tambahan yang bertujuan untuk memperkuat sebuah sistem keamanan mesin ATM secara keseluruhan.

Sampai saat ini, jenis-jenis keamanan pada mesin ATM ada tersedia dalam beberapa bentuk. Namun, khusus di Indonesia sistem keamanan yang umum digunakan oleh penyedia jasa perbankan adalah sistem keamanan menggunakan kombinasi 6 digit PIN. Sistem keamanan lain yang mulai diterapkan di luar negeri adalah sistem keamanan menggunakan berbasis biometrik. Sistem keamanan yang berbasis biometrik ialah seperti sistem keamanan sidik jari, sistem keamanan pola retina, dan sistem keamanan menggunakan pengenalan wajah.

Selain itu, sistem keamanan berupa verifikasi menggunakan gadget juga mulai dipertimbangkan menjadi sistem keamanan yang dapat melengkapi sistem keamanan seperti di atas.

- Kecepatan

Kecepatan proses pada sistem merupakan salah satu kriteria yang penting dalam menetapkan desain alat yang akan dibuat. Kriteria kecepatan ini diturunkan dari bagian spesifikasi di dokumen B200. Pada bagian tersebut ditekankan bahwa proses transaksi tidak menghabiskan banyak waktu (maksimal 2 menit). Oleh karena itu, faktor kecepatan proses pada sistem menjadi salah satu poin yang menjadi kriteria yang muncul dari penurunan spesifikasi tersebut.

Mesin ATM yang baik haruslah mempertimbangkan aspek kecepatan untuk sistem yang dimilikinya. Seperti diketahui bersama, nasabah pengguna jasa perbankan tentunya memiliki latar belakang pekerjaan yang berbeda-beda. Diantara pekerjaan yang berbeda-beda tersebut tentulah ada pekerjaan yang membutuhkan waktu yang banyak dan fokus yang tinggi. Agar desain yang ada dapat memudahkan dan mengganggu

kegiatan sehari-hari *users* (para nasabah) dengan latar belakang pekerjaan yang berbeda-beda, maka kriteria kecepatan merupakan aspek yang sangat penting dalam proses pertimbangan desain.

- Kemudahan bagi pengguna

Aspek kemudahan bagi pengguna adalah salah satu hal yang penting dalam proses pertimbangan desain. Berdasarkan spesifikasi pada B200 yang menekankan kemudahan pengoperasian dengan user interaction yang mudah serta praktis. Hal tersebut menjadikan kemudahan user menjadi salah satu aspek yang perlu menjadi parameter dalam pemilihan desain.

Jika alat yang dibuat merupakan inovasi dari alat yang sudah ada sebelumnya di pasar maka aspek kemudahan dalam pengoperasianya adalah salah satu hal yang penting untuk dipertimbangkan. Hal ini bertujuan untuk membuat user tidak menjadi bingung dalam mengoperasikan alat yang bersangkutan.

Jika inovasi dari sebuah sistem yang dibuat cenderung berbeda dari sistem yang sudah ada maka kemungkinan besar pengguna akan mengalami kesusahan dalam pengoperasian alat tersebut sampai pengguna beradaptasi seiring dengan berjalananya waktu. Hal tersebut tentunya bukanlah sesuatu yang mudah bagi pengguna dalam mencoba mengoperasikan alat yang ada.

Cara mengukur kemudahan user secara kuantitatif adalah dengan menghitung jumlah alat yang harus dioperasikan. Sebagai contoh, mengoperasikan dua buah alat berbeda yang mempunyai fungsi saling melengkapi pada sebuah sistem akan menjadi jauh lebih tidak mudah dari pada mengoperasikan hanya satu alat untuk sebuah sistem keseluruhan.

- Stabilitas sistem

Stabilitas sistem merupakan kriteria diturunkan dari beberapa spesifikasi yang terdapat dalam dokumen B200 seperti sistem tidak memakan waktu lama pada saat transaksi dan sistem mampu bekerja pada kondisi yang ada di Indonesia. Pada bagian sistem yang tidak memakan waktu lama saat transaksi, stabilitas pada sistem akan berdampak pada kecepatan sistem dalam melakukan proses transaksi sehingga memakan waktu lama atau tidak. Untuk bagian spesifikasi yang berkaitan dengan kondisi di Indonesia, stabilitas pada sistem dapat dipengaruhi dari faktor luar seperti kondisi lingkungan dan infrastruktur suatu tempat dimana sistem tersebut berada, oleh karena itu akan sangat penting mendesain alat yang mengacu pada kondisi di Indonesia.

Sebuah alat yang baik tentulah harus memiliki stabilitas sistem yang baik. Apalagi ketika alat tersebut berkaitan dengan aspek yang penting dalam kehidupan sehari-hari seperti kegiatan perekonomian. Mesin ATM merupakan alat yang sangat erat kaitannya dengan sistem perekonomian, mulai dari transaksi pembelian dan pembayaran serta penarikan uang secara tunai, semuanya hal tersebut sangat erat kaitannya dengan proses perekonomian. Oleh karena itu, supaya proses perekonomian tetap berjalan lancar maka sistem pada alat haruslah memiliki stabilitas yang baik dalam melakukan setiap fungsinya.

- Biaya tambahan per transaksi

Dalam mendesain sebuah sistem keamanan keamanan pada mesin ATM, sistem yang baik seharusnya meminimalisir aspek biaya dalam proses keberlangsungannya. Hal tersebut bukanlah ditinjau dari sisi penyedia layanan perbankan saja, namun hal tersebut juga ditinjau dari sisi penggunanya (nasabah). Sudah menjadi barang umum di Indonesia bahwa sesuatu yang rendah biaya akan lebih diminati dari pada sesuatu dengan biaya yang lebih dengan kualitas yang sama. Secara umum, nasabah akan

memilih sistem yang tidak membebani nasabah dalam hal finansial untuk kualitas yang tidak jauh berbeda.

- Biaya instalasi dan *maintenance*

Alat ini di desain dengan tujuan untuk dipasarkan secara masif dan tetap mampu bekerja sesuai spesifikasi yang terlampir pada B200 seperti tidak membutuhkan banyak waktu untuk bertransaksi, mampu bekerja pada kondisi di Indonesia, mampu mengenali pola dan karakteristik sidik jari, dan sistem dapat dipakai untuk menyimpan data nasabah. Salah satu faktor yang muncul ketika dipasarkan secara masif adalah berhubungan dengan proses instalasi dari mesin ATM dan ketika alat diproyeksikan untuk bekerja tahan lama, *maintenance* adalah aspek yang harus dipertimbangkan supaya mesin ATM tetap dapat memenuhi spesifikasi yang tercantum.

Ketika kita berbicara instalasi, maka hal yang umum terbersit dalam benak kita adalah biaya dan kemudahan dalam instalasi. Dengan biaya yang rendah, sistem akan menjadi semakin diterima oleh konsumen (dalam hal ini operator jasa perbankan). Untuk kemudahan dalam instalasi, hal ini akan membuat pemasang menjadi semakin mudah dalam melakukan pekerjaan dan peluang terjadi kesalahan dalam pemasangan menjadi semakin kecil.

Sedangkan untuk alat yang diproyeksikan agar dapat digunakan dalam rentang waktu yang lama, perawatan adalah aspek yang menjadi pertimbangan mengingat semakin kompleks sebuah sistem tentulah membuat tingkat kesulitan perawatan menjadi semakin tinggi. Di sisi lain, banyaknya jumlah komponen dengan fungsi yang berbeda pada setiap komponen akan berakibat pada intensitas perawatan yang semakin banyak mengingat MTBF (*Mean Time Between Failures*) yang berbeda-beda setiap komponen.

2.3.2 Analisis konsep

Dari dua pilihan konsep sistem yang telah dikembangkan pada bagian 2.2, konsep desain pada pilihan sistem tersebut dinilai berdasarkan pertimbangan kriteria yang telah disampaikan pada 2.3.1. Berikut ini adalah hasil analisis konsep yang telah didesain berdasarkan kriteria yang ditetapkan.

➤ **Pilihan desain sistem 1**

Pada bagian ini, pilihan desain sistem 1 akan dianalisis menurut enam kriteria yang dirasa esensial sebagai pertimbangan dalam menentukan tepat atau tidaknya desain yang dipilih.

Berikut ini adalah analisis desain sistem 2 bedasarkan kriteria yang telah ditentukan sebelumnya

KRITERIA	DESAIN SISTEM 1
KEAMANAN	<ul style="list-style-type: none">• Sidik jari• Kombinasi 6 digit PIN• Memakai kartu Chip• Data sidik jari disimpan di kartu Chip
KECEPATAN	Data sidik jari disimpan di kartu Chip

KEMUDAHAN BAGI PENGGUNA	<ul style="list-style-type: none"> • Kombinasi 6 digit PIN • Sidik jari
KESTABILAN SISTEM	Server
BIAYA TAMBAHAN PER TRANSAKSI	Tidak ada
BIAYA INSTALASI DAN MAINTENANCE	Ada <i>card reader</i>

Untuk lebih jelasnya, berikut ini merupakan penjabaran dari analisis desain sistem berdasarkan kriteria yang telah ditetapkan

- Keamanan

Ketika membahas keamanan pada desain ini, fokus utama poin keamanan pada desain ini berfokus pada bagaimana untuk menjaga uang nasabah tetap aman.

Pada desain 1, sistem keamanan yang digunakan adalah sistem keamanan menggunakan sidik jari yang dikombinasikan dengan kombinasi 6 digit PIN. Pada kasus ini taraf keamanan pada sistem yang ada menjadi berlipat dua yaitu verifikasi sidik jari dan juga verifikasi PIN. Hal tersebut menjadikan proses verifikasi menjadi lebih susah untuk dimanipulasi karena memakai 2 buah tingkat dalam melakukan verifikasi terhadap barang.

Selain itu, dengan menggunakan pemakaian kartu berjenis chip dan bukan berjenis magnetik strip akan membuat informasi mengenai identitas nasabah menjadi tidak dapat untuk *diskimming*. Dengan kata lain, kartu menjadi aman dari tindakan pencurian identitas melalui *skimming* yang menjadi salah satu bentuk kejahatan paling umum ditemui saat ini pada mesin ATM.

- Kecepatan

Pada mesin ATM, isu kecepatan merupakan isu yang sangat penting untuk dijadikan sebagai bahan pertimbangan pada pemilihan desain sistem mesin ATM.

Desain sistem 1 ini menggunakan media penyimpanan sidik jari pada kartu chip. Pada sistem yang ada di mesin ATM, sidik jari dapat disimpan melalui 2 cara. Yang pertama sidik jari disimpan pada kartu ATM dan yang kedua sidik jari dapat disimpan pada data base di server. Sidik jari yang disimpan pada kartu memiliki kelebihan berupa kecepatan dalam melakukan verifikasi. Jika sidik jari disimpan di server maka mesin ATM harus terhubung dengan jaringan untuk melakukan verifikasi dengan ATM mesin ATM. Ketika terhubung pada jaringan, maka secara tidak langsung lebar *bandwidth* menjadi salah satu faktor yang mempengaruhi kecepatan. *Bandwidth* yang ada pada saat ini diset untuk jalur komunikasi akses akun dan PIN, ketika sidik jari yang notabanya berukuran jauh lebih besar dari pada PIN dilewatkan ke *bandwidth* maka ketika banyak ATM melakukan komunikasi proses transaksi secara bersamaan, maka lalu lintas data pada

jaringan akan penuh. Hal tersebut tentu mengakibatkan pada waktu transaksi yang terhambat.

- Kemudahan bagi pengguna

Kemudahan merupakan aspek yang harus dipertimbangkan pada desain sistem keamanan pada mesin ATM. Seperti diketahui bersama, ketika kita mendesain sebuah alat yang merupakan inovasi dari alat yang sudah ada pada *market*, salah satu hal yang perlu menjadi pertimbangan adalah kemudahan untuk pengoperasian oleh nasabah pengguna jasa perbankan. Ketika dilihat dari jenis sistem yang ada, ada 2 sistem keamanan yang digunakan yaitu sistem keamanan sidik jari dan sistem keamanan menggunakan kombinasi PIN. Jenis sistem keamanan dengan menggunakan sidik jari adalah sistem yang baru. Sedangkan untuk sistem keamanan tambahan menggunakan kombinasi PIN, sistem ini adalah sistem keamanan yang umum dipakai pada mesin ATM di Indonesia.

Ketika sistem pada sebuah alat sudah umum digunakan oleh pengguna (nasabah), dapat dikatakan bahwa pengguna sudah terbiasa dengan sistem tersebut. Dengan kata lain, sistem kemanan tambahan menggunakan kombinasi PIN memberikan kemudahan karena pengguna sudah terbiasa memakai sistem keamanan jenis ini.

Sesuatu hal yang baru disini adalah sistem keamanan menggunakan sidik jari. Dimungkinkan, nasabah akan mengalami kesulitan untuk pengoperasiannya di awal–awal sistem ini diterapkan karena ini merupakan sesuatu yang baru pada mesin ATM di Indonesia.

- Stabilitas sistem

Stabilitas dari sebuah sistem merupakan sebuah kriteria yang harus dipertimbangkan dalam melakukan pemilihan terhadap desain dari sistem pada sebuah alat yang akan dibuat. Semakin stabil sebuah sistem maka sistem menjadi semakin baik.

Pada desain sistem 1, dapat diamati bahwa salah satu gangguan yang mungkin dapat terjadi dan gangguan tersebut mengganggu stabilitas sistem dalam bekerja adalah ketika koneksi antara sistem dan server mengalami gangguan. Ketika koneksi antara mesin ATM dengan server mengalami gangguan, maka yang proses transaksi pada mesin ATM akan menjadi bermasalah. Hal tersebut tentunya akan berimbas pada kestabilan sebuah sistem secara keseluruhan.

- Biaya tambahan per transaksi

Pada desain sistem 1 ini, nasabah tidak perlu mengeluarkan biaya tambahan pada saat transaksi berlangsung. Proses yang terjadi pada sistem mulai dari proses verifikasi sidik jari, proses verifikasi dengan kombinasi PIN, proses transaksi, sampai proses akhir tidak membuat nasabah mengeluarkan biaya setiap biaya transaksi berlangsung.

Pada mesin ATM saat ini, biaya yang dikeluarkan pelanggan (nasabah) adalah biaya bulanan yang dibebankan pada nasabah untuk dapat memanfaatkan fasilitas pada mesin ATM. Biaya tersebut dipotong dari dana

pada akun nasabah setiap bulannya. Selain dari analisis biaya tersebut, nasabah tidak dibebankan untuk mengeluarkan biaya tambahan per transaksi, setiap nasabah melakukan aktivitas transaksi pada mesin ATM untuk desain sistem 1.

- Biaya instalasi dan *maintenance*

Pada aspek ini, desain sistem dipasangi dengan *card reader*. Jika dibandingkan dengan sistem yang *card less* yang tidak membutuhkan *card reader* maka sistem akan menjadi lebih mahal dalam segi biaya pemasangan. Faktor banyaknya komponen yang memiliki fungsi berbeda juga akan berpengaruh dengan intensitas perwatan mengingat MTBF (*Mean Time Between Failures*) setiap komponen yang berbeda-beda untuk setiap komponen dengan fungsi yang berbeda.

➤ Pilihan desain sistem 2

Pada bagian ini, pilihan desain sistem 2 akan dianalisis menurut enam kriteria yang dirasa esensial sebagai pertimbangan dalam menentukan tepat atau tidaknya desain yang dipilih.

Berikut ini adalah analisis desain sistem 2 bedasarkan kriteria yang telah ditentukan sebelumnya

KRITERIA	DESAIN SISTEM 2
KEAMANAN	<ul style="list-style-type: none"> • Sidik jari • Menggunakan verifikasi SMS via telepon seluler • Data sidik jari disimpan di server • Memakai kartu magnetik strip
KECEPATAN	<ul style="list-style-type: none"> • Menggunakan verifikasi SMS via telepon seluler • Data sidik jari disimpan di server
KEMUDAHAN BAGI PENGGUNA	<ul style="list-style-type: none"> • Menggunakan verifikasi SMS via telepon seluler • Sidik jari
KESTABILAN SISTEM	<ul style="list-style-type: none"> • Server • Menggunakan verifikasi SMS via telepon seluler
BIAYA TAMBAHAN PER TRANSAKSI	SMS via telepon seluler
BIAYA INSTALASI DAN MAINTENANCE	<ul style="list-style-type: none"> • Ada <i>card reader</i> • Ada modul GSM

Untuk lebih jelasnya, berikut ini merupakan penjabaran dari analisis desain sistem berdasarkan kriteria yang telah ditetapkan

- Keamanan

Ketika membahas keamanan pada desain ini, fokus utama poin keamanan pada desain ini berfokus pada bagaimana untuk menjaga uang nasabah tetap aman.

Pada desain 2 ini, sistem keamanan yang dipakai adalah sistem keamanan menggunakan sidik jari yang dikombinasikan dengan proses verifikasi melalui telepon seluler yang dimiliki oleh nasabah penyedia jasa perbankan. Dengan kata lain, ada dua tahapan dalam proses verifikasi pada yang harus dilalui nasabah agar dapat melakukan transaksi melalui mesin ATM. Dengan sistem keamanan yang berlipat yaitu menggunakan sidik jari dan juga melakukan verifikasi melalui telepon seluler, maka sistem keamanan akan menjadi semakin baik dari pada sistem keamanan yang ada pada mesin ATM yang ada di Indonesia saat ini.

Selain itu, desain sistem 2 ini juga menjadi semakin baik dalam hal keamanan ketika data sidik jari milik nasabah disimpan pada server dan bukan pada kartu ATM. Hal tersebut dikarenakan ketika kartu ATM dan telepon selular oleh dicuri oleh seseorang yang sama dan orang tersebut dapat mengekstrak data yang ada pada kartu chip yang sudah terenkripsi sebelumnya. Orang tersebut masih memerlukan sampel sidik jari dari nasabah untuk dapat melakukan pencurian uang milik nasabah yang bersangkutan. Dengan kata lain, untuk dapat mencuri uang nasabah, dibutuhkan 3 variabel yaitu kartu ATM, telepon selular, dan juga sidik jari dari nasabah yang bersangkutan.

Namun salah satu hal yang menjadi kekurangan pada desain sistem 2 dalam hal keamanan adalah pemakaian kartu ATM berupa magnetik strip. Pemakaian kartu jenis ini akan sangat rawan terhadap tindak kejahatan *skimming*. Namun informasi yang ada pada kartu hanya nomer identitas akun nasabah saja sehingga efek yang ditimbulkan tidaklah besar.

- Kecepatan

Pada mesin ATM, isu kecepatan merupakan isu yang sangat penting untuk dijadikan sebagai bahan pertimbangan pada pemilihan desain sistem mesin ATM.

Pada mesin ATM ada 2 tempat yang dapat dimanfaatkan untuk menyimpan sidik jari nasabah. Kedua tempat yang dimanfaatkan untuk melakukan penyimpanan sidik jari nasabah adalah kartu ATM atau server yang dikelola oleh penyedia jasa perbankan. Pada desain sistem 2 ini, yang digunakan sebagai media penyimpanan sidik jari nasabah adalah server milik penyedia jasa perbankan. Jika dilakukan analisis dari sisi kecepatan sistem, ketika sidik jari disimpan di server milik penyedia jasa perbankan, maka sistem tersebut memiliki potensi untuk menjadi lebih lambat jika dibandingkan dengan sistem dengan data sidik jari disimpan pada kartu ATM.

Alur koneksi antara server dengan mesin ATM lebih kompleks dan panjang dari pada alur koneksi antara mesin ATM dengan kartu ATM. Dengan kata lain, proses untuk verifikasi menjadi lebih lambat ketika data sidik jari harus diunduh dari server terlebih dahulu. Selain itu, hal lain yang paling umum ketika membahas soal server adalah lebar *bandwidth* yang dimiliki oleh

jaringan yang bersangkutan. *Bandwidth* yang dimiliki sistem ATM saat ini diseting untuk dapat dilewati oleh data akun nasabah dan kombinasi PIN 6 digit yang dimiliki oleh nasabah. Ketika *bandwidth* yang ada saat ini dipaksakan untuk dapat dilewati oleh data sidik jari yang notabanya lebih besar dari data kombinasi PIN 6 angka, maka ketika banyak ATM dipakai secara bersamaan dapat dipastikan lalu lintas data yang melewati *bandwidth* yang ada menjadi sangat padat. Hal tersebut tentunya akan berimbas pada kecepatan sistem karena lalu lintas data yang digunakan menjadi terhambat. Dengan kata lain, sistem akan bekerja lebih lambat.

- Kemudahan bagi pengguna

Kemudahan merupakan aspek yang harus dipertimbangkan pada desain sistem keamanan pada mesin ATM. Seperti diketahui bersama, ketika kita mendesain sebuah alat yang merupakan inovasi dari alat yang sudah ada pada *market*, salah satu hal yang perlu menjadi pertimbangan adalah kemudahan untuk pengoperasian oleh nasabah pengguna jasa perbankan.

Pada desain sistem 2 ini, sistem keamanan yang digunakan adalah sistem keamanan sidik jari yang dikombinasikan dengan verifikasi sms menggunakan telepon selular. Jenis sistem keamanan dengan menggunakan sidik jari dan verifikasi sms menggunakan telepon selular merupakan dua hal yang baru.

Ketika inovasi diterapkan pada sebuah mesin ATM, dan inovasi itu cenderung baru serta meninggalkan sistem keamanan yang ada, maka salah satu kriteria penting untuk menjadi pertimbangan dalam pemilihan desain adalah kemudahan mesin ATM yang dilihat sisi user yang dalam konteks ini adalah nasabah dari penyedia jasa perbankan. Pada umumnya, nasabah akan mengalami kesulitan untuk mengoperasionalkan sesuatu yang baru dari pada sesuatu yang telah lama digunakan. Oleh karena itu baik sistem keamanan menggunakan sidik jari maupun verifikasi sms menggunakan telepon selular kurang memudahkan nasabah dalam beberapa periode di awal-awal pemakaian karena kedua bentuk sistem keamanan ini merupakan sistem yang baru di mesin ATM di Indonesia.

Selain itu, pemakaian telepon selular juga dianggap mengurangi kemudahan dari nasabah dalam pengoperasian mesin ATM. Ketika melakukan kegiatan tarik tunai atau proses transaksi lain memakai mesin ATM, nasabah diharuskan membawa telepon seluler. Hal tersebut tentunya membuat kemudahan dari pengoperasian desain sistem menjadi berkurang. Faktor baterai yang lemah serta sinyal pada telepon selular juga dapat menjadi aspek yang membuat desain sistem dianggap kurang mudah untuk dioperasikan.

- Stabilitas sistem

Stabilitas dari sebuah sistem merupakan sebuah kriteria yang harus dipertimbangkan dalam melakukan pemilihan terhadap desain dari sistem pada sebuah alat yang akan diimplementasikan. Semakin kecil peluang sistem untuk terjadi kegagalan maka sistem dapat dikatakan menjadi semakin stabil dan efektif.

Pada desain sistem 2 ini, dapat kita amati bahwa salah satu gangguan yang mungkin dapat terjadi dan gangguan tersebut mengganggu stabilitas sistem dalam bekerja adalah ketika koneksi antara mesin ATM dan server mengalami gangguan. Ketika koneksi antara mesin ATM dengan server mengalami gangguan, maka yang proses transaksi pada mesin ATM akan menjadi bermasalah. Hal tersebut tentunya akan berimbas pada kestabilan sebuah sistem secara keseluruhan.

Selain dari faktor di atas, faktor digunakannya data telepon seluler sebagai media verifikasi juga dapat berpotensi membuat sistem menjadi tidak stabil dalam proses kerjanya. Ada beberapa hal yang membuat sistem menjadi kurang stabil ketika memanfaatkan perangkat telepon seluler menjadi media verifikasi tambahan pada sistem. Salah satu faktor yang menyebabkan adalah sinyal yang diterima oleh telepon seluler, ketika telepon seluler nasabah mengalami kesulitan dalam jaringan sinyalnya, maka notifikasi dari pihak penyedia jasa perbankan menjadi sulit untuk terkirim ke telepon seluler nasabah, hal ini tentunya akan sangat menggangu proses yang terjadi pada sistem. Selain dari hal tersebut, faktor baterai pada telepon seluler juga akan sangat berpengaruh kinerja pada sistem. Ketika baterai pada telepon pada kondisi yang “kritis” (sangat lemah) atau bahkan habis, maka proses pada sistem akan terganggu dan hal tersebut mempengaruhi kestabilan sistem secara keseluruhan. Selain faktor di atas, nasabah yang lupa membawa telepon selular juga akan mengalami kesulitan dalam melakukan verifikasi akun ketika menggunakan mesin ATM.

- Biaya transaksi

Mesin ATM yang ada pada saat ini membebankan biaya bulanan yang dipotong dari rekening nasabah agar nasabah bisa menikmati fasilitas mesin ATM yang disediakan oleh penyedia jasa perbankan. Biaya tersebut merupakan biaya bulanan tanpa melihat seberapa sering pengguna melakukan transaksi pada mesin ATM setiap bulannya.

Untuk desain sistem 2 ini, nasabah dikenakan biaya tambahan yang harus dikeluarkan oleh nasabah setiap kali nasabah menggunakan mesin ATM. Biaya tambahan tersebut berasal dari biaya sms yang diterima maupun dikirimkan oleh nasabah ketika nasabah melakukan transaksi menggunakan mesin ATM. Dengan kata lain, selain nasabah dibebani oleh biaya bulanan yang diambil melalui rekening nasabah, nasabah juga diharuskan untuk mengeluarkan biaya tambahan yang berasal dari penerimaan dan pengiriman sms dari telepon seluler milik nasabah ketika nasabah hendak melakukan aktivitas transaksi pada mesin ATM.

- Biaya instalasi dan *maintenance*

Pada aspek ini, desain sistem dipasangi dengan card reader. Jika dibandingkan dengan sistem yang card less yang tidak membutuhkan card reader dan sistem yang tidak membutuhkan modul GSM maka sistem akan menjadi lebih mahal dalam segi biaya pemasangan karena komponen yang dipasang menjadi semakin banyak.

Fator banyaknya komponen yang memiliki fungsi berbeda juga akan berpengaruh dengan intensitas perawatan mengingat MTBF (Mean Time Between Failures) setiap komponen yang berbeda-beda untuk setiap jenis komponen.

➤ Pilihan desain sistem 3

Pada bagian ini, pilihan desain sistem 3 akan dianalisis menurut enam kriteria yang dirasa esensial sebagai pertimbangan dalam menentukan tepat atau tidaknya desain yang dipilih.

Berikut ini adalah analisis desain sistem 3 bedasarkan kriteria yang telah ditentukan sebelumnya

KRITERIA	DESAIN SISTEM 3
KEAMANAN	<ul style="list-style-type: none"> • Sidik jari • Kombinasi 6 digit PIN • <i>Cardless</i> • Data sidik jari disimpan di server dan memori local
KECEPATAN	<ul style="list-style-type: none"> • Data sidik jari disimpan di mesin ATM • Simpan di server
KEMUDAHAN BAGI USER	<ul style="list-style-type: none"> • <i>Cardless</i> • Kombinasi 6 digit PIN • Sidik jari
KESTABILAN SISTEM	Server
BIAYA TAMBAHAN PER TRANSAKSI	Tidak ada
BIAYA INSTALASI DAN MAINTENANCE	Tidak ada <i>card reader</i> dan modul GSM

Untuk lebih jelaskannya, berikut ini merupakan penjabaran dari analisis desain sistem berdasarkan kriteria yang telah ditetapkan

- Keamanan

Ketika membahas keamanan pada desain ini, fokus utama poin keamanan pada desain ini berfokus pada bagaimana untuk menjaga uang nasabah tetap aman.

Pada desain 3 ini, sistem keamanan yang dipakai adalah sistem keamanan sidik jari yang dikombinasikan dengan kombinasi 6 buah PIN. Dengan kata lain, ada 2 tahapan verifikasi yang harus dilakukan nasabah agar bisa melakukan transaksi menggunakan mesin ATM. Pada sistem keamanan ganda tersebut, dibutuhkan dua buah informasi berupa sidik jari dan juga

kombinasi 6 buah PIN untuk dapat melakukan transaksi menggunakan akun nasabah yang bersangkutan.

Ketika melihat pada desain sistem 3 yang *cardless* (tanpa menggunakan kartu), hal tersebut justru membuat desain sistem menjadi kurang aman dari pada desain menggunakan kartu. Hal tersebut terjadi karena ketika pencuri ingin membobol akun ATM nasabah, maka pencuri hanya membutuhkan informasi berupa sidik jari dan juga kombinasi 6 digit PIN saja tanpa perlu mencuri kartu ATM milik nasabah yang bersangkutan.

- Kecepatan

Pada mesin ATM, isu kecepatan merupakan isu yang sangat penting untuk dijadikan sebagai bahan pertimbangan pada pemilihan desain sistem mesin ATM.

Pada mesin ATM ada 2 tempat yang dapat dimanfaatkan untuk menyimpan sidik jari nasabah. Kedua tempat yang dimanfaatkan untuk melakukan penyimpanan sidik jari nasabah adalah kartu ATM atau server yang dikelola oleh penyedia jasa perbankan. Namun pada desain sistem 3 ini, ada sedikit modifikasi mengenai tempat penyimpanan. Pada desain sistem 3 ini, digunakan 2 tempat penyimpanan sidik jari yaitu server dan mesin ATM. Server merupakan tempat penyimpanan primer dari sidik jari, sedangkan mesin ATM merupakan tempat penyimpanan sekunder dari sidik jari. Ketika nasabah menggunakan ATM yang baru, maka data sidik jari untuk verifikasi akan didapatkan pada server. Namun ketika nasabah sudah menggunakan mesin ATM yang sama sebelumnya dengan maksimal jarak dengan pemakaian selama seminggu, maka data sidik jari untuk proses verifikasi disimpan pada mesin ATM dengan rentang waktu maksimal 1 minggu setelah pemakaian terakhir nasabah yang bersangkutan pada mesin ATM yang sama. Hal ini tentunya akan sangat membutuhkan banyak waktu ketika sidik jari disimpan pada server. Hal tersebut karena harus dilakukan pencarian 1 banding N total sidik jari yang ada pada server belum lagi ketika bandwidth yang ada menjadi pertimbangan pada kecepatan. Namun ketika sidik jari pada mesin ATM, maka otomatis proses verifikasi dapat berlangsung dengan cepat.

- Kemudahan

Kemudahan merupakan aspek yang harus dipertimbangkan pada desain sistem keamanan pada mesin ATM. Seperti diketahui bersama, ketika kita mendesain sebuah alat yang merupakan inovasi dari alat yang sudah ada pada market, salah satu hal yang perlu menjadi pertimbangan adalah kemudahan untuk pengoperasian oleh nasabah pengguna jasa perbankan.

Desain sistem 3 ini merupakan desain yang memberikan kemudahan yang lebih dari pada desain yang lain. Hal ini mengacu pada ditiadakannya kartu ATM (*cardless*). Dengan tanpa menggunakan kartu ATM, nasabah tidak usah memikirkan kartu ATM lupa terbawa ataupun rusak. Untuk proses transaksi, nasabah hanya perlu melakukan verifikasi sidik jari dan juga kombinasi 6 digit PIN. Hal ini tentunya sangat memberikan kemudahan bagi nasabah untuk melakukan proses transaksi melalui mesin ATM.

- Stabilitas sistem

Stabilitas dari sebuah sistem merupakan sebuah kriteria yang harus dipertimbangkan dalam melakukan pemilihan terhadap desain dari sistem pada sebuah alat yang akan diimplementasikan. Semakin kecil peluang sistem untuk terjadi kegagalan maka sistem dapat dikatakan menjadi semakin stabil dan efektif.

Untuk desain sistem 3 ini, salah satu faktor yang menyebabkan sistem mengalami gangguan yang mengganggu stabilitas sistem adalah koneksi antara mesin ATM dengan server. Ketika koneksi antara mesin ATM dengan server mengalami gangguan, maka yang proses transaksi pada mesin ATM akan menjadi bermasalah. Hal tersebut tentunya akan berimbas pada kestabilan sebuah sistem secara keseluruhan.

- Biaya transaksi

Mesin ATM yang ada pada saat ini membebankan biaya bulanan yang dipotong dari rekening nasabah agar nasabah bisa menikmati fasilitas mesin ATM yang disediakan oleh penyedia jasa perbankan. Biaya tersebut merupakan biaya bulanan tanpa melihat seberapa sering pengguna melakukan transaksi pada mesin ATM setiap bulannya.

Selain biaya rutin bulanan di atas, tidak ditemukan biaya tambahan per transaksi yang dibebankan pada nasabah melalui sistem.

- Biaya instalasi dan *maintenance*

Desain model 3 merupakan desain yang sangat hemat jika dilihat dari biaya instalasi dan intensitas perawatan. Dengan minusnya *card reader* dan modul GSM, maka otomatis akan membuat biaya instalasi menjadi semakin hemat. Selain itu sedikitnya komponen yang terpasang juga akan mengakibatkan alat memiliki intensitas perawatan yang rendah dibandingkan alat yang memiliki komponen yang lebih banyak.

2.4 Sistem yang akan dikembangkan

2.4.1 Metode pemilihan

Metode penentuan keputusan yang digunakan untuk memilih antara desain pertama, desain kedua, dan desain ketiga adalah *Decision Matrix* dengan *Analytical Hierarchy Process*. Konsep *Analytical Hierarchy Process* diambil dari buku *Design for Electrical and Computer Engineering* karya Ralph M. Ford dan Chris S. Coulston (2008). Matriks keputusan adalah tabel yang memungkinkan orang atau sekelompok orang secara sistematis mengidentifikasi, menganalisis, dan menilai kekuatan hubungan antara sekelompok informasi. Sekelompok informasi tersebut bisa berupa pilihan, usulan, kejadian, obyek, atau hal lainnya yang akan dipilih. Salah satu metoda yang dapat digunakan untuk menyusun matrik keputusan yaitu metode AHP (*Analytical Hierarchy Process*)

Langkah pertamanya yaitu menentukan tingkatan/bobot kriteria. Untuk menentukannya digunakan *pairwise matrix* yaitu matriks yang akan membandingkan tingkatan kepentingan

kriteria tersebut satu per satu. Nilai-nilai tersebut kemudian dicari rata-rata geometriknya untuk setiap kriteria yaitu

$$\text{Geometric mean} = \sqrt[n]{a_1 a_2 \dots a_n}$$

Kemudian nilai tersebut dijumlahkan, dan nilai bobot untuk setiap kriteria didapat dari perbandingan nilai rata-rata geometrik kriteria tersebut dengan total untuk semua kriteria.

Tabel 1 – Perbandingan Kepentingan Kriteria

	Keamanan sistem	Kecepatan sistem	Kemudahan bagi pengguna	Kestabilan sistem	Biaya tambahan per transaksi	Biaya instalasi dan maintenance
Keamanan sistem	1	3	5	5	7	7
Kecepatan sistem	$\frac{1}{3}$	1	3	3	5	5
Kemudahan bagi pengguna	$\frac{1}{5}$	$\frac{1}{3}$	1	1	3	3
Kestabilan sistem	$\frac{1}{5}$	$\frac{1}{3}$	1	1	3	3
Biaya tambahan per transaksi	$\frac{1}{7}$	$\frac{1}{5}$	$\frac{1}{3}$	$\frac{1}{3}$	1	1
Biaya instalasi dan maintenance	$\frac{1}{7}$	$\frac{1}{5}$	$\frac{1}{3}$	$\frac{1}{3}$	1	1

Tabel 2 – Penentuan Bobot Kriteria

	Geometric mean	Bobot
Keamanan sistem	3.92	0.45
Kecepatan sistem	2.05	0.24
Kemudahan bagi pengguna	0.92	0.11
Kestabilan sistem	0.92	0.11
Biaya tambahan per transaksi	0.38	0.04
Biaya instalasi dan maintenance	0.38	0.04

Didapat bobot untuk setiap kriteria adalah demikian. Kemudian nilai/rating untuk setiap desain untuk masing-masing kriteria didapatkan dengan cara yang sama. Berikut adalah perhitungan rating untuk setiap desain dan kriteria dengan skor desain per kriteria kami berada dalam rentang 0 – 10 dengan keterangan sebagai berikut:

- 0 = Desain tidak memenuhi kriteria
- 5 = Desain memenuhi sebagian dari kriteria
- 10 = Desain sangat memenuhi kriteria

Keamanan Sistem

KRITERIA	DESAIN SISTEM 1	DESAIN SISTEM 2	DESAIN SISTEM 3
KEAMANAN	+ Sidik jari (+3) + Kombinasi 6 digit PIN (+1) + Memakai kartu Chip (+2) ± Data sidik jari disimpan di kartu Chip (+1)	+ Sidik jari (+3) + Menggunakan verifikasi SMS via telepon seluler (+3) + data sidik jari disimpan di server (+3) - Memakai kartu magnetik strip (+0)	+ Sidik jari (+3) + Kombinasi 6 digit PIN (+1) + Data sidik jari disimpan di server dan memori local (+1) - <i>Cardless</i> (+0)
TOTAL	+7	+9	+5

1. Desain sistem 1

Pada desain sistem 1 ini, sistem keamanan yang dipakai adalah sistem keamanan sidik jari yang dikombinasikan dengan 6 digit PIN. Keamanan semakin bertambah ketika memakai kartu chip karena tidak bisa di *skimming*. Namun data sidik jari dapat yang disimpan di chip akan dapat menimbulkan pencurian database sidik jari ketika ada peretas yang dapat membobol identitas dan informasi terkait verifikasi nasabah melalui katu ATM.

2. Desain sistem 2

Sistem keamanan pada desain ini meliputi kombinasi sidik jari dan verifikasi SMS oleh nasabah dan nasabah juga di bekali dengan kartu ATM. Selain itu, database sidik jari juga disimpan di server akan memperkuat sistem keamanan yang ada. Untuk dapat mencuri uang pada sistem ini, pencuri harus memiliki 3 hal yang harus dipenuhi yaitu sidik jari nasabah, telepon seluler nasabah dan juga kartu ATM nasabah. Kelemahan dari sistem ini adalah masih dipakainya kartu magnetik strip, pemakaian kartu tersebut akan membuat informasi pada kartu rawan *diskrimming*. Namun efek dari skimming pada sistem ini tidak terlampau besar, karena kartu hanya menyimpan data informasi nasabah saja, sedangkan data verifikasi disimpan di server.

3. Desain sistem 3

Sistem keamanan pada desain ini adalah kombinasi dari sidik jari dan kombinasi 6 digit PIN saja tanpa dilengkapi dengan kartu ATM. Dengan demikian, untuk dapat membobol sistem, peretas hanya perlu mendapat sidik jari dan kombinasi 6 digit PIN milik nasabah saja. Sidik jari dapat dicuri dengan menggunakan teknik-teknik tertentu dan PIN dapat dicuri menggunakan teknik PIN capturing.

Berikut adalah tabel penilaian untuk kriteria keamanan sistem

Tabel 3 – Penentuan Rating Keamanan Sistem

	Desain 1	Desain 2	Desain 3	Geometric mean	Rating
Desain 1	1.00	0.78	1.40	1.03	0.33

Desain 2	1.29	1.00	1.80	1.32	0.43
Desain 3	0.71	0.56	1.00	0.73	0.24

Kecepatan

KRITERIA	DESAIN SISTEM 1	DESAIN SISTEM 2	DESAIN SISTEM 3
KECEPATAN	+ Data sidik jari disimpan di kartu Chip (+9)	- Menggunakan verifikasi SMS via telepon seluler (+4) - Data sidik jari disimpan di server (+2)	+Data sidik jari disimpan di mesin ATM (+5) - Simpan di server (+2)
TOTAL	+9	+6	+7

1. Desain sistem 1

Data sidik jari yang disimpan di server akan lebih cepat dalam proses verifikasi. Hal ini terjadi karena sistem tidak perlu mencari sidik jari nasabah yang bersangkutan pada server yang notabanya menimbulkan waktu yang lebih lama.

2. Desain sistem 2

Karena sidik jari lebih besar ukurannya dari data pin, *bandwidth* jaringan akan lebih cepat penuh karena pada kondisi peak/penuh nasabah pada setiap mesin ATM dapat melakukan autentifikasi secara bersamaan sehingga menimbulkan antrian yang kecepatannya berkurang dibandingkan dengan desain sistem 1 dan desain sistem 3.

3. Desain sistem 3

Data sidik jari pada sistem ini disimpan di mesin ATM ketika mesin ATM telah dipakai oleh nasabah maksimal satu minggu dari pemakaian berikutnya sehingga metode pencarian akan lebih cepat dibandingkan dengan server dibandingkan dengan desain sistem 2. Namun kecepatan dari proses verifikasi menjadi agak lebih lambat daripada desain sistem 1 karena pencocokannya juga dibandingkan dengan sidik jari orang lain yang masih tersimpan pada mesin ATM/modul sidik jari.

Berikut adalah tabel penilaian untuk kriteria kecepatan sistem

Tabel 4 – Penentuan Rating Kecepatan Sistem

	Desain 1	Desain 2	Desain 3	Geometric mean	Rating
Desain 1	1.00	1.50	1.29	1.24	0.41
Desain 2	0.67	1.00	0.86	0.83	0.27
Desain 3	0.78	1.17	1.00	0.97	0.32

Kemudahan bagi pengguna

KRITERIA	DESAIN SISTEM 1	DESAIN SISTEM 2	DESAIN SISTEM 3
KEMUDAHAN BAGI PENGGUNA	+ Kombinasi 6 digit PIN (+4) - Sidik jari (+2)	- Menggunakan verifikasi SMS via telepon seluler (+2) - Sidik jari (+2)	+ Cardless (+3) + Kombinasi 6 digit PIN (+4) - Sidik jari (+2)
TOTAL	+6	+4	+9

1. Desain sistem 1

Pada desain sistem 1 ini, nasabah hanya perlu membawa kartu dan mengingat kombinasi PIN serta membawa Kartu ATM saat akan melakukan transaksi pada mesin ATM. Namun potensi lupa dalam mengingat kombinasi PIN serta masalah pada kartu ATM masih bisa terjadi.

2. Desain sistem 2

Pada desain sistem 2 ini, terjadi ketidakmudahan bagi pengguna. Selain nasabah harus membawa telepon seluler dan kartu ATM. Selain itu, desain sistem 3 ini juga harus membuat nasabah mengoperasikan 2 device atau alat yang berbeda dalam melakukan transaksi.

3. Desain sistem 3

Desain sistem 3 ini adalah desain yang paling memberikan kemudahan karena tidak nasabah perlu membawa barang tambahan seperti kartu ATM dan telepon seluler seperti desain sistem yang lain. Tetapi nasabah masih perlu untuk mengingat kombinasi PIN dalam melakukan transaksi.

Berikut adalah tabel penilaian untuk kriteria kemudahan bagi pengguna

Tabel 5 – Penentuan Rating Kemudahan bagi Pengguna

	Desain 1	Desain 2	Desain 3	Geometric mean	Rating
Desain 1	1.00	1.50	0.67	1.00	0.32
Desain 2	0.67	1.00	0.44	0.67	0.21
Desain 3	1.50	2.25	1.00	1.50	0.47

Kestabilan sistem

KRITERIA	DESAIN SISTEM 1	DESAIN SISTEM 2	DESAIN SISTEM 3
KESTABILAN SISTEM	- Server (+2) + Kartu ATM Chip (+2) + Tidak ada verifikasi SMS (+3)	- Server (+2) - Menggunakan verifikasi SMS via telepon seluler (+1) - Kartu ATM Magnetic (+1)	- Server (+2) + Cardless (+4) + Tidak ada verifikasi SMS (+3)

TOTAL	+7	+4	+9
--------------	----	----	----

1. Desain sistem 1

Pada desain sistem 1 ini. Selain masalah server yang dapat *down* kapan saja, potensi kerusakan pada kartu ATM juga merupakan suatu hal perlu menjadi pertimbangan.

2. Desain sistem 2

Pada desain sistem 2 ini. Selain masalah server yang dapat *down* kapan saja dan potensi kerusakan pada kartu ATM, masalah dari telepon seluler yang dipakai untuk verifikasi juga dapat mempengaruhi kestabilan dari sistem yang ada. Masalah tersebut dapat berupa sinyal telepon seluler yang buruk dan faktor lain seperti baterai telepon seluler yang lemah atau bahkan habis juga dapat mempengaruhi sistem

3. Desain sistem 3

Desain sistem 3 ini tidak membutuhkan perangkat lain seperti kartu ATM dan telepon sehingga membuat pertimbangan menjadi semakin banyak. Masalah utama pada sistem ini adalah server sama seperti masalah pada desain sistem yang lain yang dapat *down* kapan saja.

Berikut adalah tabel penilaian untuk kriteria kestabilan sistem

Tabel 6 – Penentuan Rating Kestabilan Sistem

	Desain 1	Desain 2	Desain 3	Geometric mean	Rating
Desain 1	1.00	1.75	0.78	1.11	0.35
Desain 2	0.57	1.00	0.44	0.63	0.20
Desain 3	1.29	2.25	1.00	1.42	0.45

Biaya tambahan per transaksi

KRITERIA	DESAIN SISTEM 1	DESAIN SISTEM 2	DESAIN SISTEM 3
BIAYA TAMBAHAN PER TRANSAKSI	+ Tidak ada (+10)	- SMS via telepon seluler (+5)	+ Tidak ada (+10)
TOTAL	+10	+5	+10

1. Desain sistem 1

Tidak ada biaya tambahan per transaksi pada desain sistem 1 ini karena hanya membutuhkan kartu ATM, sidik jari, dan PIN saja.

2. Desain sistem 2

Pada desain sistem 2 nasabah di bebankan biaya tambahan per transaksi berupa biaya SMS yang dipakai untuk verifikasi.

3. Desain sistem 3

Tidak ada biaya tambahan per transaksi pada desain sistem 3 ini karena hanya membutuhkan sidik jari dan PIN saja.

Berikut adalah tabel penilaian untuk kriteria biaya tambahan per transaksi

Tabel 7 – Penentuan Rating Biaya Tambahan per Transaksi

	Desain 1	Desain 2	Desain 3	Geometric mean	Rating
Desain 1	1.00	2.00	1.00	1.26	0.40
Desain 2	0.50	1.00	0.50	0.63	0.20
Desain 3	1.00	2.00	1.00	1.26	0.40

Biaya instalasi dan *maintenance*

KRITERIA	DESAIN SISTEM 1	DESAIN SISTEM 2	DESAIN SISTEM 3
BIAYA INSTALASI DAN MAINTENANCE	- Ada <i>card reader</i> (+3) - Tidak ada modul GSM (+3)	- Ada <i>card reader</i> (+3) - Ada modul GSM (+2)	+ Tidak ada <i>card reader</i> (+5) + Tidak ada modul GSM (+3)
TOTAL	+6	+5	+8

1. Desain sistem 1

Pada desain system ini, penambahan *card reader* membuat biaya instalasi menjadi semakin besar dari pada desain sistem 3 yang tidak menggunakannya. Selain itu, semakin banyak komponen yang terpasang akan berpengaruh pada intensitas perawatan.

2. Desain sistem 2

Selain dari biaya penambahan *card reader*, desain sistem ini juga membutuhkan biaya dalam pemasangan modul GSM yang terkoneksi pada mesin ATM. Dari sisi perawatan, semakin banyak komponen yang terpasang maka akan membutuhkan intensitas perawatan yang semakin besar.

3. Desain sistem 3

Komponen tambahan yang terpasang pada desain sistem 3 ini merupakan yang paling sedikit. Dengan kata lain, biaya instalasi dan intensitas perawatan menjadi lebih kecil dari pada yang lain.

Berikut adalah tabel penilaian untuk biaya instalasi dan maintenance

Tabel 7 – Penentuan Rating Biaya Instalasi dan Maintenance

	Desain 1	Desain 2	Desain 3	Geometric mean	Rating
Desain 1	1.00	1.20	0.75	0.97	0.32

Desain 2	0.83	1.00	0.63	0.80	0.26
Desain 3	1.33	1.60	1.00	1.29	0.42

Kemudian nilai akhir dihitung dengan mengalikan bobot yang telah didapat dan rating untuk seluruh desain per kriteria

$$Score = Rating * Weight$$

$$Total Score = \sum_{n=1}^N Rating(n) * Weight(n)$$

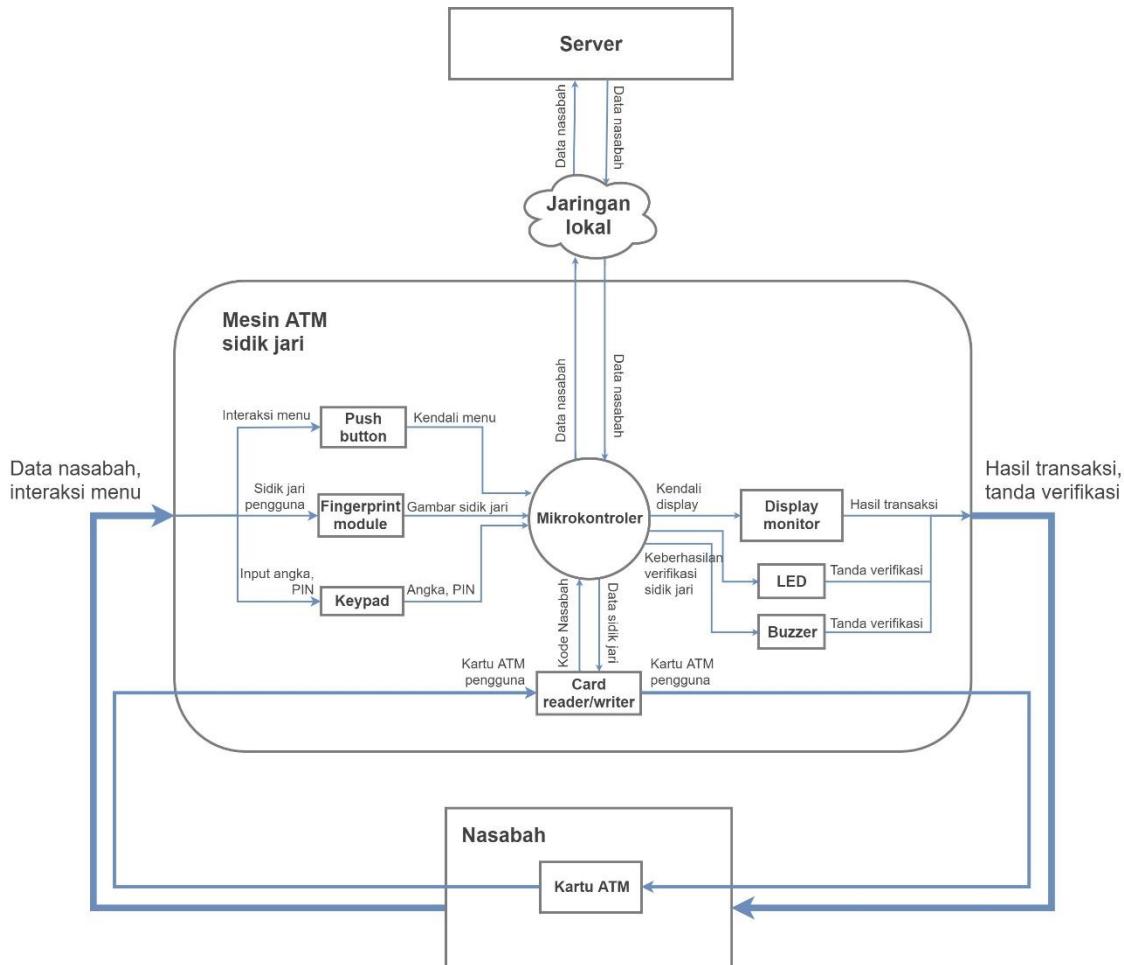
Decision matrix untuk ketiga desain adalah sebagai berikut.

Tabel 8 – Decision Matriks untuk Ketiga Desain Alternatif

Kriteria	Bobot	Desain 1		Desain 2		Desain 3	
		Rating	Score	Rating	Score	Rating	Score
Keamanan Sistem	0.45	0.33	0.148	0.43	0.193	0.24	0.108
Kecepatan Sistem	0.24	0.41	0.098	0.27	0.065	0.32	0.077
Kemudahan bagi pengguna	0.11	0.32	0.038	0.21	0.023	0.47	0.052
Kestabilan Sistem	0.11	0.35	0.038	0.2	0.022	0.45	0.049
Biaya tambahan per transaksi	0.04	0.4	0.016	0.2	0.008	0.4	0.016
Biaya Instalasi dan Maintenance	0.04	0.32	0.013	0.26	0.010	0.42	0.017
	1	1	0.349	1	0.322	1	0.318

2.4.2 Konsep sistem terpilih

Dari hasil *Decision Matrix*, nilai paling tinggi didapatkan oleh Desain Sistem Pertama. Secara garis besar, konsep pada desain pertama ini adalah menerima input sidik jari nasabah, PIN nasabah, dan kartu ATM. Seluruh input tersebut akan diproses, diolah, dan dicocokkan dengan menggunakan mikrokontroler. Data nasabah dan PIN dikirimkan server melalui jaringan lokal, sedangkan data sidik jari terdapat pada kartu ATM yang kemudian akan data-data tersebut akan dicocokkan kebenarannya dengan input. Setelah semua proses selesai, mikrokontroler akan mengeluarkan output pada LED, Buzzer, dan display monitor sebagai user interface sistem. Proses registrasi sidik jari untuk user baru juga dapat dilakukan pada sistem ini. Detail konsep sudah tedapat pada subbab 2.2 sebelumnya



Gambar 12 Flowchart Sistem Desain Pertama

Desain pertama sudah dapat menyelesaikan masalah kejahatan ATM yang paling sering terjadi saat ini yang sudah dijabarkan pada dokumen sebelumnya, yaitu *ATM Skimming* dan *PIN Capturing*. Hal ini disebabkan oleh kartu ATM yang sudah menggunakan chip sehingga data magnetic yang biasa dicuri sudah tidak dapat dilakukan kembali. Selain itu, *PIN Capturing* yang biasa digunakan untuk mencuri kombinasi PIN dengan kamera atau keypad palsu juga menjadi percuma karena pencuri masih membutuhkan data sidik jari untuk dapat melakukan transaksi. Selain itu, fungsionalitas dan dataflow desain sistem pertama juga paling dekat dengan sistem ATM ideal atau yang ada pada saat ini.

Desain pertama memiliki keamanan yang cukup handal yang cukup untuk melindungi nasabah ketika melakukan transaksi. Sistem keamanan yang dirancang berlapis yaitu menggunakan sidik jari dan kombinasi 6 digit PIN. Kartu ATM yang dirancang juga menggunakan chip sehingga akan sangat sulit untuk mencuri data yang terdapat di dalam kartu ATM tersebut. Jika didapatkanpun, pencuri akan sangat sulit untuk merekonstruksi data sidik jari yang ada di dalamnya.

Desain pertama memiliki kecepatan verifikasi dan transaksi yang mumpuni. Hal ini disebabkan oleh data sidik jari yang disimpan pada kartu sehingga pada saat autentifikasi, input data sidik jari pada scanner modul fingerprint hanya akan dicocokkan dengan data sidik jari yang terdapat pada kartu saja. Selain itu, karena hanya account data nasabah dan PIN saja yang diverifikasi melalui jaringan server, *bandwidth* akan jauh berkurang jika dibandingkan dengan harus mengirimkan data sidik jari ke server sehingga data tidak akan

mengalami *traffic* yang mengakibatkan waktu transaksi terhambat. Selain cepat, desain pertama juga cukup stabil. Hal ini dapat dilihat dari gangguan yang mungkin terjadi hanya koneksi dari server dan sistem ATM saja yang sebenarnya jarang sekali terjadi.

Desain pertama memiliki kemudahan bagi user karena user sudah terbiasa dengan sistem keamanan yang ada pada saat ini. User hanya perlu membiasakan diri dengan sistem keamanan tambahan berupa sidik jari saja. Selain itu, user juga tidak perlu menambah biaya apapun yang dapat menghambat saat melakukan transaksi.

Desain pertama juga tidak membutuhkan banyak biaya instalasi dan maintenance. Hal ini disebabkan oleh jumlah komponen yang digunakan juga tidak terlalu banyak. Komponen yang dirancang pun menyesuaikan sistem ATM yang ada sehingga maintenance dapat dilakukan seperti biasa.

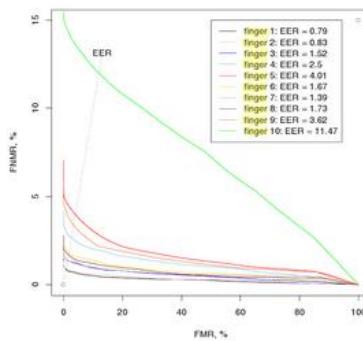
Kombinasi desain seperti *cardless* dan *Modul GSM* masih memiliki celah pada kriteria yang ditetapkan di atas sehingga tidak digunakan. Selain itu, Desain pertama sudah cukup menjawab permasalahan yang ada dan memenuhi standar kriteria mesin ATM yang baik untuk digunakan. Walaupun beberapa kriteria lebih baik seperti keamanan, namun jika dibandingkan dengan desain pertama, maka secara keseluruhan nilai yang dihasilkan tetap lebih tinggi pada desain pertama seperti faktor kecepatan merupakan hal yang tidak bisa diabaikan begitu saja. *User experience* juga merupakan faktor yang penting dalam pemilihan desain, karena nasabah akan mengurangi penggunaan ATM seaman apapun jika prosesnya tidak dilakukan dengan cepat dan nyaman.

Mekanisme registrasi sidik jari dilakukan dengan menggunakan 2 jari user/nasabah, yang berupa jari telunjuk dan jari jempol sebanyak masing-masing 2 kali. Hal ini merujuk pada paper pada referensi [7] yang sudah menguji FMR dan FNMR.

Table 1. Relation of the small fingers to other fingers (Neurotechnology). Numbers are given in %. Bold is with respect to the best finger.

Finger type	Scanner 1	Scanner 2	Scanner 3	Scanner 4	Scanner 5					
	F_5	F_{10}	F_5	F_{10}	F_5	F_{10}	F_5	F_{10}	F_5	F_{10}
Finger 1	1118.2	1115.2	75.2	77.1	525.9	385.2	81.4	92.4	407.6	351.9
Finger 2	1082.4	1079.4	256.1	260	397.1	285.3	411.5	442.6	383.1	1281.9
Finger 3	351.7	350.6	122.6	125	445.2	322.6	119.7	133.1	163.8	654.6
Finger 4	142.2	141.6	36	37.4	133.6	81.1	13	19.9	60.4	358.8
Finger 6	500	498.5	45.6	47.2	267.4	184.8	50	59.1	140.1	586.8
Finger 7	209.2	208.5	245	248.8	360.9	257.3	345.7	372.9	188.5	725.2
Finger 8	282.9	281.9	106	108.2	193.1	127.2	155.7	171.3	131.8	563
Finger 9	46.7	46.4	26.6	28	70.7	32.3	23.3	30.8	10.8	216.9

- Finger 1 - right thumb
- Finger 2 - right index
- Finger 3 - right middle
- Finger 4 - right ring
- Finger 5 - right small
- Finger 6 - left thumb
- Finger 7 - left index
- Finger 8 - left middle
- Finger 9 - left ring
- Finger 10 - left small



Gambar 13 Data FNMR dan FMR untuk Semua Jari

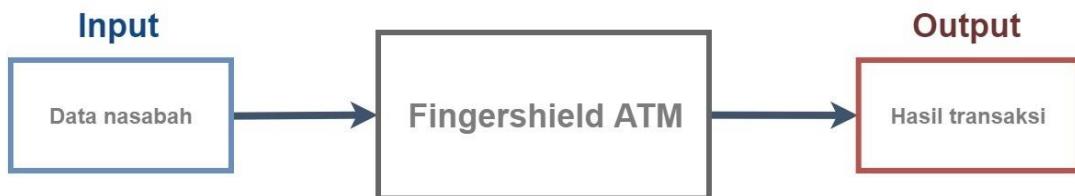
Dapat terlihat bahwa ketika seluruh jari dibandingkan dengan kelingking yang memiliki tingkat akurasi paling kecil, didapatkan nilai yang paling besar adalah telunjuk kanan dan jempol kanan. Dengan demikian, kedua jari tersebutlah yang memiliki akurasi paling tinggi dalam menentukan mana sidik jari yang cocok dan tidak cocok.

3 Desain Sistem

3.1 Pemodelan Fungsional Sistem

3.1.1 Desain Level 0 Sistem

Desain level 0 kami adalah sebagai berikut



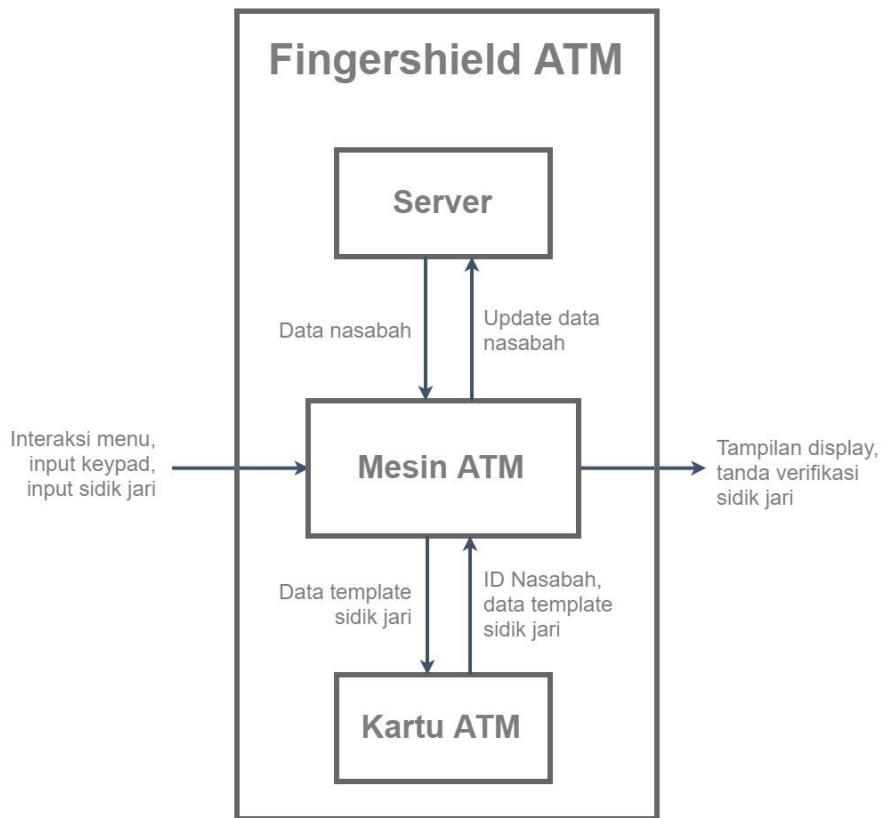
Gambar 13 Desain Level 0 Sistem

Parameter	Keterangan
Input	<ul style="list-style-type: none">Data nasabah <p>Masukan data nasabah mencakup sidik jari, kombinasi 6 digit PIN, dan detail transaksi yang dilakukan nasabah</p>
Output	<ul style="list-style-type: none">Hasil transaksi <p>Hasil transaksi merupakan hasil akhir dari transaksi yang telah selesai dilakukan oleh nasabah</p>
Fungsionalitas	<ul style="list-style-type: none">Fungsionalitas dari desain level 0 ini adalah sistem yang ada dapat melayani kebutuhan nasabah akan verifikasi akun nasabah dan proses transaksi dalam

Pada desain level 0 fingershield ATM ini, data nasabah yang dapat berupa PIN, sidik jari, dan detail interaksi menu transaksi yang menjadi masukan dalam sistem ini akan diolah dalam Fingershield ATM sehingga menghasilkan keluaran berupa hasil transaksi yang hendak dilakukan nasabah ketika nasabah tersebut menggunakan Fingershield ATM. Proses pada sistem di Fingershield ATM mencakup verifikasi identitas nasabah dengan menggunakan PIN dan sidik jari milik nasabah serta rangkaian proses transaksi yang dapat dilakukan setelah proses verifikasi sukses dilakukan oleh nasabah. perangkat Fingershield mencakup mesin ATM, server, dan juga kartu ATM yang notabanya merupakan media penyimpanan yang portabel yang dimiliki pada sistem ATM.

3.1.2 Desain Level 1 Sistem

Desain level 1 dari sistem keamanan Mesin ATM menggunakan sidik jari kami adalah sebagai berikut



Gambar 14 Desain Level 1 Sistem

Parameter	Keterangan
Input	<ul style="list-style-type: none"> Input dari sistem merupakan masukan yang berasal dari <i>user</i> (nasabah) ke mesin ATM. Masukan berupa sidik jari, kombinasi 6 digit PIN, dan masukan lanjutan berupa interaksi menu yang dilakukan oleh nasabah pada saat proses transaksi berlangsung
Output	<ul style="list-style-type: none"> Tampilan display, LED dan buzzer pada tanda verifikasi, transaksi yang bergantung pada aktivitas yang dilakukan oleh nasabah yang melakukan
Fungsionalitas	<ul style="list-style-type: none"> Melakukan verifikasi identitas milik nasabah dengan identitas nasabah yang bersangkutan yang tersimpan pada sistem di mesin ATM, memproses transaksi yang dilakukan oleh nasabah, melakukan pembacaan informasi pada kartu ATM, mengunduh dan mengunggah informasi akun nasabah pada server

Pada sistem keamanan sidik jari di mesin ATM ini, secara umum masukan yang dipakai berasal dari nasabah berupa sidik jari milik nasabah, kombinasi 6 digit PIN milik nasabah serta input pada interaksi menu transaksi yang dilakukan oleh nasabah. Input sidik jari dari nasabah akan dimasukkan melalui *fingerprint module* yang terdapat pada mesin ATM. Kemudian untuk input PIN dimasukkan melalui keypad, sedangkan input berupa interaksi menu transaksi dimasukkan melalui keypad dan push button.

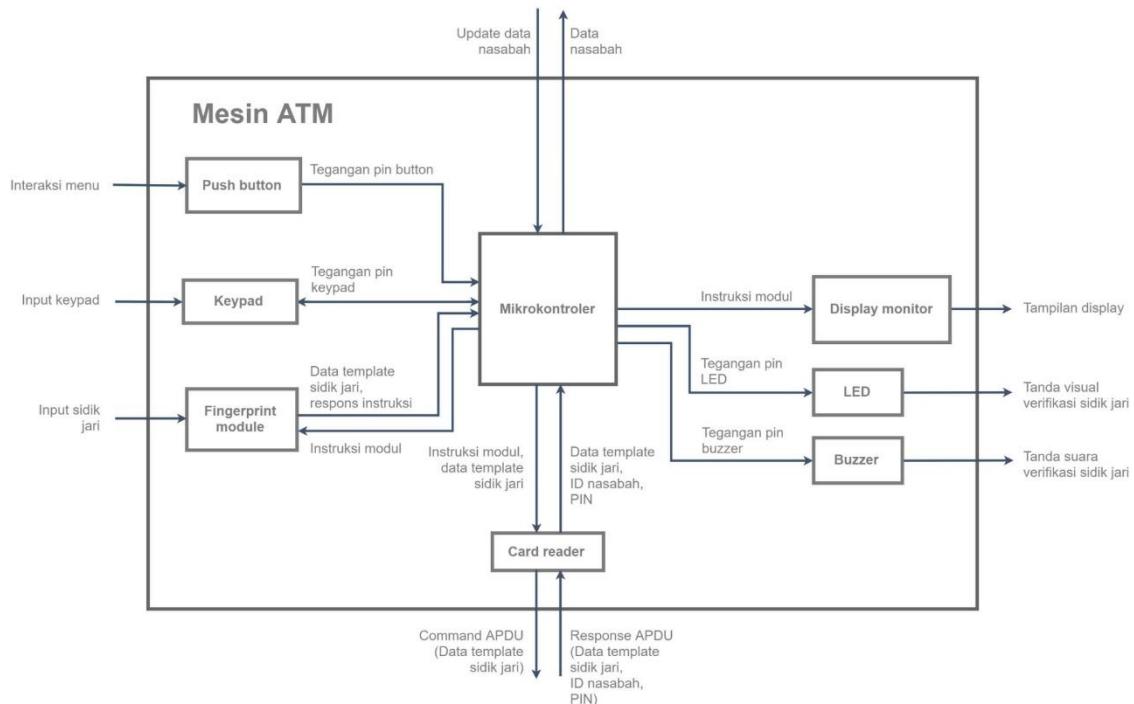
Untuk keluaran yang dihasilkan oleh mesin ATM ini, mesin ATM memakai display, LED dan juga buzzer sebagai interaksi antara nasabah dan juga mesin ATM. Tampilan layar display merupakan komunikasi tatap muka sebagai representasi proses verifikasi dan proses transaksi yang sedang berlangsung.

Sedangkan dari segi fungsionalitas dari mesin ATM, ada beberapa hal yang menjadi fungsi utama dari mesin ATM yang di desain, Hal tersebut adalah melakukan verifikasi identitas milik nasabah dengan identitas nasabah yang bersangkutan yang tersimpan pada sistem di mesin ATM, memproses transaksi yang dilakukan oleh nasabah, melakukan pembacaan informasi pada kartu ATM, serta mengunduh dan mengunggah informasi akun nasabah pada server.

3.1.3 Desain Level 2 Sistem

Berdasarkan Desain level 0, Desain level 1 dari sistem keamanan Mesin ATM menggunakan sidik jari dapat dibagi menjadi 3 sub-sistem, yaitu Mesin ATM, Kartu ATM, dan Server

3.1.3.1 Desain Level 2 mesin ATM



Gambar 15 Desain Level 2 Sistem Mesin ATM

Parameter	Keterangan
Input	<p>Input digolongkan menjadi 3 bagian utama</p> <ul style="list-style-type: none"> • Sidik jari Input ini dimasukkan pada saat proses verifikasi identitas nasabah melalui <i>finger print module</i> • Kombinasi 6 digit PIN Input ini dimasukkan pada saat proses proses verifikasi tambahan identitas nasabah, yang dimasukkan adalah kombinasi 6 digit PIN melalui keypad • Interaksi menu transaksi

	Pada input ini, nasabah memasukkan varian transaksi yang dipilih dan besaran uang yang dipakai dalam varian transaksi
Output	<p>Output digolongkan menjadi 3 bagian</p> <ul style="list-style-type: none"> • Tampilan display Output pada tampilan display menjadi keluaran yang menampilkan proses verifikasi identitas nasabah dan proses transaksi yang sedang berlangsung. • Tanda verifikasi (LED) Output ini merupakan tanda dari hasil verifikasi sidik jari yang telah dilakukan • Tanda verifikasi (buzzer) Output ini merupakan tanda dari hasil verifikasi sidik jari yang telah dilakukan
Fungsionalitas	<p>Ada beberapa fungsi dari desain ini</p> <ul style="list-style-type: none"> • Membaca informasi data dan sidik jari nasabah yang ada dalam kartu ATM • Mengunduh dan mengunggah data akun nasabah pada server • Melakukan verifikasi identitas melalui sidik jari dan kombinasi PIN • Memproses transaksi yang dilakukan nasabah

Keterangan terperinci desain level 2 dari mesin ATM

- Push Button

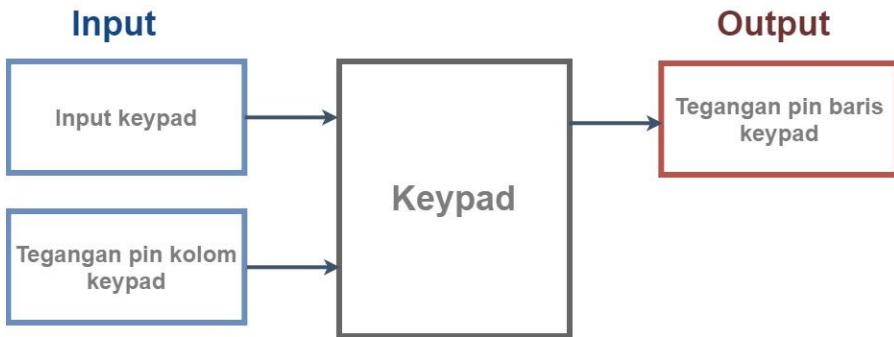


Gambar 16 Desain Level 2 Sistem Mesin ATM

Parameter	Keterangan
Input	<ul style="list-style-type: none"> • Interaksi menu Interaksi menu merupakan input yang dilakukan oleh nasabah. Bentuk dari interaksi menu transaksi merupakan penekanan menggunakan jari pada perangkat push button.
Output	<ul style="list-style-type: none"> • Tegangan pin button (0 – 5 V)
Fungsionalitas	<ul style="list-style-type: none"> • Mengubah penekanan yang dilakukan oleh nasabah yang menekan menggunakan jari tangan nasabah (interaksi menu transaksi) menjadi sebuah nilai tegangan yang dapat diproses oleh bagian pemrosesan data dari sistem

Fungsi utama dari push button adalah mengubah masukan yang berupa interaksi menu (dalam bentuk penekanan push button dengan jari) oleh nasabah menjadi sebuah nilai tegangan yang dapat terdeteksi oleh mikrokontroler. Seting rangkaian dari push button dapat berupa *pull up* maupun *pull down* sesuai dengan kebutuhan dan pemrograman pada sistem utama apakah nilai input pin *low* atau *high*.

- Keypad

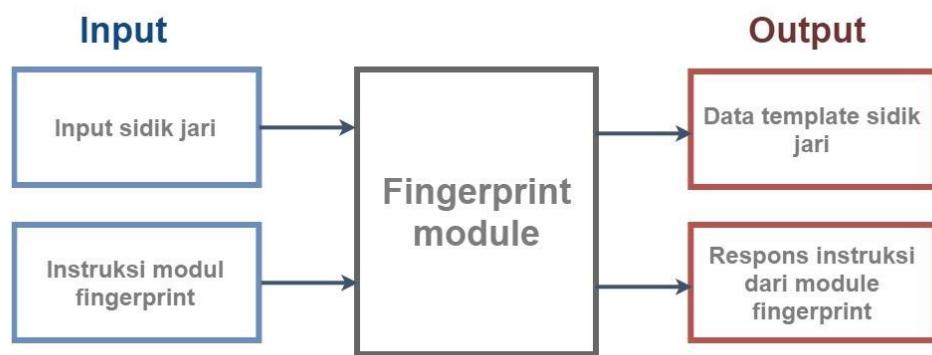


Gambar 17 Desain Level 2 Sistem Mesin ATM

Parameter	Keterangan
Input	<p>Input keypad merupakan masukan yang diterima keypad dari nasabah ketika nasabah hendak mengoperasikan mesin ATM. Input keypad dapat berupa</p> <ul style="list-style-type: none"> • Kombinasi 6 digit PIN Kombinasi 6 digit PIN merupakan input yang dimasukkan nasabah pada saat proses verifikasi akun dari nasabah yang bersangkutan • Interaksi menu transaksi Interaksi menu transaksi merupakan input yang dimasukkan oleh nasabah pada saat proses transaksi <p>Tegangan pin kolom keypad (0 – 5 V)</p> <p>Tegangan pin kolom keypad adalah tegangan yang diterima oleh keypad dari bagian pemroses utama sistem pada mesin ATM. Tegangan pin kolom fungsinya adalah sebagai scanning pada keypad.</p>
Output	<ul style="list-style-type: none"> • Tegangan pin baris keypad (0 – 5 V) Tegangan pin baris merupakan tegangan yang dihasilkan dari penekanan pada keypad oleh nasabah. Baris dimana nasabah melakukan penekanan akan menjadi keluaran berupa nilai tegangan pin baris.
Fungsionalitas	<ul style="list-style-type: none"> • Mengubah input keypad (kombinasi 6 digit PIN, interaksi menu) menjadi sebuah nilai tegangan yang dapat diproses oleh bagian pemrosesan data dari sistem

Pada keypad, cara yang digunakan untuk dapat mendeteksi input adalah dengan cara membagi karakter-karakter keypad dalam sebuah matriks. Kolom matriks tersebut dijadikan diberi tegangan input yang berasal dari mikrokontroler dengan teknik scanning secara periodik dalam periode ber orde milisekon. Kemudian baris pada keypad akan menghasilkan tegangan input ketika karakter pada baris tersebut ditekan oleh nasabah. Nilai karakter akan diketahui dengan posisi kolom dan baris yang terdefinisi lewat tegangan scanning dan juga tegangan output sehingga nilai karakter dapat terbaca oleh mikrokontroler.

- Fingerprint module



Gambar 18 Desain Level 2 Fingerprint module

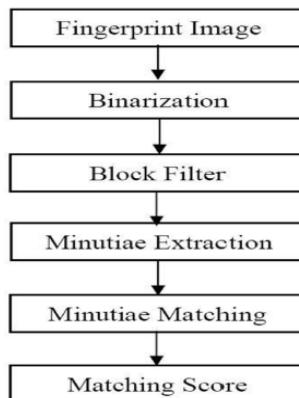
Parameter	Keterangan
Input	<p>Ada 2 input pada pada finggerprint modul ini</p> <ul style="list-style-type: none"> • Sidik jari nasabah Sidik jari nasabah merupakan input yang dimasukkan pada saat verifikasi sidik jari nasabah ketika nasabah yang bersangkutan menggunakan mesin ATM • Instruksi modul (komunikasi UART) Instruksi modul merupakan sebuah masukan pada modul sidik jari yang fungsinya perintah untuk memulai fungsi pada finggerprint modul yang bersangkutan
Output	<p>Berikut ini merupakan keluaran dari fingerprint module</p> <ul style="list-style-type: none"> • Template sidik jari nasabah (Array ukuran 512 bytes per template) Template sidik jari nasabah berisi data bifurcation dan ridge ending dari sidik jari nasabah • Respons instruksi (komunikasi UART) Respon instruksi merupakan respon dari perintah instruksi terhadap fingerprint module
Fungsionalitas	<p>Fungsi utama dari perangkat module sidik jari</p> <ul style="list-style-type: none"> • Mengcapture sidik jari nasabah dalam bentuk grayscale • Melakukan binerisasi sidik jari nasabah • Thining pada citra sidik jari sehingga informasi ridge ending dan bifurcation menjadi sebesar 1 pixel • Melakukan ekstraksi bufurcation dan ridge ending untuk dijadikan data template sidik jari

Fingerprint module adalah perangkat yang berfungsi untuk melakukan deteksi terhadap sidik jari dari nasabah untuk di ekstrak bifurcation dan ridge endingnya supaya menjadi data template yang dapat dicocokkan dengan data template sidik jari tersimpan pada proses verifikasi. Proses ini merupakan rangkaian dari pengolahan citra digital yang dimulai dari pengcapturean sidik jari dan diakhiri dengan ekstraksi ridge ending dan bifurcation pada untuk dijadikan data template sidik jari.

Komunikasi yang dipakai antara fingerprint module dengan komponen mikrokontroler adalah komunikasi **UART** (*Universal Asynchronous Receiver-Transmitter*). **UART**

merupakan sirkuit terintegrasi yang sering dipakai komunikasi serial pada perangkat komputer atau port serial pada perangkat periperal.

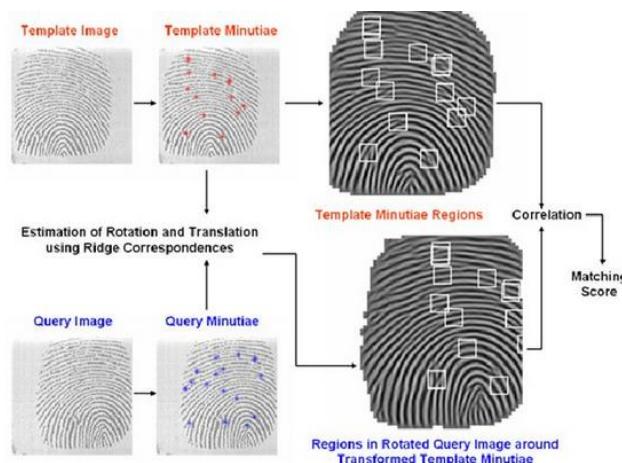
Terdapat 2 pilihan algoritma dalam *fingerprint matching*, yaitu *minutiae matching* dan *correlation based matching*. *Minutiae matching* memiliki prinsip untuk menemukan titik minutiae terlebih dahulu. Proses yang dilakukan adalah sebagai berikut



Gambar 19 Proses Minutiae Matching

Proses yang dilakukan pertama adalah mengambil gambar sidik jari dengan sensor. Setelah itu, gambar sidik jari dibinerisasi dari grayscale menjadi hitam-putih. Gambar sidik jari biner tersebut akan masuk block filter atau proses *thinning* untuk membuat pola sidik jari memiliki lebar 1 pixel dengan tujuan agar lebih mudah mendapatkan fitur minutiae. Setelah itu, baru lah minutiae di-extract berdasarkan ciri bentuk tertentu. Proses pencocokan dilakukan dengan melihat jarak antar minutiae terhadap acuannya. Terakhir, sidik jari dinilai berdasarkan score yang dilihat dari *Euclidean Distance*. Apabila score lebih tinggi dari threshold yang telah ditetapkan, maka sidik jari dikatakan cocok atau valid. Kelebihan dari algoritma ini adalah akurat, paling banyak digunakan, dan size template yang kecil karena hanya berupa array saja. Kelemahannya adalah tidak dapat mendekripsi sidik jari yang berkualitas rendah/rusak dan masih bisa terdapat *false minutiae*.

Correlation Based Matching dilakukan dengan mencocokkan pixel yang sama antar gambar sidik jari dengan memperhatikan perataan dan rotasi. Proses yang dilakukan adalah sebagai berikut



Gambar 20 Proses Correlation Matching

Proses yang pertama dilakukan adalah membuat template sidik jari berdasarkan gambar grayscale image. Pada proses ini juga terjadi, phase shifting atau phase rotation jika gambar sidik jari miring atau tidak tepat. Antar template sidik jari kemudian dicocokkan setiap per pixelnya. Score didapatkan dari hasil rata-rata kuadrat penjumlahan jarak antar pixel yang sama. Kelebihan dari algoritma ini adalah tidak memerlukan banyak proses dan lebih banyak informasi karena gambar masih dalam gray-level. Kekurangannya adalah komputasi lebih kompleks dan memory template sidik jari lebih besar karena berupa gambar grayscale.

Dengan mempertimbangkan kelebihan dan kekurangan masing-masing algoritma dan spesifikasi pengolahan dan penyimpanan data sidik jari tersebut, maka algoritma *minutiae matching* yang dipilih sebagai metode *fingerprint matching*.

- Display monitor



Gambar 21 Desain Level 2 Display monitor

Parameter	Keterangan
Input	<ul style="list-style-type: none"> • Instruksi (tegangan 0 - 5 V) <p>Instruksi ini merupakan beberapa baris bit dengan nilai tegangan 0 atau 1 yang akan menghasilkan sebuah karakter pada display monitor sesuai dengan kombinasi dari 8 bit instruksi yang diinputkan</p>
Output	<ul style="list-style-type: none"> • Tampilan display <p>Tampilan display ini merupakan kumpulan karakter yang membentuk kata sebagai bentuk komunikasi antara mesin ATM dan nasabah</p>
Fungsionalitas	<ul style="list-style-type: none"> • Menampilkan tampilan display sebagai komunikasi tatap muka antara sistem mesin ATM dengan nasabah

- LED



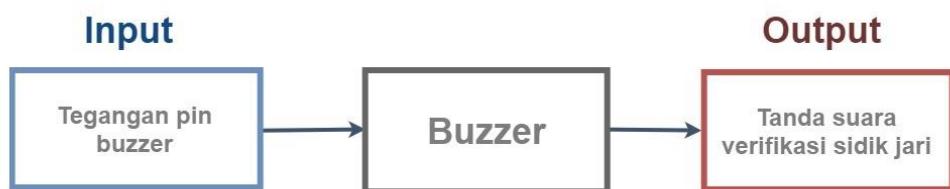
Gambar 22 Desain Level 2 LED

Parameter	Keterangan
Input	<ul style="list-style-type: none"> • Tegangan pin LED (0 - 5 V)

	Tegangan pin LED diperoleh dari sistem pemrosesan utama mesin ATM
Output	<ul style="list-style-type: none"> Kedip LED <p>Kedip LED merupakan tanda dari hasil proses verifikasi sidik jari milik nasabah yang bersangkutan</p>
Fungsionalitas	<ul style="list-style-type: none"> Fungsi utama dari LED adalah sebagai notifikasi dari hasil verifikasi sidik jari nasabah. Hasil verifikasi yang sukses dan hasil verifikasi yang gagal akan memberikan pola kedip LED yang berbeda.

LED adalah komponen berbahan dasar diode yang dapat memancarkan cahaya sehingga dapat digunakan untuk penanda dari hasil verifikasi terhadap data template sidik jari nasabah dengan data template sidik jari tersimpan. Umumnya pemasangan LED juga disertai dengan resistor dengan tujuan untuk membuat arus yang melalui dioda pada LED tidak terlalu besar.

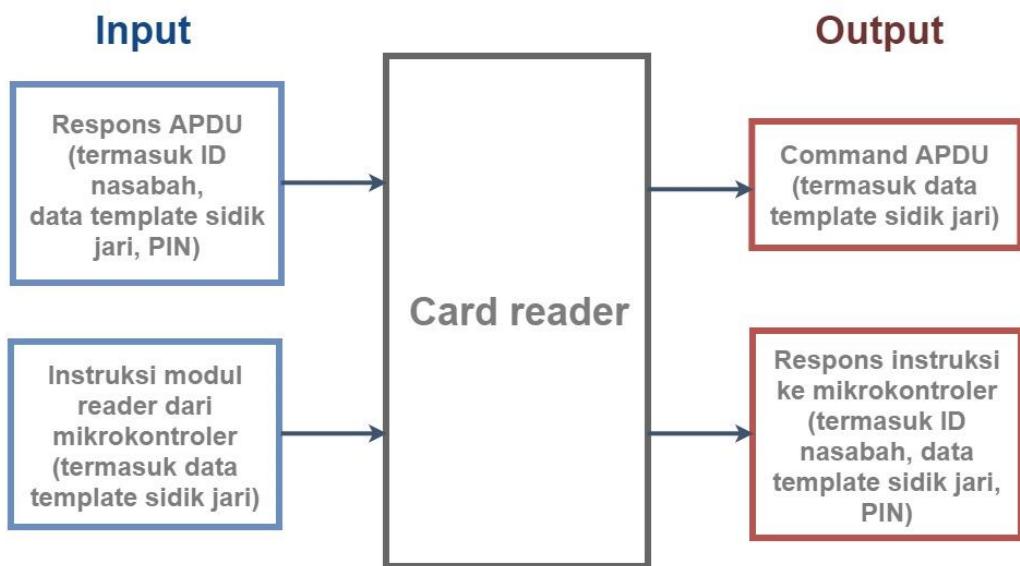
- Buzzer



Gambar 23 Desain Level 2 Buzzer

Parameter	Keterangan
Input	<ul style="list-style-type: none"> Tegangan pin buzzer (0 - 5 V) <p>Tegangan pin buzzer diperoleh dari sistem pemrosesan pemrosesan mesin ATM</p>
Output	<ul style="list-style-type: none"> Suara dari buzzer <p>Merupakan tanda dari hasil proses verifikasi sidik jari milik nasabah yang bersangkutan</p>
Fungsionalitas	<ul style="list-style-type: none"> Fungsi utama dari buzzer adalah sebagai notifikasi dari hasil verifikasi sidik jari nasabah. Hasil verifikasi yang sukses dan hasil verifikasi yang gagal akan memberikan pola buzzer yang berbeda.

- Card reader



Gambar 24 Desain Level 2 Card reader

Parameter	Keterangan
Input	<p>Berikut ini merupakan masukan dari card reader</p> <ul style="list-style-type: none"> • Instruksi modul reader (komunikasi port USB) <p>Instruksi ini berasal dari bagian utama pemrosesan mesin ATM. Instruksi ini merupakan sebuah perintah yang berfungsi untuk membuat perangkat card reader mulai membaca kartu ATM. Data template sidik jari merupakan</p> <ul style="list-style-type: none"> • Respons APDU <p>APDU merupakan format file yang berasal dari card reader. File ini berisi instruksi dan data yang berasal dari kartu ATM. Berikut ini adalah data yang ada dalam APDU</p> <ul style="list-style-type: none"> - ID nasabah - Template sidik jari - PIN
Output	<p>Berikut ini adalah keluaran yang dihasilkan oleh perangkat card reader</p> <ul style="list-style-type: none"> • Command APDU <p>Command APDU adalah sebuah output yang isinya adalah instruksi dan kumpulan data yang diisikan ke kartu. Data yang diisikan ke kartu adalah data template sidik jari nasabah</p> <ul style="list-style-type: none"> • Response instruksi ke mikrokontroler (komunikasi port USB) <p>Response instruksi ke mikrokontroler adalah data yang dikirimkan ke mikrokontroler sebagai feedback dari instruksi. Berikut ini adalah data yang menjadi keluaran dari reader</p> <ul style="list-style-type: none"> - ID nasabah - Template sidik jari - PIN

Fungsionalitas	<ul style="list-style-type: none"> Fungsi utama card reader adalah melakukan pembacaan APDU dari kartu ATM yang dimiliki oleh nasabah dan kemudian meneruskan data yang sudah diekstraksi dari APDU menjadi data ID nasabah, template sidik jari, dan PIN ke bagian pemrosesan utama sistem pada mesin ATM
----------------	---

Card reader adalah perangkat yang memiliki fungsi utama sebagai alat pembacaan kartu ATM pada sistem Fingershield ATM. File yang terbaca pada kartu ATM adalah dalam format APDU yang didalamnya mencakup instruksi dan juga data yang ada pada kartu ATM seperti sidik jari, PIN dan ID akun nasabah.

Setelah data terbaca oleh card reader, maka yang selanjutnya dilakukan adalah meneruskan data tersebut ke mikrokontroler. Card reader dan mikrokontroler terhubung dalam komunikasi USB.

3.1.3.2 Desain Level 2 Kartu ATM



Gambar 25 Desain Level 2 Sistem Kartu ATM

Parameter	Keterangan
Input	<ul style="list-style-type: none"> Data template sidik jari (Array ukuran 512 bytes per template)
Output	<ul style="list-style-type: none"> APDU <p>APDU adalah format file beberapa bit yang berisi instruksi dan data yang dikirimkan. Data yang menjadi output adalah</p> <ul style="list-style-type: none"> - ID nasabah - PIN - Data template sidik jari nasabah
Fungsionalitas	<p>Kartu ATM memiliki beberapa fungsi</p> <ul style="list-style-type: none"> • Sebagai data identitas dari akun nasabah yang bersangkutan • Sebagai media penyimpanan dari data template sidik jari akun nasabah yang bersangkutan yang dipakai untuk proses verifikasi dari identitas nasabah

Pada desain level 2 pada kartu ATM, fokus utama pada desain ini adalah kartu ATM sebagai media penyimpanan dari identitas akun nasabah dan juga data template sidik jari dari nasabah yang digunakan sebagai data yang dicocokkan dengan sidik jari yang dimiliki nasabah pada proses verifikasi. Input yang digunakan adalah template sidik jari dan data akun nasabah yang dimasukkan pada saat awal pertama kali pemakaian kartu. sedangkan pada sisi output, karena pada dasarnya kartu itu dimanfaatkan sebagai media penyimpanan,

maka output akan sama dengan masukan input di awal pertama kali pemakaian yaitu data akun nasabah dan template sidik jari dari nasabah yang bersangkutan.

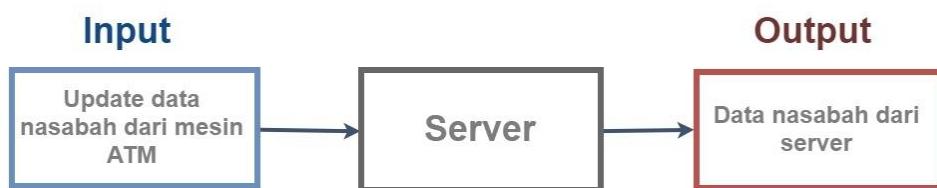
Komunikasi antara Kartu ATM dengan Card Reader masih bersifat contact.

3.1.3.2.1 Standard Kartu ATM mengacu Regulasi

Berdasarkan surat edaran yang dikeluarkan oleh Bank Indonesia (BI) nomer 17/52/DKSP, tentang Bank Indonesia menetapkan NSICCS (*National Standard Indonesian Chip Card Specification*) sebagai standar nasional teknologi chip untuk kartu ATM dan/atau kartu debit. Paling lambat pada tahun 2022, semua kartu debet dan kartu ATM yang ada di Indonesia wajib memakai kartu chip dan memiliki 6 digit kombinasi PIN dari yang tadinya 4 digit kombinasi PIN.

Dengan menggunakan kartu ATM dengan chip, dapat dipastikan bahwa desain kartu ATM yang ada mendukung rencana jangka panjang yang diproyeksikan oleh Bank Indonesia

3.1.3.3 Desain Level 2 Server



Gambar 26 Desain Level 2 Sistem Server ATM

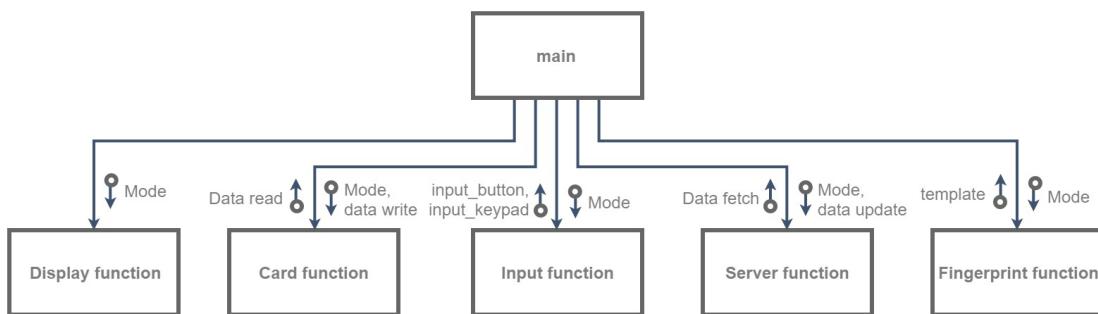
Parameter	Keterangan
Input	<p>Berikut ini adalah input dari server</p> <ul style="list-style-type: none">• Instruksi (komunikasi port ethernet)• Input yang dimasukkan pada server adalah instruksi untuk melakukan pengunduhan informasi akun nasabah yang bersangkutan• Update data nasabah• Input ini merupakan input yang digunakan untuk <i>replace</i> data nasabah ketika nasabah yang bersangkutan selesai melakukan transaksi
Output	<ul style="list-style-type: none">• Data nasabah (komunikasi port ethernet)• Keluaran dari server merupakan data akun nasabah yang berupa informasi akun, jumlah nominal uang di rekening nasabah ketika nasabah yang bersangkutan melakukan akses menggunakan mesin ATM
Fungsionalitas	<ul style="list-style-type: none">• Fungsi utama dari server ini adalah sebagai tempat penyimpanan database dari semua data nasabah pada sebuah penyedia jasa perbankan

Pada desain level 2 server, yang menjadi penekanan adalah pemakaian server sebagai database dari seluruh nasabah dari penyedia jasa perbankan. Database pada server berisi data akun seluruh nasabah dan informasi terkait saldo dan informasi transaksi nasabah penyedia jasa perbankan. Input pada bagian server ini merupakan data dari nasabah terupdate yang diunggah ke server setelah nasabah yang bersangkutan menyelesaikan proses transaksi. Kemudian output yang dihasilkan pada sever merupakan data akun

nasabah serta infomasi saldo dan transaksi dari nasabah ketika nasabah menggunakan mesin ATM sebagai media transaksi.

3.1.4 Desain Software

Desain software dilakukan dengan memecah fungsi-fungsi yang terjadi di dalam mikrokontroler sistem yang memproses input menjadi output. Diagramnya adalah sebagai berikut



Gambar 27 Desain Software Sistem

Gambar di atas merupakan struktur dari desain software yang dimiliki oleh mesin ATM. Berdasarkan gambar, yang ada dapat diamati bahwa satu program utama dan 5 fungsi yang membentuk dasar dari sebuah sistem pada mesin ATM.

Berikut ini adalah penjabaran dari desain software di atas.

- Main

Main merupakan program utama dari desain mesin ATM yang ada. Main memiliki fungsi sebagai pengordinasi dari fungsi-fungsi yang ada di bawahnya (display function, card function, input function, server function, dan fingerprint function), mengcall fungsi-fungsi di bawahnya untuk menjalankan sebuah sistem secara terpadu, sebagai pengontrol jalannya sebuah sistem software secara keseluruhan, dan sebagai pengatur flow lalu lintas dari data-data yang ada pada sistem.

Selain peran-peran di atas, main juga memiliki 2 bagian yang esensial dari sistem software mesin ATM. Berikut ini adalah bagian yang dimaksud.

- Verifikasi

Peran utama dari proses verifikasi adalah sebagai pembanding antara identitas ID nasabah, PIN, dan template sidik jari yang tersimpan pada kartu ATM dengan ID nasabah yang tersimpan pada server, PIN yang tersimpan pada kartu, template sidik jari nasabah yang tersimpan pada kartu.

- Transaksi

Transaksi berperan dalam pengolahan aktivitas keuangan yang dilakukan oleh nasabah. Pada proses transaksi ini, main akan memakai data yang menjadi keluaran dari input function dan juga server function untuk diolah sehingga didapatkan hasil dari transaksi yang akan ditampilkan / diteruskan oleh display function dan akan diteruskan ke server oleh server function.

- **Display function**

Display function merupakan fungsi yang bertugas mengatur komunikasi tatap muka antara mesin ATM dan juga nasabah. Display function tersebut merupakan fungsi software yang mengatur perangkat penampil output pada mesin ATM. Komponen tersebut adalah monitor, LED dan Buzzer.

Masukan dari main yang diterima oleh display function dari main adalah berupa mode. Dengan perubahan mode yang diterima oleh display function, komunikasi tatap muka yang ditampilkan oleh perangkat output juga akan menyesuaikan dengan mode yang menjadi masukan.

- **Card function**

Card function merupakan fungsi software yang mengatur hubungan antara mesin ATM dengan kartu ATM. Hubungan yang terjadi antara mesin ATM dan kartu adalah meliputi komunikasi pengiriman data dari kartu ATM ke mesin ATM atau dari mesin ATM ke kartu ATM.

Mode, dan data write adalah masukan card function yang diterima dari main. Mode merupakan masukan yang menjadi acuan dalam proses yang sedang berlangsung pada card function apakah mode tersebut merupakan mode pembacaan data dari kartu ATM, ataukah mode pengiriman data menuju kartu ATM. Data write merupakan data yang diteruskan ke kartu ATM dan diubah menjadi APDU agar dapat dituliskan di kartu ATM.

Sedangkan untuk sisi keluaran yang diteruskan ke main, keluaran yang dihasilkan adalah data read yang merupakan data yang berisi ID nasabah, PIN, dan juga data template sidik jari dalam bentuk array.

- **Input function**

Input function merupakan fungsi software yang mengatur fungsi software dari perangkat push button dan keypad yang merupakan bagian dari perangkat input dari sistem.

Mode merupakan masukan fungsi dari main menuju input function yang berfungsi sebagai acuan dalam proses input pada mesin ATM yang sedang berlangsung. Proses tersebut dapat berupa proses pemasukan PIN dan interaksi menu transaksi.

Sedangkan untuk sisi keluaran yang diteruskan ke main, keluaran yang dihasilkan adalah input_button dan input_keypad. Input_keypad adalah data olahan dari hasil interaksi antara nasabah dan keypad yang dapat berupa masukan PIN dan interaksi menu . Sedangkan input_button merupakan data olahan dari interaksi menu antara nasabah dengan push button.

- **Server function**

Server function merupakan fungsi software yang mengatur hubungan antara mesin ATM dengan server. Hubungan yang terjadi antara mesin ATM dan kartu adalah meliputi pengunduhan data dari server ke mesin ATM atau pengunggahan update data dari mesin ATM ke server.

Mode dan data update adalah masukan yang diterima oleh server function dari main. Mode merupakan masukan yang menjadi acuan dalam proses yang sedang berlangsung pada card function apakah mode tersebut merupakan mode pengunduhan data dari server, ataukah mode pengunggahan data menuju server.

Data update merupakan data yang mencakup informasi trasnsaksi terbaru yang telah dilakukan nasabah, data update juga merupakan data masukan yang akan diteruskan ke server.

Sedangkan untuk sisi keluaran, keluaran yang dihasilkan adalah data fetch yang merupakan data yang berisi informasi nilai nominal yang dimiliki nasabah.

- Fingerprint function

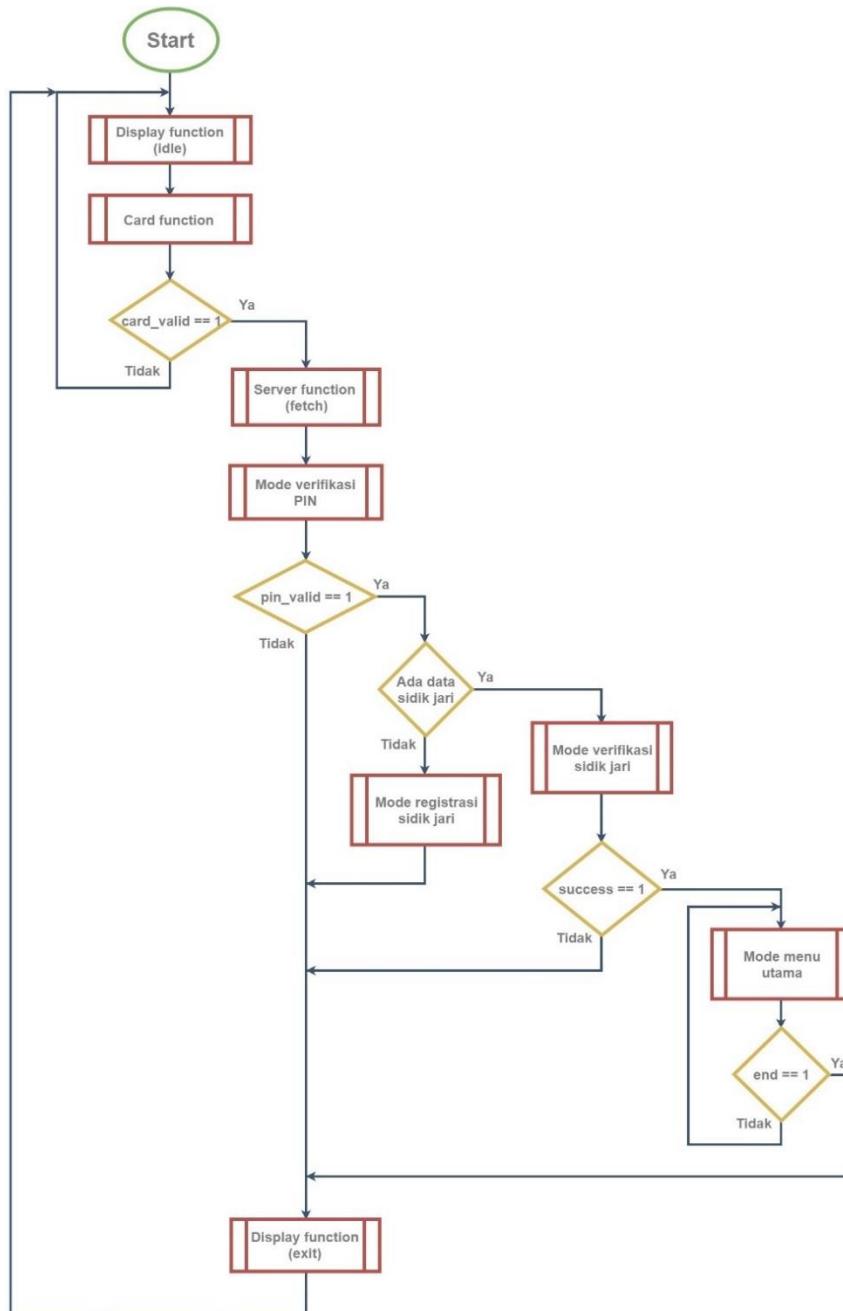
Fingerprint function merupakan fungsi software yang mengatur fungsi software dari perangkat fingerprint modul yang merupakan bagian dari perangkat input dari sistem.

Mode merupakan masukan fungsi dari main yang diterima fingerprint function yang berfungsi sebagai acuan dalam proses input sidik jari nasabah pada mesin ATM.

Sedangkan untuk sisi keluaran yang diteruskan ke main, keluaran yang dihasilkan adalah template sidik jari dalam bentuk array. Template sidik jari merupakan data sidik jari yang telah di ekstrak informasi ridge ending dan bifurcationnya sebagai sarana untuk proses verifikasi sidik jari pada proses verifikasi di mesin ATM.

3.2 Pemodelan Tingkah Laku Sistem

3.2.1 Behavioral Sistem Utama Mesin ATM



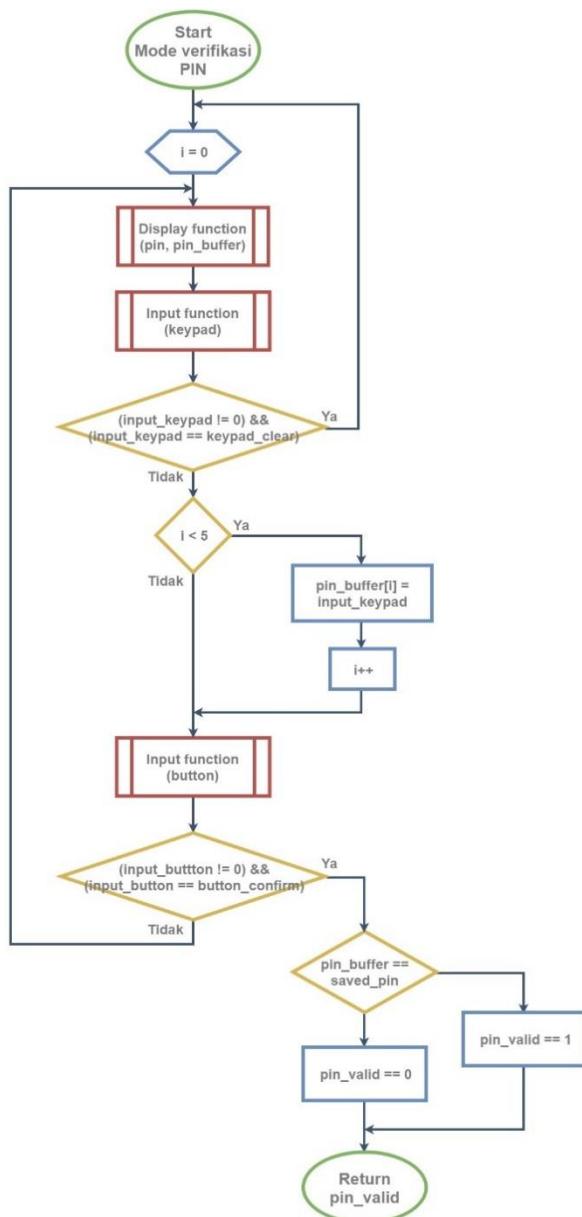
Gambar 28 Flowchart Program Utama

Data	Tipe Data	Keterangan
card_valid	Boolean	Nilai True akan menyatakan bahwa terdapat kartu yang valid di reader, nilai False menyatakan bahwa tidak ada kartu pada reader/kartu tidak valid.
pin_valid	Boolean	Nilai True akan menyatakan bahwa verifikasi PIN berhasil, nilai False menyatakan bahwa verifikasi PIN gagal.
success	Boolean	Nilai True akan menyatakan bahwa verifikasi sidik jari berhasil, nilai False menyatakan bahwa verifikasi sidik jari gagal.

end	Boolean	Nilai True akan menyatakan bahwa pengguna ingin mengakhiri operasi mesin ATM, nilai False menyatakan bahwa pengguna masih ingin melakukan transaksi lain.
-----	---------	---

Program utama akan memulai dengan mode idle, yaitu ketika mesin ATM sedang tidak digunakan siapapun. Lalu bila menerima input kartu ATM, mesin ATM akan melakukan fetching data nasabah dari server, dan memulai untuk melakukan verifikasi PIN. Setelah PIN berhasil dimasukkan dan benar, akan dicek keberadaan data template sidik jari. Bila tidak ditemukan, maka pengguna akan memasuki mode registrasi sidik jari; bila ditemukan, pengguna akan melakukan verifikasi sidik jari. Lalu bila verifikasi sidik jari berhasil, pengguna akan memasuki menu utama yang dapat melakukan beberapa proses transaksi yang tersedia.

3.2.1.1 Flowchart Mode Verifikasi PIN



Gambar 29 Flowchart Mode Verifikasi PIN

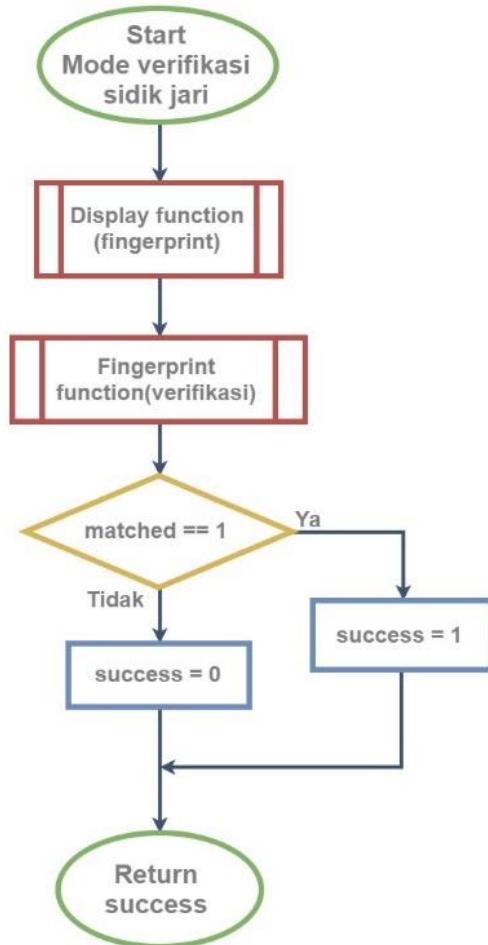
Data	Tipe Data	Keterangan
i	Integer	Variabel yang digunakan untuk iterasi looping, juga menunjukkan banyaknya angka PIN yang telah diinput oleh pengguna.
input_keypad	Integer	Variabel keluaran dari input function, menyatakan nilai penekanan keypad, 0 menyatakan bahwa keypad tidak ditekan dan nilai antara 1 sampai 16 menyatakan bahwa keypad tombol ke-sekian ditekan. keypad_cancel dan keypad_clear adalah salah representasi penekanan tombol cancel dan clear pada keypad, yang akan didefinisikan oleh suatu angka.
input_button	Integer	Variabel keluaran dari input function, menyatakan nilai penekanan button, 0 menyatakan bahwa button tidak ditekan dan nilai antara 1 sampai 6 menyatakan bahwa button tombol ke-sekian ditekan. button_confirm adalah salah representasi penekanan tombol konfirmasi benar pada button yang ada, yang akan didefinisikan oleh suatu angka.
pin_buffer	Array of integer	Variabel ini akan menyimpan nilai keypad yang ditekan pengguna ke dalam array yang akan merepresentasikan kode PIN pengguna.
pin_valid	Boolean	Variabel yang menyatakan konfirmasi cocok tidaknya PIN input dengan PIN tersimpan, True menyatakan cocok, False menyatakan tidak cocok.

Pada mode verifikasi PIN, akan ditampilkan layar dengan 6 baris kosong yang merupakan input PIN dari pengguna melalui keypad. Setiap input angka PIN maka baris kosong tersebut akan terisi dengan karakter ‘*’, bila pengguna ingin menghapus inputnya, digunakan tombol keypad clear dan bila ingin mengkonfirmasi PIN yang telah diinput tersebut, pengguna dapat menekan tombol button yang sesuai untuk konfirmasi.

3.2.1.1 Standar PIN pada sistem ATM

Berdasarkan regulasi dari BI, yaitu Surat Edaran Bank Indonesia No. 13/22/DASP tanggal 18 Oktober 2011 tentang Implementasi Teknologi Chip dan Penggunaan Personal Identification Number pada Kartu ATM dan / atau Kartu Debet yang diterbitkan di Indonesia. Bank Indonesia menetapkan peraturan PIN sebanyak 6 digit kombinasi angka. Dengan acuan surat edaran tersebut, Sistem keamanan sistem ATM ini dibuat memiliki 6 digit PIN sebagai salah satu sistem keamanan selain sidik jari.

3.2.1.2 Flowchart Mode Verifikasi Sidik Jari

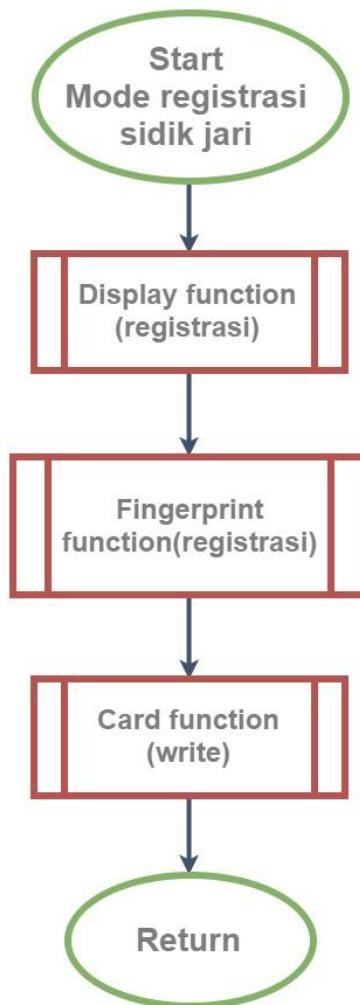


Gambar 30 Flowchart Mode Verifikasi Sidik Jari

Data	Tipe Data	Keterangan
matched	Boolean	Variabel yang dikembalikan oleh fingerprint function, True menyatakan bahwa pencocokan berhasil, False menyatakan bahwa pencocokan gagal.
success	Boolean	Variabel akan dikembalikan oleh fungsi ini, True menyatakan bahwa pencocokan berhasil, False menyatakan bahwa pencocokan gagal.

Pada mode verifikasi sidik jari, akan ditampilkan instruksi untuk meletakkan sidik jari pada sensor yang tersedia, lalu proses verifikasi sidik jari akan berlangsung. Bila berhasil maka pengguna dapat memasuki menu utama, dan bila gagal akan mengulangi input sidik jarinya. Fungsi akan mengembalikan nilai kesuksesan verifikasi, dengan 1 menyatakan berhasil, dan 0 menyatakan gagal.

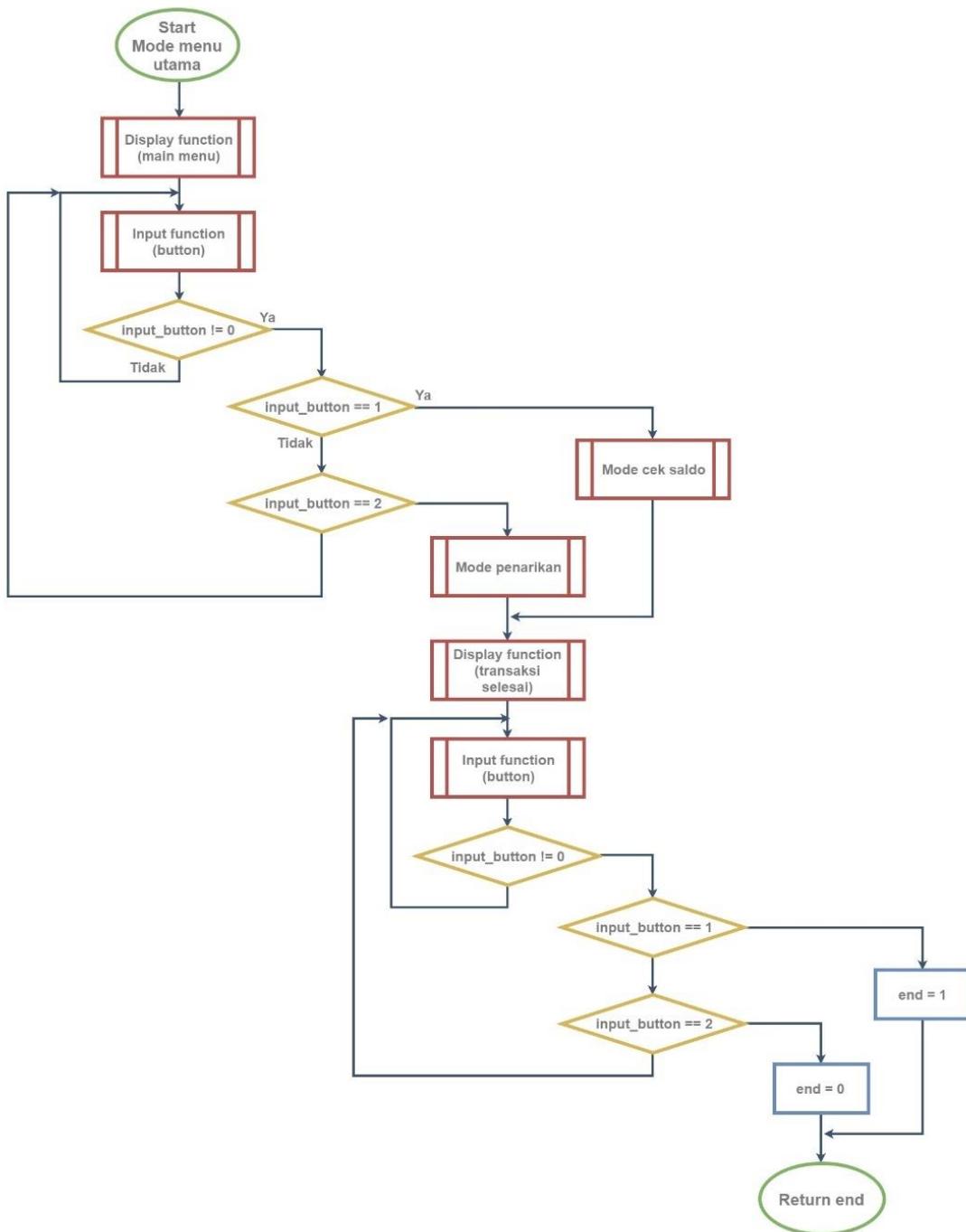
3.2.1.3 Flowchart Mode Registrasi Sidik Jari



Gambar 31 Flowchart Mode Registrasi Sidik Jari

Pada mode registrasi, akan ditampilkan instruksi untuk menempelkan jari pengguna pada sensor. Lalu fingerprint function untuk registrasi akan dipanggil dan setelah melalui proses registrasi, data template sidik jari akan disimpan ke dalam kartu dengan menggunakan fungsi write pada kartu.

3.2.1.4 Flowchart Mode Menu Utama

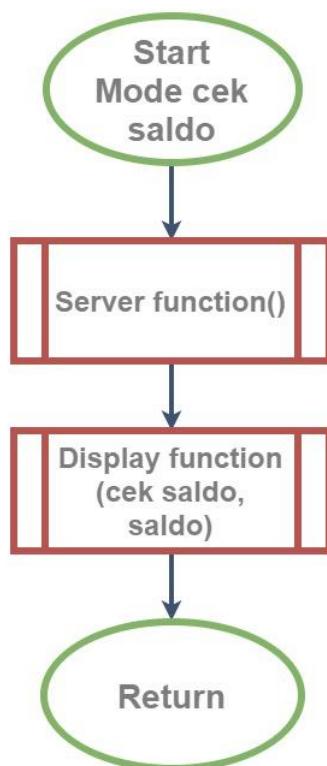


Gambar 32 Flowchart Mode Menu Utama

Data	Tipe Data	Keterangan
input_button	Integer	Variabel yang dikembalikan oleh input function, nilai 0 menyatakan tidak ada button ditekan, dan nilai 1-6 akan menyatakan penekanan button ke-sekian.
end	Boolean	Variabel akan dikembalikan oleh fungsi ini, True menyatakan bahwa operasi mesin ATM akan diakhiri, False menyatakan bahwa operasi mesin ATM akan dilanjutkan.

Pada mode ini, akan ditampilkan pilihan transaksi di layar, yaitu untuk melakukan pengecekan saldo atau melakukan penarikan saldo. Pilihan tersebut dipilih menggunakan button yang ada. Lalu setelah transaksi selesai dilakukan, akan ditampilkan pilihan untuk melakukan transaksi lain atau tidak. Bila tidak maka pengguna akan keluar dari menu utama dan mengakhiri operasi mesin ATM. Fungsi akan mengembalikan nilai yang menyatakan pengakhiran transaksi, dengan 1 menyatakan mengakhiri transaksi, dan 0 menyatakan melakukan transaksi lainnya.

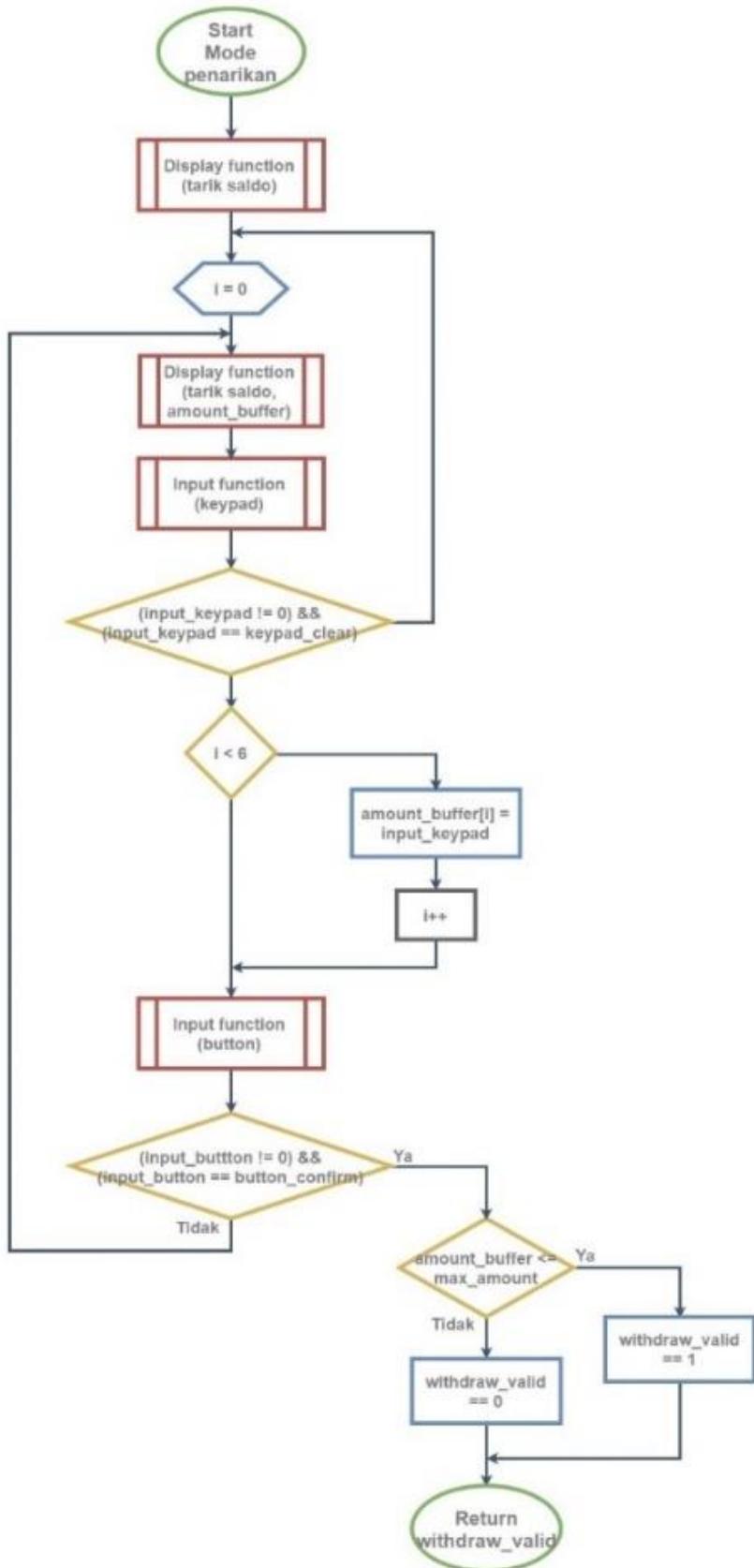
3.2.1.5 Flowchart Mode Cek Saldo



Gambar 33 Flowchart Mode Cek Saldo

Pada mode ini, akan dilakukan fetching data nasabah dari server, kemudian akan ditampilkan saldo nasabah yang tersisa pada layar.

3.2.1.6 Flowchart Mode Penarikan Saldo



Gambar 34 Flowchart Mode Penarikan Saldo

Data	Tipe Data	Keterangan
i	Integer	Variabel yang digunakan untuk iterasi looping, juga menunjukkan banyaknya angka yang telah diinput oleh pengguna.
input_keypad	Integer	Variabel keluaran dari input function, menyatakan nilai penekanan keypad, 0 menyatakan bahwa keypad tidak ditekan dan nilai antara 1 sampai 16 menyatakan bahwa keypad tombol ke-sekian ditekan. keypad_cancel dan keypad_clear adalah salah representasi penekanan tombol cancel dan clear pada keypad, yang akan didefinisikan oleh suatu angka.
input_button	Integer	Variabel keluaran dari input function, menyatakan nilai penekanan button, 0 menyatakan bahwa button tidak ditekan dan nilai antara 1 sampai 6 menyatakan bahwa button tombol ke-sekian ditekan. button_confirm adalah salah representasi penekanan tombol konfirmasi benar pada button yang ada, yang akan didefinisikan oleh suatu angka.
amount_buffer	Array of integer	Variabel ini akan menyimpan nilai keypad yang ditekan pengguna ke dalam array yang akan merepresentasikan jumlah uang yang ingin ditarik oleh pengguna.
max_amount	Integer	Variabel ini menyatakan jumlah maksimal yang dapat ditarik oleh pengguna, tergantung dari regulasi yang ada dan jumlah saldo pengguna saat ini.
withdraw_valid	Boolean	Variabel yang menyatakan valid tidaknya penarikan pengguna. True menyatakan valid, dan False menyatakan tidak valid.

Pada mode ini, pengguna akan diminta untuk menginput nilai uang yang akan diambil, dan setiap input akan ditampilkan nilainya pada layar. Bila ingin menghapus nilai yang telah diinput maka dapat digunakan tombol keypad clear, dan bila proses input telah selesai, pengguna dapat menekan tombol konfirmasi. Kemudian sebelum dibandingkan, array integer tadi akan dikonversi menjadi integer biasa, lalu akan dicek bila nilai tersebut valid, yaitu kurang dari saldo pengguna saat ini dan kurang dari batas maksimum sesuai regulasi, bila benar maka keberhasilan proses akan ditampilkan di layar. Fungsi akan mengembalikan nilai yang menyatakan keberhasilan transaksi, dengan 1 menyatakan berhasil, dan 0 menyatakan gagal.

3.2.1.6.1 Standar ketentuan tarik tunai dan transfer pada mesin ATM

Berdasarkan surat edaran BI no 17/51/DKSP, berikut ini merupakan batas penarikan tunai dan transfer pada mesin ATM yang dibedakan berdasarkan pada pemakaian kartu chip

Teknologi kartu magnetik strip

- Batas maksimal tarik tunai Rp. 10.000.000,00
- Batas maksimal transfer Rp. 25.000.000,00

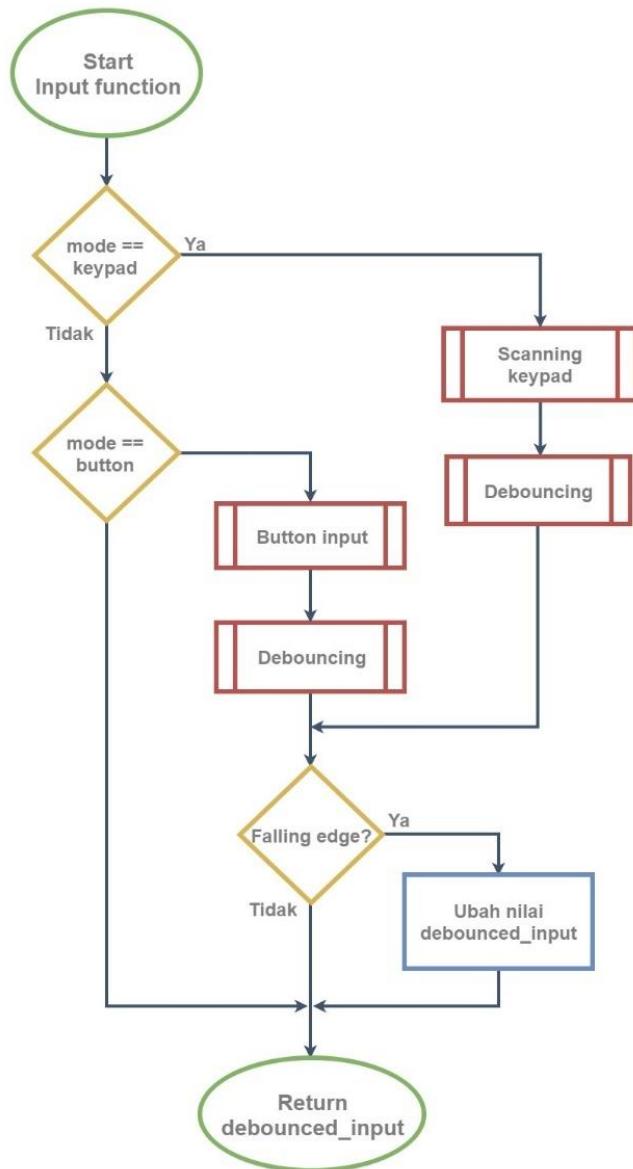
Teknologi kartu chip

- Batas maksimal tarik tunai Rp. 15.000.000,00
- Batas maksimal transfer Rp. 50.000.000,00

Mengacu pada surat edaran tersebut, karena standar teknologi kartu yang dipakai pada mesin ATM ini adalah menggunakan kartu chip (smart card). Namun pada riset kali ini, penarikan saldo dimungkinkan mengalami kenaikan. Hal tersebut karena kombinasi sistem keamanan sidik jari dan kartu ATM yang membuat sistem keamanan menjadi lebih baik.

Jika dilakukan pengamatan, besar transaksi tersebut mengacu pada standar keamanan sistem ATM.

3.2.2 Behavioral Input Function

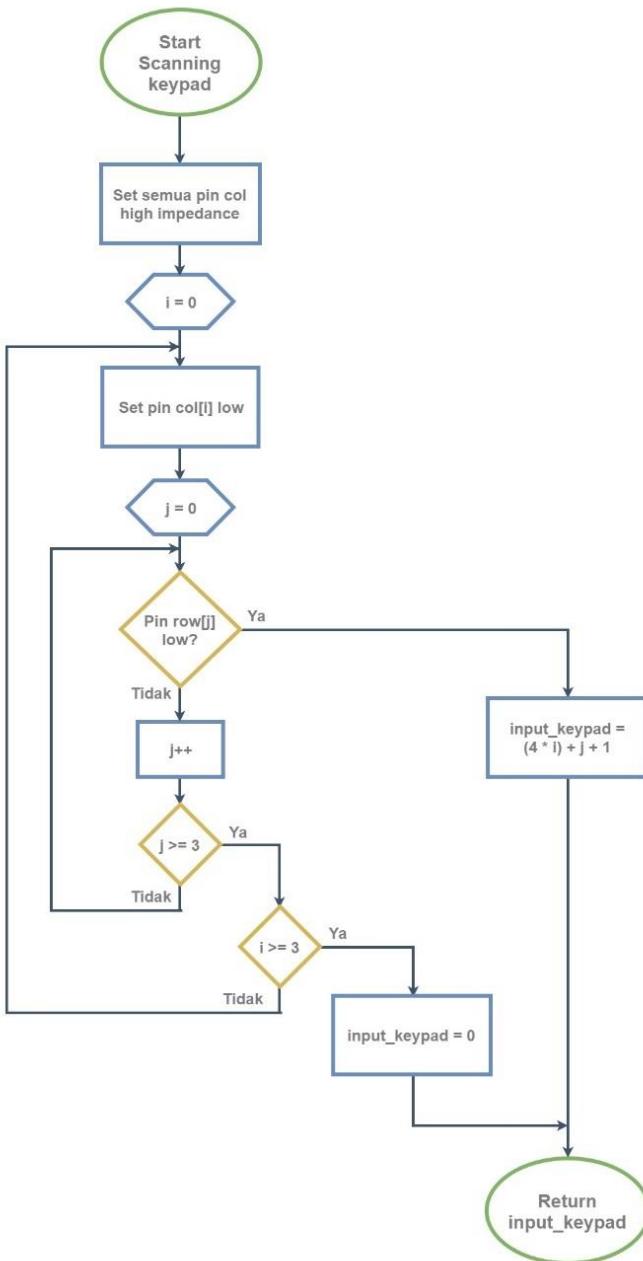


Gambar 35 Flowchart Input Function

Data	Tipe Data	Keterangan
mode	String	Variabel input yang digunakan untuk menunjukkan mode, pilihannya adalah keypad atau button.
debounced_input	Integer	Variabel yang akan dikembalikan oleh input function ini, menyatakan nilai penekanan keypad atau button sesuai mode, 0 menyatakan bahwa tidak ada input dan nilai angka akan menyatakan adanya penekanan tombol input.

Input function memiliki dua pilihan, yaitu untuk menerima input keypad atau button. Untuk input keypad, akan dilakukan proses scanning dan debouncing sampai didapat input dari pengguna. Untuk input button akan dilakukan proses debouncing dan tombol yang ditekan akan ditranslasikan menjadi nomor urutan button agar variabelnya mudah diproses. Input yang didapat hanya dibaca bila terjadi falling edge, yaitu tombol yang dilepas. Fungsi akan mengembalikan nilai input yang valid dan telah didebounce.

3.2.2.1 Flowchart Scanning Keypad



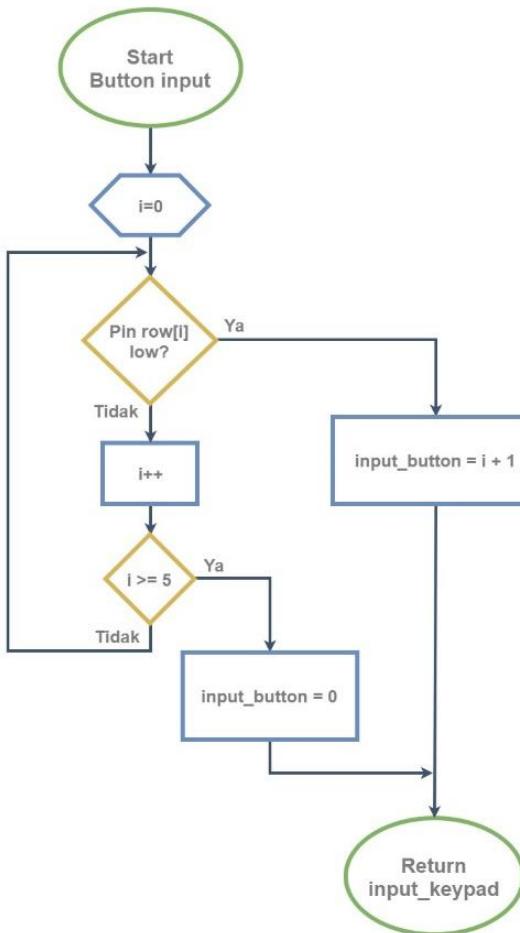
Gambar 36 Flowchart Scanning Keypad

Data	Tipe Data	Keterangan
i, j	Integer	Variabel yang digunakan untuk iterasi looping, variabel i untuk looping kolom, dan variabel j untuk looping baris.

row[], col[]	Array of boolean	Variabel ini akan berisi tegangan dari pin dan kolom untuk GPIO yang terhubung dengan keypad. Tipenya adalah boolean, pada mode read, True untuk penekanan button dan False untuk button tidak ditekan.
input_keypad	Integer	Variabel yang akan dikembalikan oleh scanning keypad ini, menyatakan nilai penekanan keypad, 0 menyatakan bahwa keypad tidak ditekan dan nilai antara 1 sampai 16 menyatakan bahwa keypad tombol ke-sekian ditekan.

Untuk melakukan scanning keypad, pertama semua pin kolom akan diatur high impedance, lalu proses looping akan dimulai dengan mengubah salah satunya menjadi tegangan low dan membaca tegangan pin baris. Bila ditemukan tegangan low maka tombol di posisi kolom ke-i dan baris ke-j sedang ditekan. Fungsi akan mengembalikan nilai input keypad, nilai 1-16 menyatakan penekanan keypad, dan nilai 0 menyatakan keypad tidak ditekan.

3.2.2.2 Flowchart Button Input



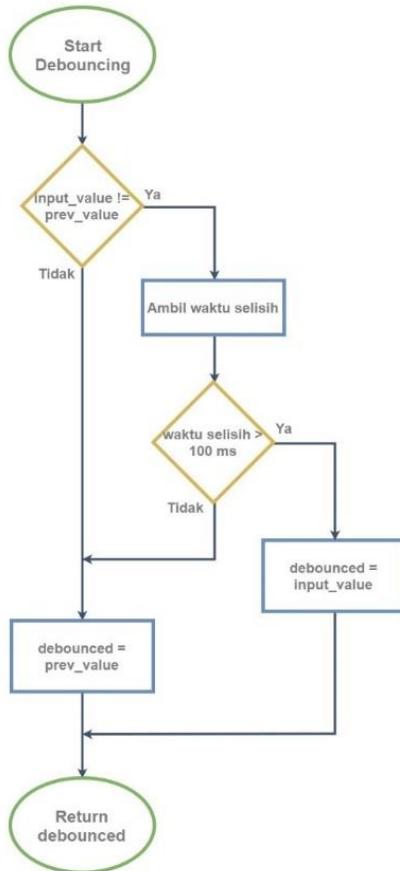
Gambar 37 Flowchart Button Input

Fungsi button input akan menerima input button, yaitu menyatakan button mana yang sedang ditekan. Fungsi akan mengembalikan nilai input button, dengan nilai 1-6 yang menyatakan urutan button tersebut dan nilai 0 menyatakan button tidak ditekan.

Data	Tipe Data	Keterangan
i	Integer	Variabel yang digunakan untuk iterasi looping semua button.

row[]	Array of boolean	Variabel ini akan berisi tegangan dari untuk GPIO yang terhubung dengan semua button. Tipenya adalah boolean, True untuk penekanan button dan False untuk button tidak ditekan.
input_button	Integer	Variabel yang akan dikembalikan oleh button input ini, menyatakan nilai penekanan button, 0 menyatakan bahwa button tidak ditekan dan nilai antara 1 sampai 6 menyatakan bahwa button tombol ke-sekian ditekan.

3.2.2.3 Flowchart Debouncing

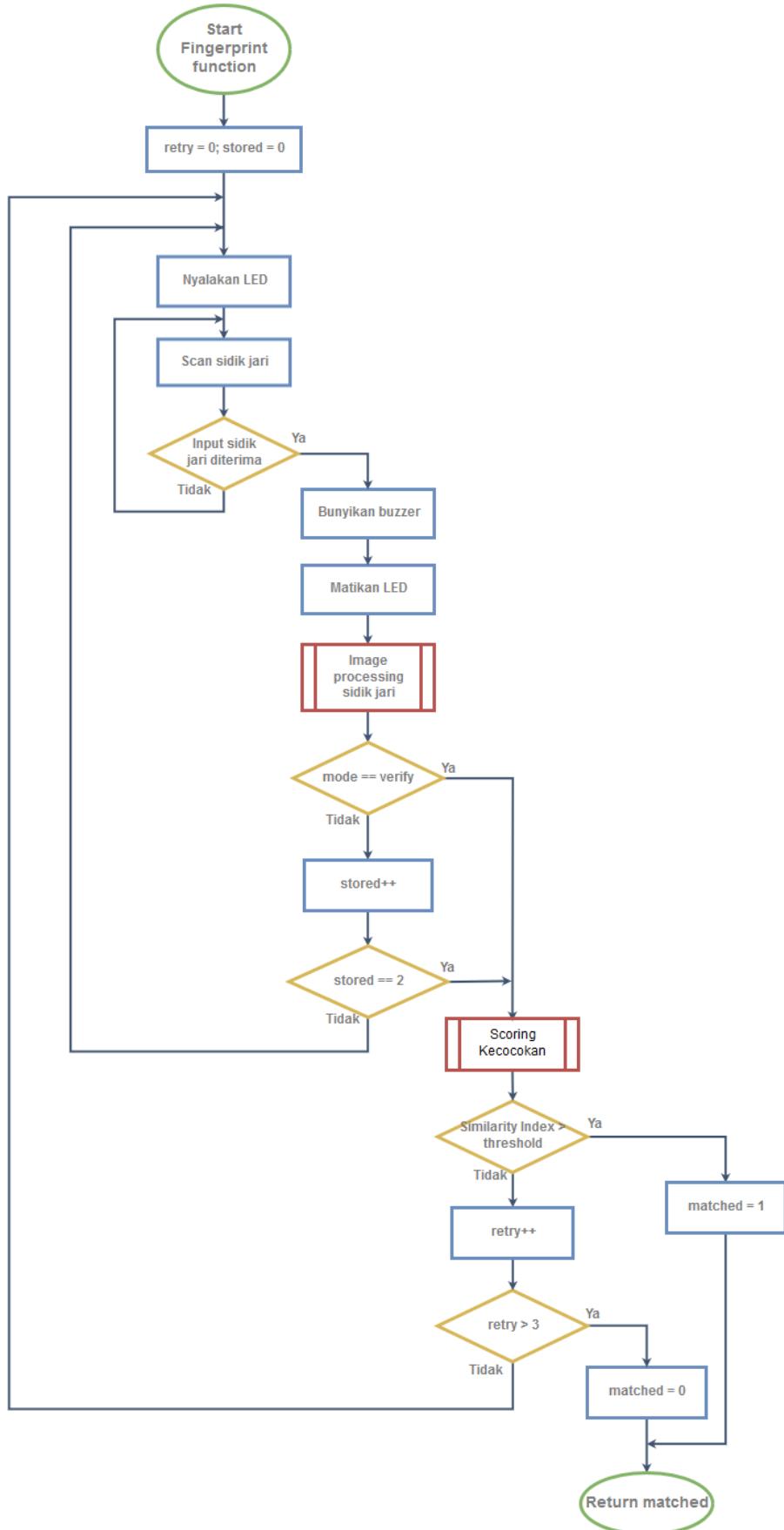


Gambar 38 Flowchart Debouncing

Data	Tipe Data	Keterangan
input_value	Boolean	Variabel input untuk fungsi ini, True menyatakan penekanan tombol, False menyatakan tombol tidak ditekan.
prev_value	Boolean	Variabel yang disimpan dari pemanggilan sebelumnya, True menyatakan penekanan tombol, False menyatakan tombol tidak ditekan.
debounced	Boolean	Variabel yang akan direturn oleh fungsi ini, True menyatakan penekanan tombol, False menyatakan tombol tidak ditekan.

Debouncing digunakan untuk menstabilkan pembacaan dari button dan keypad karena proses penekanan akan menghasilkan bagian yang berosilasi ketika transisi, diambil waktu debouncing adalah 100 ms. Fungsi akan mengembalikan nilai setelah melalui proses debouncing.

3.2.3 Behavioral Fingerprint Function

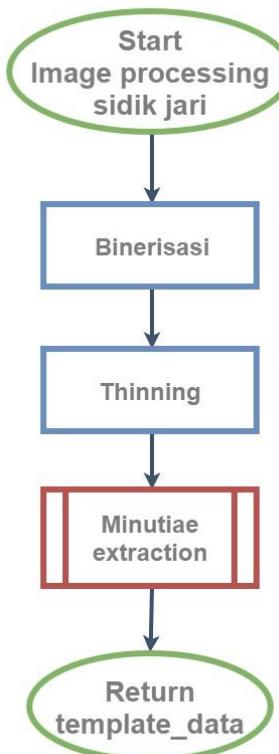


Gambar 39 Flowchart Fingerprint Function

Data	Tipe Data	Keterangan
mode	String	Variabel yang menyatakan mode fungsi ini, terdapat dua pilihan, yaitu regist (registrasi) atau verify (verifikasi).
retry	Integer	Variabel untuk iterasi pengulangan input sidik jari ketika gagal verifikasi.
stored	Integer	Variabel untuk iterasi ketika melakukan registrasi, menyatakan jumlah data template sidik jari yang tersimpan di memori. Untuk melakukan registrasi diperlukan 2 data template sidik jari yang sama tersimpan di memori.
Similarity Index	Float	Variabel yang menyatakan ringkat kemiripan atau kecocokan dari data template sidik jari yang dibandingkan.
Matched	Boolean	Variabel yang akan dikembalikan oleh fungsi ini yang menyatakan keberhasilan verifikasi atau registrasi. True menyatakan berhasil, False menyatakan gagal.

Fungsi ini memiliki dua mode, yaitu untuk verifikasi dan registrasi. Dimulai dengan meminta pengguna untuk meletakkan jarinya pada sensor lalu ketika gambar diterima akan dilakukan proses pengambilan gambar dan image processing lalu extraction. Lalu bila mode verifikasi, maka data template yang didapat kemudian dibandingkan dengan data yang ada tersimpan di kartu. Bila mode registrasi maka data template yang didapat kemudian disimpan terlebih dahulu lalu akan diminta input sidik jari untuk kedua kalinya dengan melalui proses yang sama. Fungsi akan mengembalikan nilai 1 bila diterima cocok, dan 0 bila tidak cocok.

3.2.3.1 Flowchart Image Processing

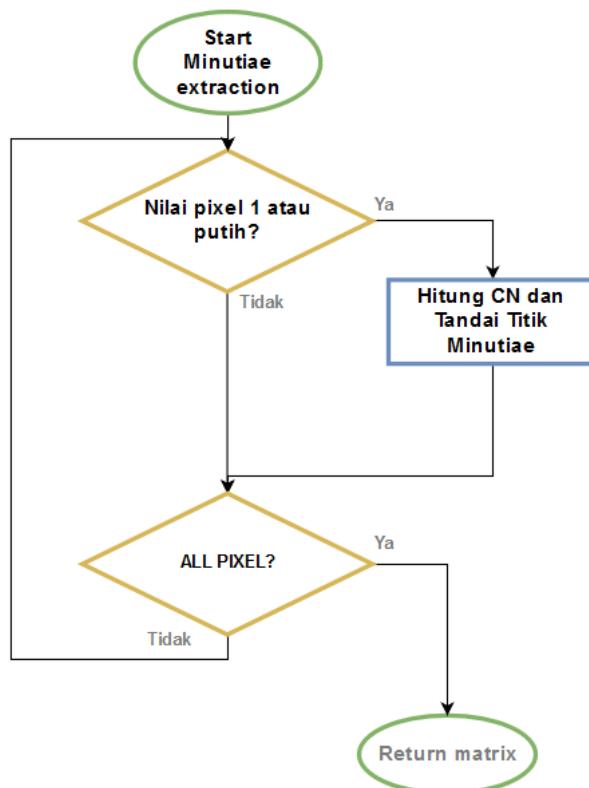


Gambar 40 Flowchart Image Processing

Data	Tipe Data	Keterangan
template_data	Array of bytes	Variabel berisi data template sidik jari yang telah diproses.

Fungsi ini akan melakukan image processing dari gambar grayscale sidik jari. Pertama akan dilakukan binerisasi untuk membuat gambar sidik jari menjadi hitam putih saja atau hanya bernilai logika 0 dan 1. Lalu akan dilakukan thinning untuk membuat pola sidik jari selebar satu pixel untuk memudahkan pencarian fitur minutiae. Setelah itu, akan dilakukan proses ekstraksi minutiae. Fungsi ini akan mengembalikan nilai template data sidik jari.

3.2.3.2 Flowchart Minutiae Extraction



Gambar 41 Flowchart Minutiae Extraction

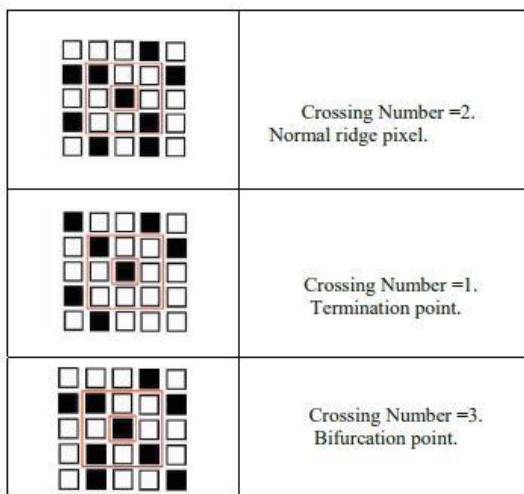
Data	Tipe Data	Keterangan
matrix	Array of bytes	Variabel berisi data template sidik jari yang telah diproses.
CN	Integer	Variabel yang menentukan karakteristik minutiae

Proses minutiae extraction akan dilakukan dengan mencari reference point untuk template, yaitu posisi fitur level 1 atau pola dasar sidik jari. Setelah itu, looping akan dilakukan pada sumbu x dan sumbu y untuk melakukan pengecekan apakah pixel berawarna putih sampai ditemukannya titik minutiae lalu koordinat minutiae tersebut disimpan. Jika sudah ditemukan, maka Crossing Number dihitung untuk menentukan tipe karakteristik minutiae dengan menggunakan rumus berikut ini.

$$CN = 0,5 \sum_{i=1}^8 | P_i - P_{i+1} | \text{ with } P_9 = P_1$$

P_4	P_5	P_6
P_5	P	P_7
P_6	P_7	P_8

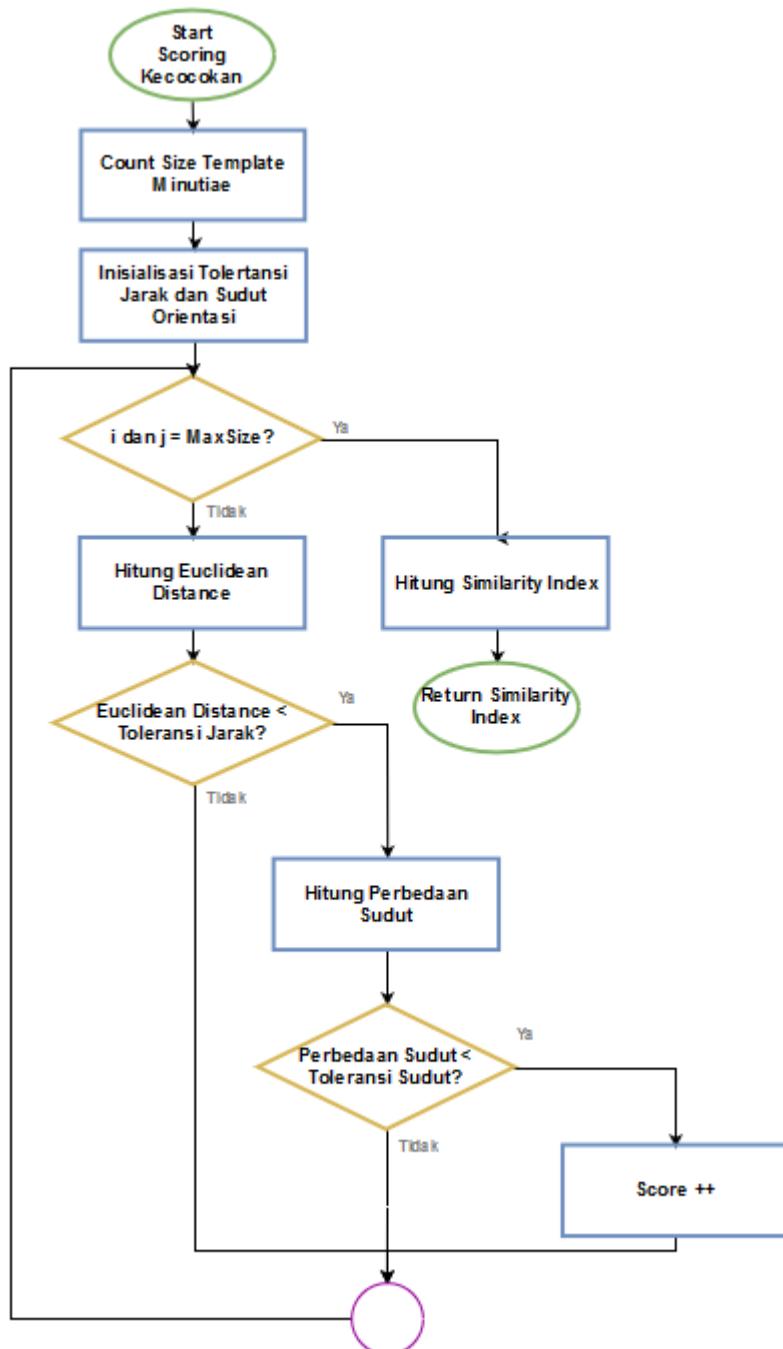
Penentuan tipe dari suatu minutiae adalah dengan melihat 3x3 window dari titik yang dicek. Apabila titik tengah 1 dan hanya memiliki 1 value neighbor, maka central tersebut adalah termination. Apabila central adalah 1 dan memiliki 3 one-value neighbor, maka central tersebut adalah bifucation point. Apabila central adalah 1 dan memiliki 2 one-value neighbor, maka pixel tersebut bukanlah minutiae dan pixel biasa.



Gambar 42 Penentuan Tipe Minutiae berdasarkan Metode Crossing Number

Proses ini akan terus berulang sampai semua pixel pada gambar sidik jari yang telah *dipreprocessing* terlingkupi. Fungsi akan mengembalikan nilai matriks yang berupa array yang berisi koordinat minutiae.

3.2.3.3 Flowchart Scoring Kecocokan



Gambar 43 Flowchart Scoring Kecocokan

Data	Tipe Data	Keterangan
Template minutiae	Array of bytes	Variabel berisi data template sidik jari yang telah diproses.
Toleransi sudut dan jarak	Integer	Variabel yang menentukan batas sudut dan jarak
i dan j	Integer	Variabel Looping

Euclidean Distance	Float	Variabel menghitung jarak antar karakteristik minutiae
Similarity Index	Float	Varabel yang menghitung tingkat kemiripan suatu template jika dibandingkan dengan template lain
Score	Integer	Variabel yang bertambah jika kondisi perbedaan sudut dan jarak dipenuhi atau berada di bawah toleransi.

Fungsi ini memiliki 2 buah input, yaitu template sidik jari pertama dan template sidik jari kedua. Output dari fungsi ini adalah tingkat kemiripan dan score dari perbandingan kedua sidik jari. Fungsi ini pertama tentunya akan membaca size template sidik jari dan mengatur nilai awal untuk threshold atau toleransi nilai jarak dan sudut orientasi yang masih dapat dikatakan sebagai minutiae yang sama. Threshold ini akan digunakan untuk batas setiap template. Sidik jari dapat dikatakan sesuai atau lolos verifikasi jika berada di dalam rentang threshold ini.

Euclidean Distance antar fitur minutiae akan dihitung dengan cara menghitung selisih posisi pada titik koordinat x dan y. Setelah itu, dicari dengan menggunakan rumus phytagoras untuk mendapatkan jarak terdekat. Rumus yang digunakan adalah sebagai berikut.

$$Ed = \sqrt{dx^2 + dy^2}$$

Jika jarak yang dihasilkan kurang dari threshold jarak yang ditentukan (15), maka akan dicek sudut orientasinya terhadap acuan. Jika kurang dari threshold sudut yang ditentukan (14), maka *score* akan bertambah satu yang menandakan fitur minutiae *match*. Prinsipnya adalah sebagai berikut

$$sd(m_i, m_j) = 1 \Leftrightarrow \sqrt{(x_i - x_j)^2 + (y_i - y_j)^2} \leq r_0$$

$$dd(m_i, m_j) = 1 \Leftrightarrow \min(|\theta_i - \theta_j|, 360 - |\theta_i - \theta_j|) < \theta_0$$

Setiap kondisi atas terpenuhi, maka score akan bertambah satu. Hal ini akan terus berulang sampai seluruh fitur minutiae melalui proses ini. Pada akhirnya, tingkat kemiripan dapat dicari dengan rumus

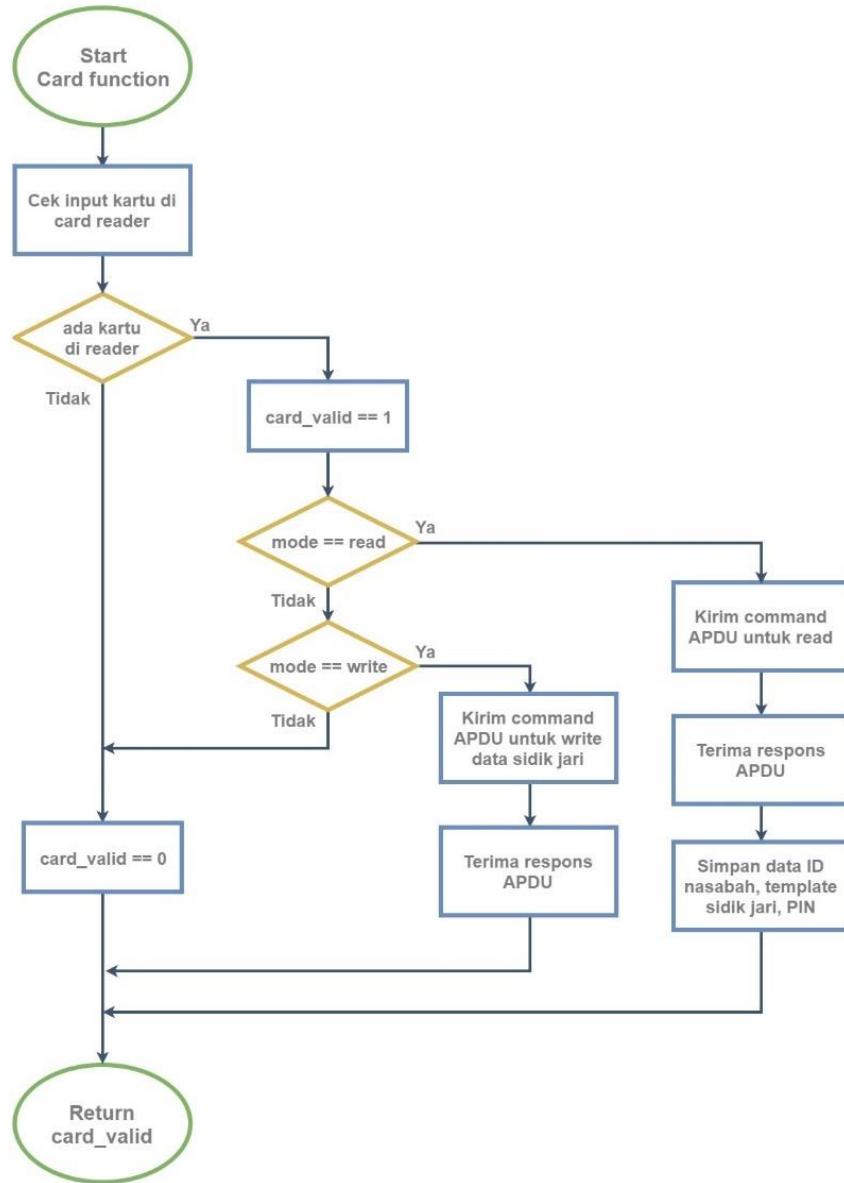
$$SM = \sqrt{\frac{Score^2}{NA * NB}}$$

Keterangan:

- NA = Size Template Minutiae Sidik Jari A
- NB = Size Template Minutiae Sidik Jari B

Tingkat kemiripan ini akan dijadikan perbandingan dengan *threshold* yang nantinya menjadi penentu apakah suatu pasangan template sidik jari *match* atau tidak.

3.2.4 Behavioral Card Function



Gambar 44 Flowchart Card Function

Data	Tipe Data	Keterangan
mode	String	Variabel yang menyatakan mode fungsi ini, terdapat dua pilihan, yaitu read dan write.
card_valid	Boolean	Variabel yang akan dikembalikan oleh fungsi ini yang menyatakan valid atau tidaknya kartu pada card reader. True menyatakan bahwa ada kartu dan valid, False menyatakan bahwa kartu tidak ada/tidak valid.

Pertama fungsi akan mengecek keberadaan kartu pada reader, bila ada dan valid maka akan dikembalikan nilainya, 1 bila valid dan 0 bila tidak. Card function memiliki dua mode, yaitu read dan write. Ketika dilakukan mode read, akan dilakukan proses pembacaan data di kartu dan disimpan pada variabel. Ketika dilakukan mode write, akan dilakukan proses penulisan data template sidik jari pada kartu yang digunakan.

3.2.4.1 Protokol APDU

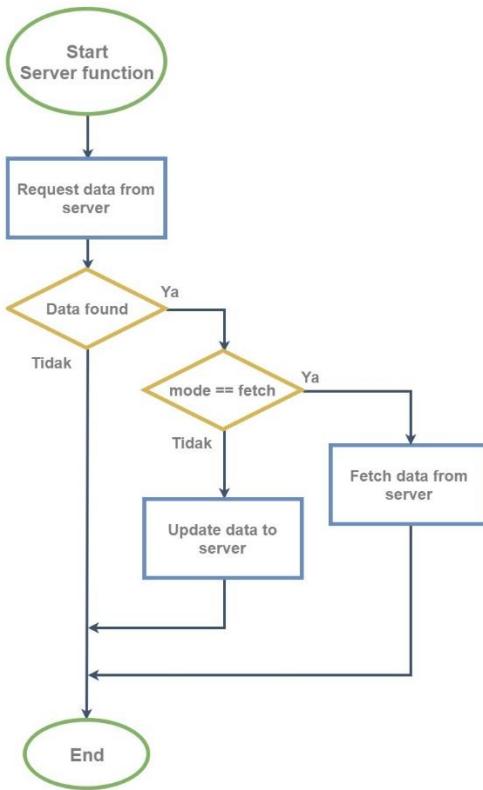
Application Protocol Data Unit (APDU) adalah unit komunikasi antara *smart card* dan *card reader*. Struktur APDU didefinisikan oleh Organisasi ISO/IEC 7816-4 *Security and Commands for interchange*.

Dalam APDU terdapat dua kategori, yaitu *Command APDU* dan *Response APDU*. Command APDU dikirim oleh *card reader* ke *smart card*. Command tersebut berukuran 4-byte. Response APDU dikirim oleh *smart card* ke *card reader*. Response tersebut berukuran 2-bytes. Untuk lebih jelasnya dapat dilihat pada table dibawah ini

Command APDU		
Field name	Length (bytes)	Description
CLA	1	Instruction class - indicates the type of command, e.g. interindustry or proprietary
INS	1	Instruction code - indicates the specific command, e.g. "write data"
P1-P2	2	Instruction parameters for the command, e.g. offset into file at which to write the data
L _c	0, 1 or 3	Encodes the number (N _c) of bytes of command data to follow 0 bytes denotes N _c =0 1 byte with a value from 1 to 255 denotes N _c with the same value 3 bytes, the first of which must be 0, denotes N _c in the range 1 to 65 535 (all three bytes may not be zero)
Command data	N _c	N _c bytes of data
L _e	0, 1, 2 or 3	Encodes the maximum number (N _e) of response bytes expected 0 bytes denotes N _e =0 1 byte in the range 1 to 255 denotes that value of N _e , or 0 denotes N _e =256 2 bytes (if L _c was present in the command) in the range 1 to 65 535 denotes N _e of that value, or two zero bytes denotes 65 536 3 bytes (if L _c was not present in the command), the first of which must be 0, denote N _e in the same way as two-byte L _e
Response APDU		
Response data	N _r (at most N _e)	Response data
SW1-SW2 (Response trailer)	2	Command processing status, e.g. 90 00 (hexadecimal) indicates success

Gambar 45 Command and Response APDU

3.2.5 Behavioral Server Function



Gambar 46 Flowchart Server Function

Data	Tipe Data	Keterangan
mode	String	Variabel yang menyatakan mode fungsi ini, terdapat dua pilihan, yaitu fetch dan update.

Pertama fungsi akan melakukan request data yang bersangkutan ke server, bila ditemukan maka proses akan dilanjutkan. Fungsi ini memiliki dua mode, yaitu fetch dan update. Fetch akan meminta data dari server dan hanya menerimanya. Update akan melakukan proses pengubahan data yang tersimpan di server.

3.2.5.1 Protokol SQL

Pada implementasi database server ini, akan digunakan MySQL. MySQL adalah software open-source yang menggunakan Relational DBMS (Database Management System) yaitu model database yang bersifat table-oriented. MySQL kami pilih sebagai database kami karena mudah didapatkan dan tidak memerlukan biaya untuk implementasinya.

Pada database, sebuah tabel didefinisikan oleh suatu nama dan berisi beberapa atribut tetap dengan tipe data yang tetap. Tabel berisi record-record yang akan memiliki data pada setiap atributnya. SQL (Structured Query Language) adalah bahasa yang digunakan untuk manajemen data pada relational database ini.

SQL memiliki beberapa command yang dapat digunakan untuk manajemen database, diantaranya adalah sebagai berikut

- CREATE

Command ini digunakan untuk membuat objek baru, bisa sebuah database, atau sebuah table. Contoh, command `CREATE DATABASE bank` akan membuat database baru bernama bank di server.

- **SHOW**

Command ini digunakan untuk menampilkan isi dari objek target, bisa database atau table. Contoh, command `SHOW TABLES` akan menunjukkan daftar tabel-tabel yang ada di database yang sedang diakses.

- **USE**

Command ini digunakan untuk mengakses sebuah database, bila ingin melakukan operasi di database lain, gunakan command ini untuk berpindah database. Contoh, command `USE mahasiswa` akan mengubah database yang diakses menjadi database mahasiswa dan semua operasi yang dilakukan seterusnya akan berada di database ini sampai diubah.

- **DESCRIBE**

Command ini digunakan untuk menunjukkan bentuk dari table. Contoh, command `DESCRIBE nasabah` akan menampilkan bentuk dari tabel nasabah dengan semua atributnya dan tipe datanya.

- **INSERT**

Command ini digunakan untuk menambah record baru pada tabel. Dapat dilengkapi dengan `INTO` untuk menyatakan tabel mana yang ingin ditambah recordnya dan `VALUES` untuk menyatakan isi dari record yang akan ditambahkan.

- **SELECT**

Command ini digunakan untuk mencari sebuah record pada tabel. Dapat dilengkap dengan `FROM` untuk menyatakan tabel mana yang ingin dicari recordnya, dan `WHERE` untuk melakukan filter lebih spesifik dari atributnya.

- **UPDATE**

Command ini digunakan untuk mengubah isi dari sebuah record pada tabel. Dapat dilengkapi dengan `SET` untuk menyatakan atribut mana yang diubah, dan `WHERE` untuk melakukan filter dari record yang ada.

3.2.5.2 Library MySQLdb

MySQLdb adalah module python untuk MySQL, dapat diambil dengan umum di internet, atau bila menggunakan Linux dapat menggunakan package manager dan menginstall package python-mysql.

Pada library ini terdapat beberapa fungsi yang dapat kami gunakan yaitu

- `MySQLdb.connect()`

Fungsi ini digunakan untuk melakukan koneksi dengan server MySQL yang aktif. Argumen dari fungsi diisi dengan host, user, password(bila ada), dan nama database yang ingin diakses. Bila operasi telah selesai, akses database sebaiknya ditutup dengan `database-name.close()` untuk tidak membebani server.

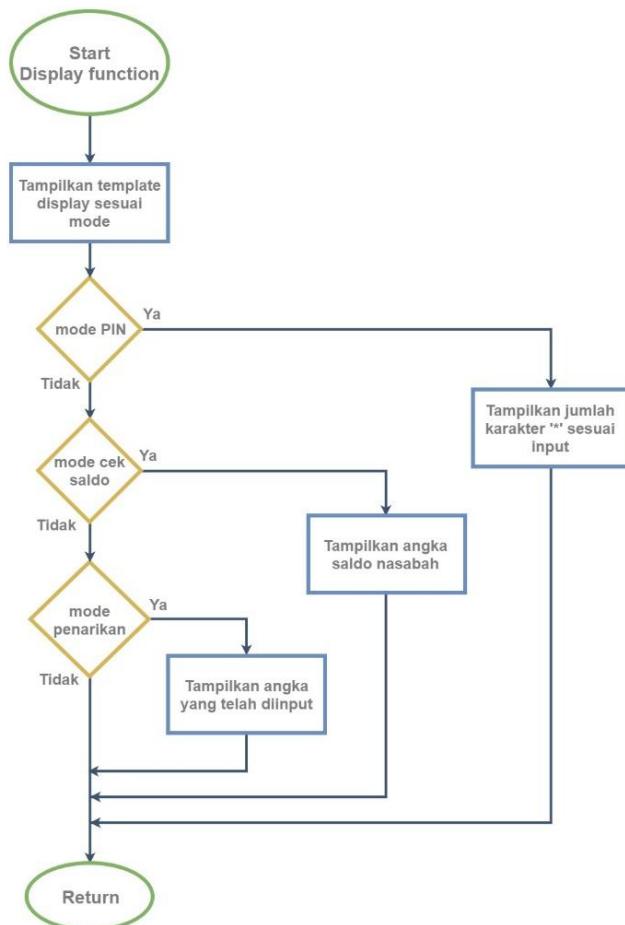
- `database-name.cursor()`

Fungsi ini digunakan untuk membuat sebuah cursor pada database-name. Cursor adalah cara python berinteraksi dengan data, mirip seperti sebuah pointer file pada bahasa C. Bila cursor telah selesai digunakan, sebaiknya ditutup dengan `cursor-name.close()` untuk tidak membebani komputer yang digunakan.

- `cursor-name.execute()`

Lalu fungsi ini digunakan untuk mengeksekusi command-command SQL melalui cursor. Contoh, dengan cursor bernama `cursor-name`, misal digunakan command `cursor-name.execute(SHOW TABLES)` maka akan ditampilkan daftar tabel yang ada di database yang sedang diakses oleh cursor.

3.2.6 Behavior Display Function



Gambar 47 Flowchart Display Function

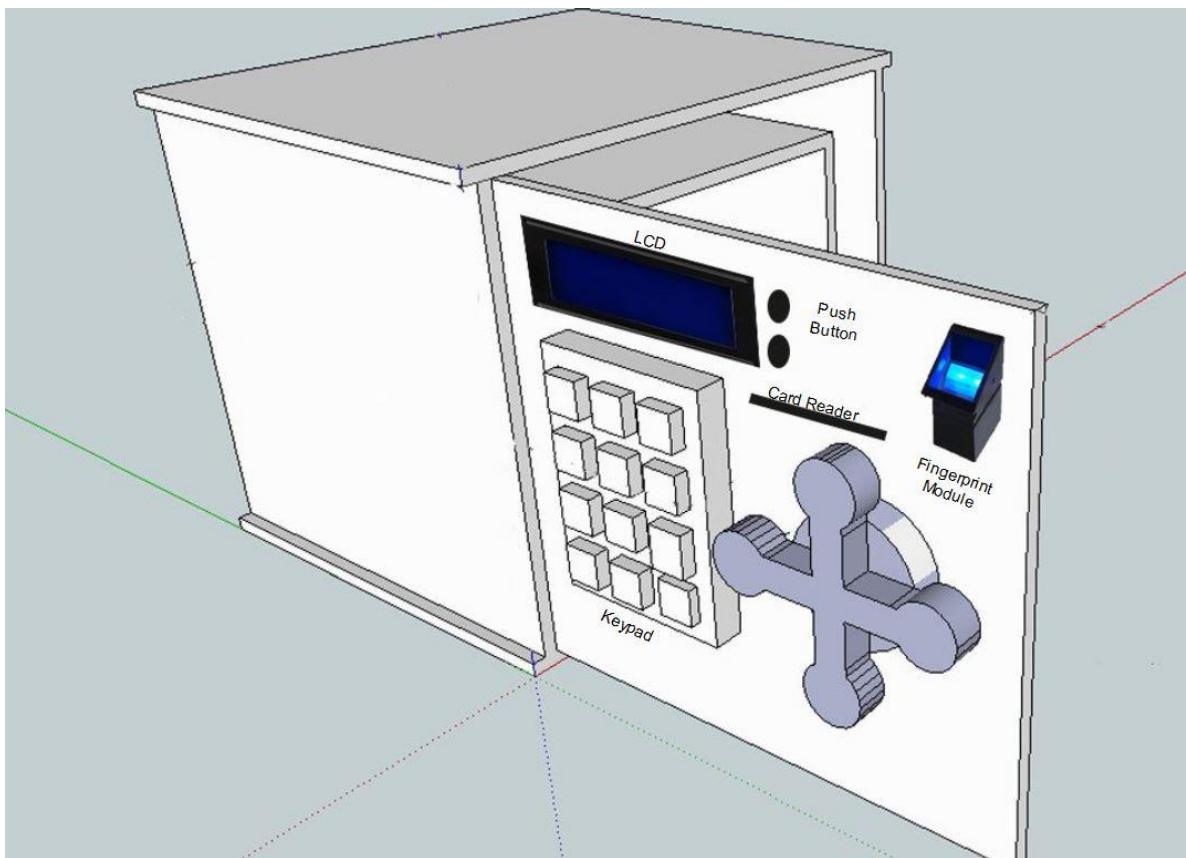
Data	Tipe Data	Keterangan
mode	String	Variabel yang menyatakan mode fungsi ini, terdapat beberapa pilihan yaitu diantaranya idle, pin, fingerprint, menu, check, withdraw, dan exit.

Fungsi ini memiliki beberapa template tersimpan untuk mode yang diterimanya, seperti mode idle, mode verifikasi pin, dan mode lainnya. Lalu fungsi ini akan mengecek beberapa

mode khusus yaitu mode PIN, cek saldo, dan penerikan saldo, karena pada mode ini nilai yang ditampilkan akan berubah sesuai variabel tersimpan.

3.3 Hardware

3.3.1 Desain Fisik



Gambar 48 Mock-Up Fingershield ATM

Alat yang akan dibuat adalah tempat penyimpanan uang yang dapat mencerminkan proses-proses yang terjadi pada mesin ATM. Box ini terbuat dari kayu dan terdiri dari pintu yang akan terbuka yang menganalogikan keluarnya uang pada saat penarikan tunai saldo. Pada pintu ini, terpasang keypad, push-button, LCD, dan fingerprint sensor, serta card reader. Prinsipnya jika seluruh autentifikasi sudah terlewati dan menu transaksi yang dipilih, maka servo motor penahan pintu akan merubah sudut atau posisinya sehingga pintu yang tadi terganjal menjadi terbuka. Jika menu cek saldo yang dipilih, maka pintu tidak akan terbuka tetapi output saldo akan ditampilkan pada LCD. Komponen lain seperti mikrokontroler dan uang akan diletakkan di dalam box.

Dimensi : 40 cm x 30 cm x 30 cm (Panjang x Lebar x Tinggi)

3.3.2 Komponen

3.3.2.1 Mikrokontroler

Seluruh system dan data akan diproses oleh mikrokontroler sebagai alat komputasi dengan dimensi yang kecil. Mikroprosesor yang menjadi pertimbangan untuk digunakan antara lain Arduino dan Raspberry Pi.

Tabel 1 Pemilihan Komponen Mikrokontroler

Spesifikasi	Arduino Mega	Raspberry Pi B
Gambar Fisik		
Fitur	54 GPIO (4 UART termasuk soft-serial, 1 SPI, 1 I2C) 16 Analog input pins	40 GPIO (1 UART) 4 USB ports Full HDMI port Ethernet port 3.5mm analogue audio-video jack Camera serial interface (CSI) Display serial interface (DSI) Micro SD card slot Arduino Uno R-3 Connectivity
Prosesor	16 MHz ATMega 2560	1.2 GHz quad-core ARM Cortex-A53 1 GB RAM
Memori	8 KB SRAM, 4 KB EEPROM, 256 KB FLASH	8 KB SRAM, 4 KB EEPROM, 1 MB SRAM, 1 MB EEPROM, 4 MB FLASH
Clock Speed	16 Mhz	900 Mhz
Operating Voltage	5 Volts	3.3 Volts
Suitable For	Hardware, <i>prototyping</i>	Software, Server
Bahasa Pemrograman	Arduino, C	Phyton, C, C++, Java, Ruby
Dimensi	101.52 mm x 53.3 mm	85.6 mm x 56 mm
Berat	37 grams	45 grams
Harga	Rp 150.000	Rp 700.000

Fingershield ATM membutuhkan komunikasi ke server melalui kabel *Ethernet* dan komunikasi ke *card reader* melalui port USB. Fitur-fitur ini terdapat pada Raspberry Pi dan harus menambahkan modul yang terpisah pada Arduino Mega. Selain itu, proses yang diolah oleh mikrokontroler sangat banyak termasuk pengolahan citra sidik jari sehingga membutuhkan prosesor 32 bit agar lebih cepat dan tidak membuat nasabah menunggu. Selain itu, karena menyangkut masalah keamanan mesin ATM tentu mikrokontroler yang digunakan harus memadai dan lebih dari cukup. Artinya spesifikasinya tidak boleh *bottle neck* untuk mengurangi resiko-resiko yang dapat terjadi. Raspberry Pi juga lebih cocok

dalam desain software dan sebagai pengolah server karena spesifikasinya sudah seperti mini computer. Arduino Mega memiliki kelebihan pada harga yang murah dan GPIO yang banyak sehingga memungkinkan untuk memakai komponen lebih banyak.

Dengan pertimbangan-pertimbangan tersebut, mikrokontroller Raspberry Pi yang terpilih dan akan dipakai pada sistem kami.

3.3.2.2 Fingerprint Module

Untuk membaca sidik jari dari user, dibutuhkan sensor sidik jari untuk melakukan *scanning* dan *image processing* sampai mendapatkan *template data* sidik jari. Modul sidik jari yang dijadikan pertimbangan antara lain optical sensor dan kapasitif sensor.

Tabel 2 Pemilihan Komponen Fingerprint Module

Spesifikasi	Optical Sensor	Capacitive Sensor
Gambar Fisik		
Tipe	R305	R306
Power	3.6 - 6 V	4.2 - 6V
Dimensi Window	18x22 mm	11x15 mm
Scanning Speed	< 0.5s	< 0.5 s
Resolusi	508 DPI	363 DPI
Template Size	512 Bytes	512 Bytes
FAR	<0.001%	<0.001%
FRR	<0.1%	<0.1%
Baudrate	57600 Bps	57600 Bps
Communication	UART and USB	UART and USB
Working Environment	Temperature : 10-44 °C Humidity : 40% - 85%	Temperature : 20-55 °C Humidity : 10% - 90%
Harga	Rp 650.000	Rp 550.000

Fitur keamanan autentifikasi sidik jari merupakan fitur utama pada sistem kami. Oleh karena itu, dibutuhkan sensor sidik jari yang sebaik mungkin dalam melakukan pengolahannya. Optical Sensor memiliki kelebihan dalam hal umur yang tahan lama karena tidak membutuhkan banyak maintenance seperti sensor kapasitif yang harus dirawat permukaannya dan *coatingnya*, serta dapat mengalami korosi jika digunakan terus menerus dan terpapar faktor eksternal lingkungan. Selain itu, resolusi sensor optic lebih tinggi dan pengambilan gambar sidik jari lebih luas sehingga menghasilkan gambar sidik jari yang lebih baik.

Dengan pertimbangan-pertimbangan tersebut, optical sensor dipilih menjadi sensor sidik jari yang akan digunakan pada sistem ini

3.3.2.3 Display Monitor

Output sistem dari setiap proses akan ditampilkan pada display monitor sebagai user interface. Display monitor yang menjadi pertimbangan adalah TFT monitor, HDMI Display, dan LCD 20x4.

Tabel 3 Pemilihan Komponen Display Monitor

Spesifikasi	TFT Monitor	HDMI Display	LCD 20x4
Gambar Fisik			
Size	3,2 inch	5 inch	2.4 inch
Communication	Serial SPI, TTL	HDMI	TTL
Resolution	240x320	800x400	20x4 character
GUI	RGB	RGB	Monochrom
Harga	Rp 200.000	Rp 650.000	Rp 109.000

User interface nasabah dengan sistem akan menggunakan monitor built in dari sistem itu sendiri. Pada sistem mesin ATM, tidak dibutuhkan perbedaan warna-warna atau GUI yang bagus. User atau nasabah bank cenderung membutuhkan desain yang simple dan cepat dalam melakukan transaksi. LCD 20x4 memiliki keunggulan karena memiliki desain yang simple dan harga penjualan juga paling murah, serta sudah dapat memberikan informasi atau instruksi yang cukup untuk nasabah ketika melakukan verifikasi dan transaksi. Kompleksitas algoritmanya pun jauh di bawah HDMI dan TFT yang membutuhkan pengaturan pixel dan warna.

Dengan pertimbangan-pertimbangan tersebut, LCD 20x4 dipilih menjadi monitor yang akan digunakan sebagai user interface sistem ini.

3.3.2.4 LED

LED diperlukan sebagai indikator saat melakukan *scanning* sidik jari untuk menentukan waktu saat sidik jari sudah terbaca. Alternatif yang terdapat untuk LED ini hanya berdasarkan dari diameter LED.

Tabel 4 Pemilihan Komponen LED

Spesifikasi	LED 10mm	LED 5mm	LED 3mm
Gambar Fisik			
Size	10 mm	5 mm	3 mm
Harga	Rp 1.500	Rp 700	Rp 200

Berdasarkan alternatif yang ada maka kami menggunakan LED dengan diameter 5mm karena persediaan LED 5mm lebih mudah didapatkan, selain itu faktor harga dan ukuran tidak berdampak besar terhadap fungsionalitas LED sebagai indikator scanning fingerprint.

3.3.2.5 Keypad dan Push Button

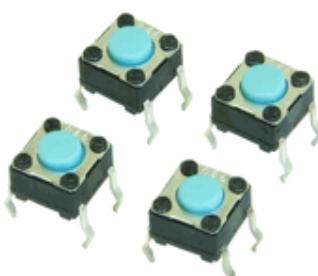
Keypad digunakan pada sistem untuk melakukan input PIN dan nominal penarikan saldo secara tunai, sedangkan Push Button digunakan untuk memilih menu mesin ATM pada saat transaksi. Alternatifnya adalah sebagai berikut

Tabel 5 Pemilihan Komponen Keypad

Spesifikasi	4x3 Keypad	4x4 Keypad
Gambar Fisik		
Tipe	Membrane Keypad	Membrane Keypad
Dimensi	70x77 mm	69x76 mm
Interface	12 keys access	16 keys access
Harga	Rp 15.000	Rp 15.000

Sistem mesin ATM membutuhkan tombol untuk clear untuk menghapus kesalahan input pengetikan saat memasukkan PIN atau nominal. Selain itu, tombol untuk cancel juga dibutuhkan untuk membatalkan transaksi. Oleh karena itu dibutuhkan tombol tambahan yang bukan hanya angka saja pada keypad. Dengan demikian, keypad 4x4 terpilih dalam sistem ini.

Tabel 6 Komponen Push-Button

Spesifikasi	Push-Button
Gambar Fisik	
Tipe	Mini Switch Push-Button
Power Rating	24 V DC
Contact Bounce	5 mS
Operating Force	2.55 N
Return Force	0.49 N
Harga	Rp 1.000

Push-button hanya digunakan untuk memilih menu transaksi saja sehingga tidak dibutuhkan alternatifnya.

3.3.2.6 Buzzer

Buzzer digunakan untuk menandakan bahwa scanning fingerprint telah berhasil dilakukan. Buzzer yang akan digunakan pada sistem adalah sebagai berikut

Tabel 7 Komponen Buzzer

Spesifikasi	Buzzer
Gambar Fisik	
Tipe	Active Buzzer
Power Rating	5 V DC
Sound	85 dB
Frekuensi Resonansi	2500 Hz
Working Temperature	-20 sampai 70 derajat Celcius
Harga	Rp 3.000

Sistem memerlukan notifikasi kepada nasabah bahwa proses tertentu telah selesai. Buzzer akan mengeluarkan suara ketika proses scanning fingerprint selesai dilakukan.

3.3.2.7 Smart Card

Smart Card digunakan untuk menyimpan ID nasabah dan data sidik jari, serta sebagai gerbang verifikasi pertama dalam melakukan transaksi mesin ATM. Smart Card yang akan digunakan berasal dari PT. Xirka. Spesifikasinya adalah sebagai berikut

Tabel 8 Komponen Smart Card

Spesifikasi	Smart Card
Gambar Fisik	
Total Size	132 Kilo Byte
ROM	32 Kilo Byte

RAM	4 Kilo Byte
CPU	16 bits
Durabilitas <i>Read/Write</i>	Minimal 100.000 kali
Daya Tahan Penyimpanan Memori	Minimal 25 Tahun

Dengan memori yang cukup besar, maka smart card ini dapat digunakan pada sistem kami untuk menyimpan data nasabah berupa nama dan ID nasabah serta beberapa data template sidik jari berupa array biner 2 dimensi.

3.3.2.7.1 Standar dimensi kartu ATM di Indonesia

Menurut badan standarisasi internasional dalam dokumen ISO (*International Organization for Standard*) 7810 (karakteristik fisik id card). Menurut ISO 7810 ada 4 ukuran yaitu:

- ID-1 : 85.60×53.98 mm (paling banyak untuk id card dan kartu bank)
- ID-2 : 105×74 mm (id card Jerman)
- ID-2 : 125×88 mm (paspor dan visa)
- ID-4 : 25×15 mm (kartu SIM untuk wilayah tertentu)

Dimensi kartu chip (smart card) ini dipilih untuk menyesuaikan dengan spesifikasi dimensi yang sesuai dengan ketentuan ISO yang berlaku.

3.3.2.8 Card Reader

Card Reader digunakan untuk membaca dan menuliskan data nasabah ke Smart Card dengan menggunakan perintah APDU. Spesifikasinya adalah sebagai berikut

9 Komponen Card Reader

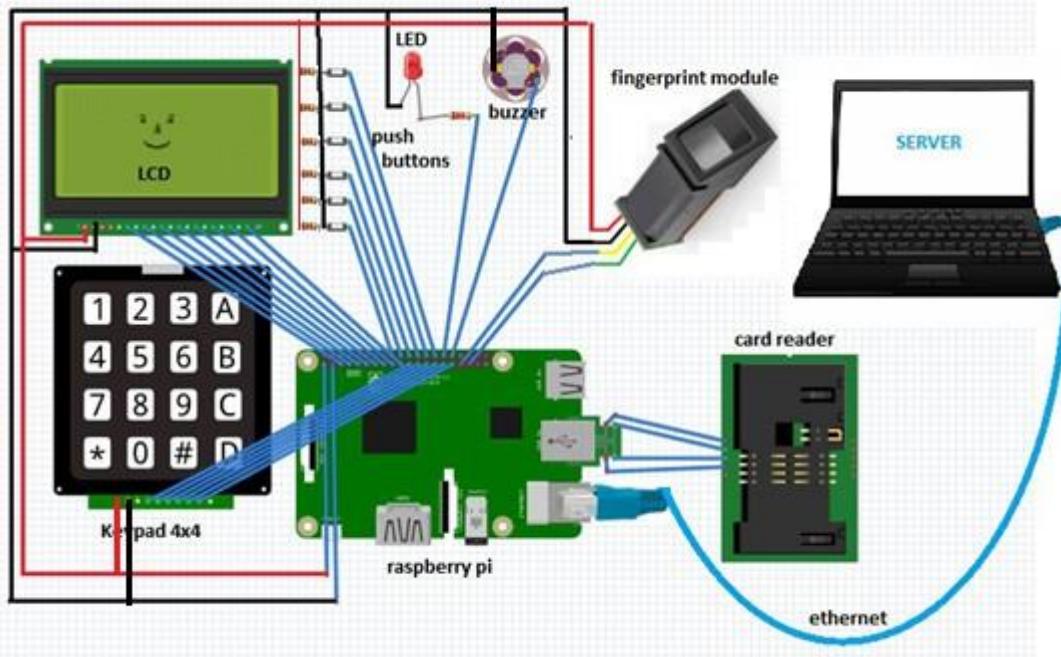
Spesifikasi	Card Reader
Gambar Fisik	
Communication	Port USB
USB Type	USB 2.0
Support OS	Windows98SE/ME/2000/XP/VISTA, Windows 7, Windows 8; MAC 10.7 and above version, Linux

Smart Card	SLE4418/4428, SLE4436/5536, 12C, Support 3V/5V IC Smart Card	SLE4432/4442,
------------	--	---------------

Card Reader yang digunakan masih bersifat *contact* dengan kartu. Data yang terbaca pada card reader akan dikirimkan ke mikrokontroler sistem untuk nantinya diverifikasi dengan data yang terdapat pada server

3.3.3 Rangkaian

Rangkaian Sistem Keamanan Mesin ATM menggunakan sidik jari adalah sebagai berikut



Gambar 49 Rangkaian Fingershield ATM

Seluruh komponen terhubung pada pusat power dari Raspberry Pi yang menggunakan sumber tegangan 5V. Rangkaian tersebut terbagi menjadi 3 mode komunikasi, yaitu komunikasi TTL, komunikasi UART, komunikasi Ethernet, dan komunikasi USB Port. Pin-pin pada LCD dan Keypad tersambung ke GPIO pada Raspberry Pi dengan menggunakan komunikasi TTL. Pin pada Fingerprint Module tersambung pada GPIO dan power-ground dengan fitur komunikasi Rx-Tx pada Raspberry Pi. Card Reader tersambung dengan menggunakan komunikasi USB Port pada Raspberry Pi. Server pada Laptop melakukan transmisi dan receive data melalui sambungan kabel Ethernet.

Push-button dan Buzzer terhubung pada GPIO Raspberry Pi. LED terhubung langsung pada power dan ground Raspberry Pi tetapi menggunakan resistor untuk membatasi arus agar tidak merusak LED.

3.4 Graphical User Interface

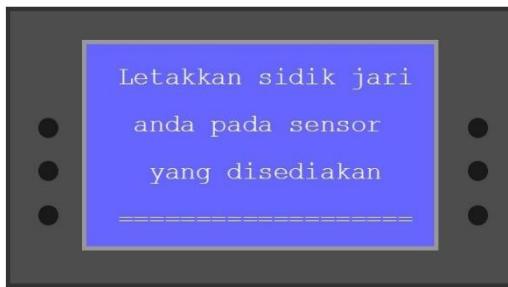
User Interface yang digunakan akan berada pada LCD 20x4 berdasarkan hasil pemilihan komponen. GUI yang akan ditampilkan pada sistem setiap statenya adalah sebagai berikut



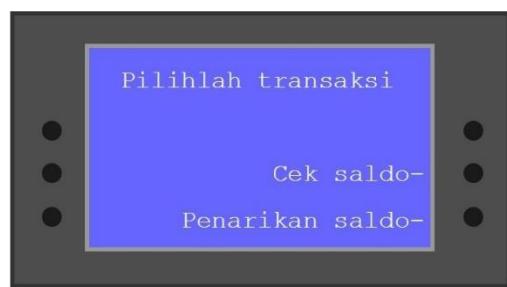
Gambar 50 GUI Idle



Gambar 51 GUI Input PIN



Gambar 52 GUI Input Sidik Jari



Gambar 53 GUI Menu Transaksi



Gambar 54 GUI Penarikan Saldo



Gambar 55 GUI Ending

Mock-up Software atau GUI di atas menggambarkan proses yang terjadi ketika melakukan transaksi menggunakan mesin ATM. Pertama-tama ketika kartu ATM belum dimasukkan maka display idle akan dimunculkan. Ketika kartu ATM telah dimasukkan, maka tampilan akan berubah menjadi Mode Verifikasi PIN yang meminta nasabah memasukkan PIN. Jika nasabah memasukkan PIN yang salah, maka display ini akan terus muncul. Setelah berhasil, Mode Verifikasi Sidik Jari akan muncul yang meminta nasabah melakukan scan sidik jari yang telah terdaftar. Jika terverifikasi dengan benar, display akan berganti menjadi menu utama transaksi yang dapat dipilih. Jika nasabah memilih penarikan saldo, maka display akan memunculkan jumlah yang ingin ditarik serta input nominal yang telah diberikan. Jika nasabah memilih cek saldo, maka display akan langsung memunculkan sisa saldo dari server. Terakhir, setelah transaksi selesai, display akan berubah menjadi transaksi lain yang masih ingin dilakukan. Jika jawaban tidak, maka display akan kembali ke mode idle.

3.5 Simulasi

3.5.1 Algoritma Fingerprint

Untuk menguji fungsionalitas dan akurasi metode yang digunakan untuk pencocokan sidik jari, dilakukan sebuah simulasi menggunakan software MATLAB dengan input database sidik jari dan output matching score yang dihasilkan. Hasil yang ditunjukkan adalah sebagai berikut



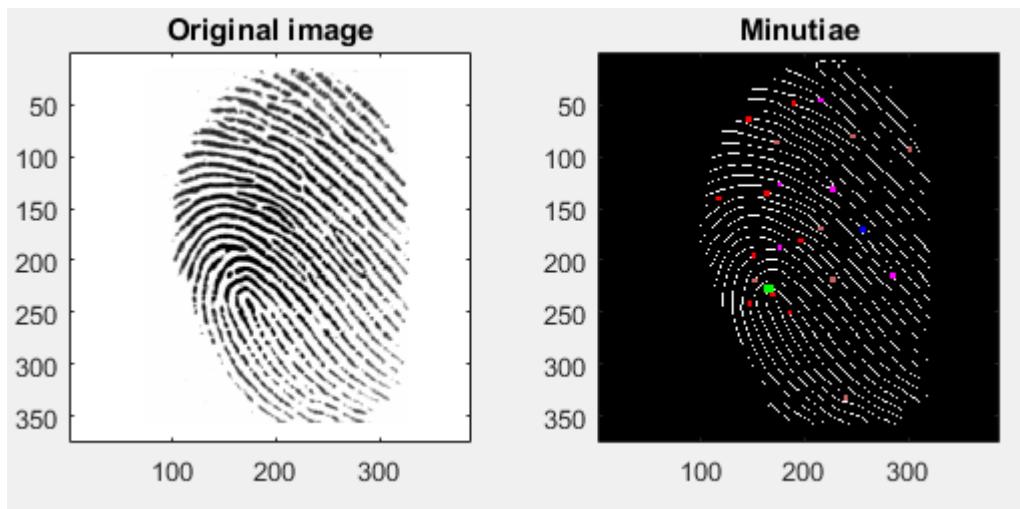
Gambar 56 Input Sidik Jari A (kiri), Input Sidik Jari B (tengah) dan Input Sidik Jari C (kanan)

Pada simulasi ini digunakan 3 buah *sample* input sidik jari dengan menggunakan database FVC2002 untuk menguji fungsionalitas algoritma. Sidik jari A dan sidik jari B dalam hal ini merupakan sidik jari dari orang yang sama, sedangkan sidik jari C merupakan sidik jari dari orang yang berbeda.



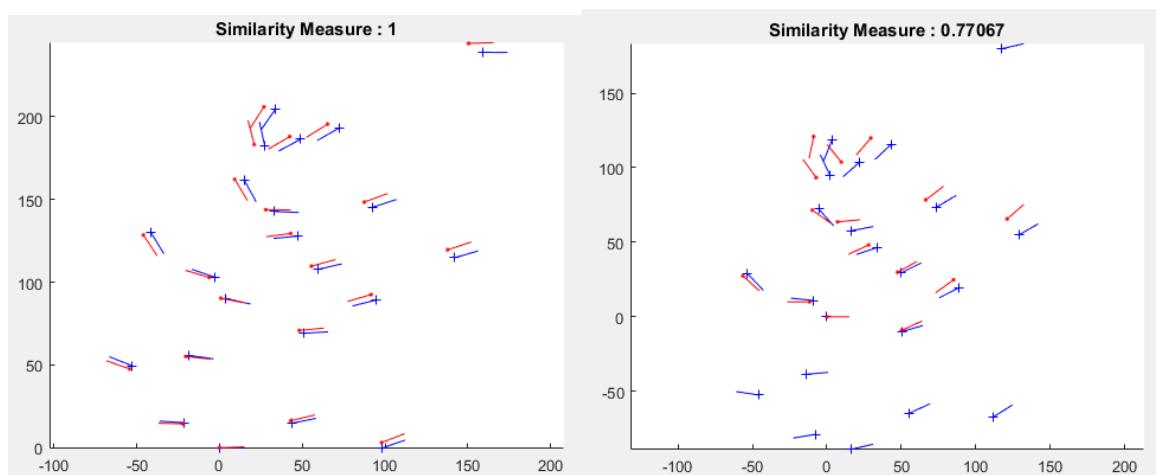
Gambar 57 Hasil Binerisasi Sidik Jari A (kiri) dan Hasil Thinning Sidik Jari A (kanan)

Sebelum dilakukan pemrosesan ekstraksi fitur *minutiae* dari sidik jari, dilakukan *image preprocessing* berupa operasi binerisasi dan morphologi atau *thinning* terlebih dahulu pada setiap sidik jari dan pembandingnya untuk agar fitur minutiae seperti *ridge ending* dan *bifurcation* dapat dengan mudah diidentifikasi.

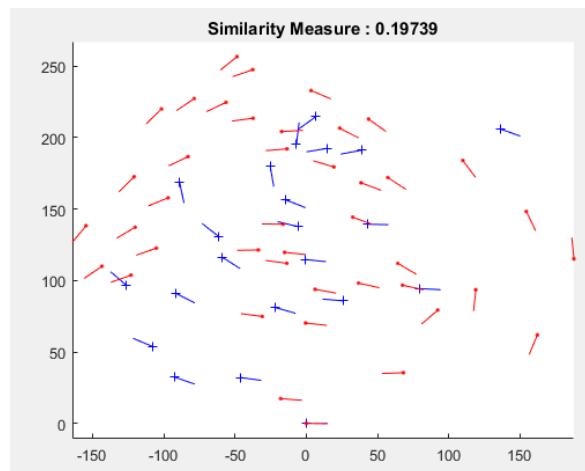


Gambar 58 Hasil Minutiae Sidik Jari A

Proses ekstraksi minutiae terjadi di semua sidik jari lalu letak minutiae ini nantinya akan dibandingkan untuk verifikasi. Untuk melakukan ekstraksi *minutiae*, dibutuhkan referensi karakteristik dan bentuk dari setiap jenisnya. Titik-titik di atas merupakan titik dimana *minutiae* terletak. Perbedaan warna menunjukkan perbedaan kelompok karakteristik *minutiae*



Gambar 59 Hasil Minutiae Matching Sidik Jari A dengan Sidik Jari A (kiri) dan Sidik Jari B (kanan)

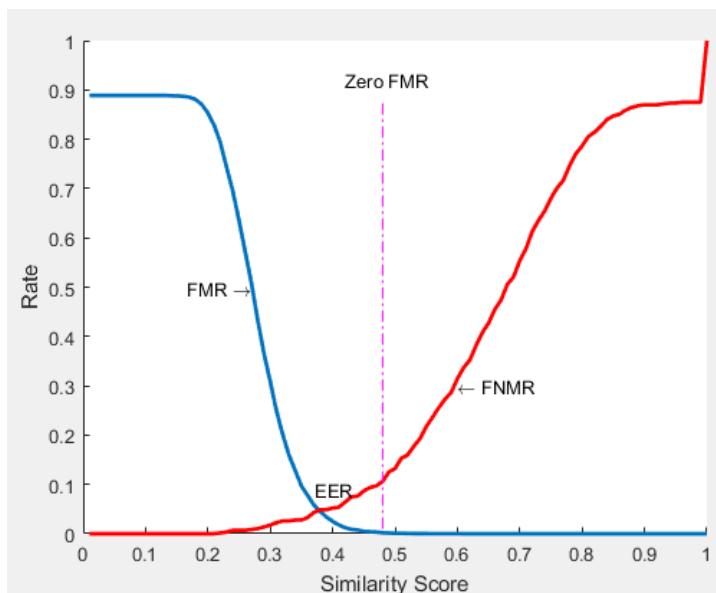


Gambar 60 Hasil Minutiae Matching Sidik Jari A dengan Sidik Jari C

Proses *matching* sidik jari ditentukan oleh jarak fitur *minutiae* uji coba dengan jarak fitur *minutiae* referensi yang disebut dengan *Euclidean Distance*. Hasil *matching* sidik jari A dengan sidik jari A tentunya menghasilkan tingkat kemiripan 100% karena merupakan sidik jari yang sama persis posisi dan ketidakpastian lainnya. Hasil *matching* sidik jari A dengan sidik jari B menghasilkan tingkat kemiripan 77% walaupun itu merupakan sidik jari yang sama dengan orang yang sama. Hal ini disebabkan oleh perbedaan posisi atau orientasi pada saat *scanning* sidik jari yang dapat mengakibatkan akurasi yang berkurang. Namun, tingkat kemiripan 77% masih cukup baik dan dapat tergolong sidik jari orang yang sama karena jarak fitur *minutiae* sidik jari B terhadap fitur *minutiae* sidik jari A tidak terlalu jauh.

Berbeda dengan hasil *matching* sidik jari A dengan sidik jari C. Kedua sidik jari tersebut berasal dari orang yang berbeda sehingga menghasilkan tingkat kemiripan yang jauh, yaitu sekitar 19,7%. Hal ini disebabkan oleh jarak fitur *minutiae* sidik jari C terhadap fitur *minutiae* sidik jari A sangat jauh dan bentuknya berbeda-beda. Dengan demikian, sidik jari tidak bisa dianggap sama dan ditolak.

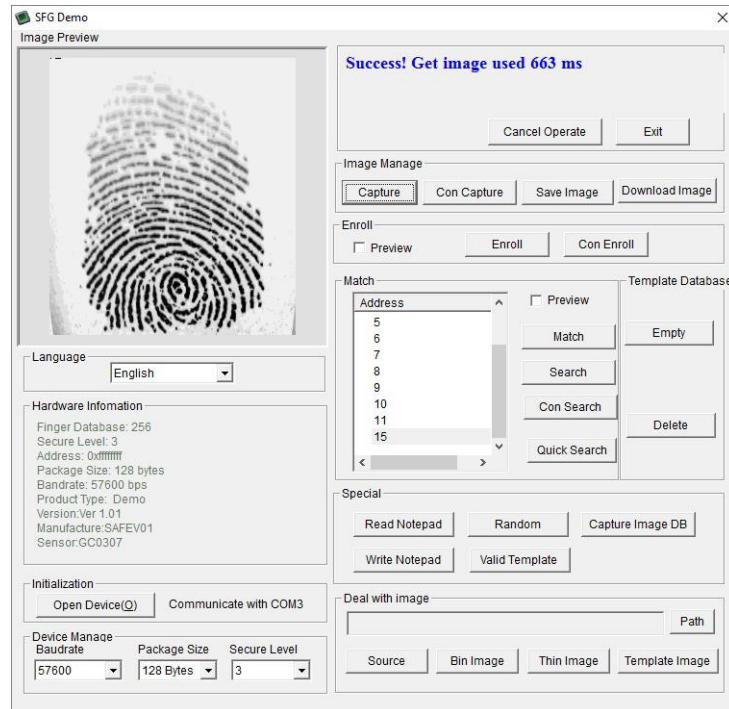
Threshold untuk menyatakan sidik jari tersebut dikatakan cocok/sesuai atau tidak cocok/ditolak dapat dicari dengan menggunakan grafik FMR dan FNMR sebagai berikut



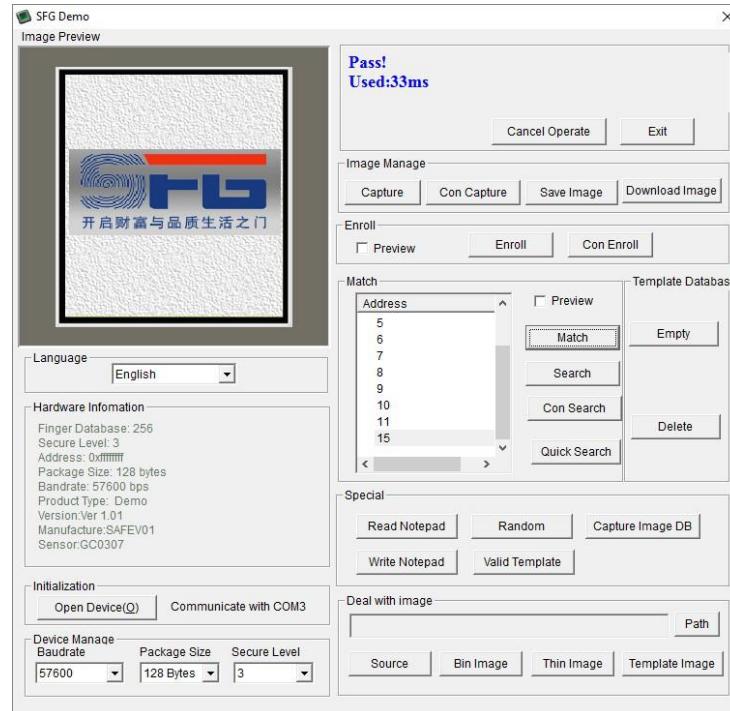
Gambar 61 Grafik FMR, FNMR, dan EER

Grafik tersebut menunjukkan FMR (*False Matching Rate*) dan FNMR (*False Non Matching Rate*). FMR adalah tingkat kesalahan sidik jari dalam mengatakan bahwa kedua sidik jari tersebut cocok yang padahal seharusnya tidak cocok, sedangkan FNMR adalah tingkat kesalahan sidik jari dalam mengatakan bahwa kedua sidik jari tersebut tidak cocok yang padahal seharusnya cocok. Kedua grafik tersebut suatu saat akan menghasilkan nilai yang sama. Inilah yang disebut EER (*Equal Error Rate*). Nilai yang ditunjukkan pada EER inilah yang merupakan nilai *threshold* optimum dalam penentuan kecocokan sidik jari. Dalam hal ini nilai *threshold* optimum pada saat EER adalah sekitar 0.39. Dengan demikian, pada simulasi ini jika tingkat kemiripan di atas *threshold* atau 0.39 atau diatas 39%, sidik jari sudah dapat dikatakan sesuai atau cocok atau mirip, tetapi jika tingkat kemiripan di bawah *threshold* atau 0.39 atau diatas 39%, sidik jari sudah dapat dikatakan tidak sesuai atau tidak cocok atau tidak mirip. Nilai *threshold* ini dapat diatur sesuai dengan keinginan sistem yang akan dibuat nantinya

Untuk menguji kecepatan proses *scanning* dan pencocokan dari modul sidik jari yang kami gunakan, dibutuhkan software *SFG Demo*



Gambar 62 Kecepatan Scanning Sidik Jari



Gambar 63 Kecepatan Verifikasi Sidik Jari 1:1

Dari kedua hasil simulasi tersebut, dapat terlihat proses scanning yang terjadi hanya memakan waktu 0.6 s yang mana kurang dari 1 detik. Proses pencocokan bahkan hanya memakan waktu 33 ms saja karena pencocokan atau verifikasi yang dilakukan hanya 1:1 sidik jari saja. Dengan demikian, hal ini sudah cukup membuktikan bahwa kecepatan proses scanning dan verifikasi sidik jari sistem yang akan kami buat cukup cepat untuk nasabah merasa nyaman.

4 Lampiran

Source Code

main_single.m

```
clear all; clc; addpath(genpath(pwd));

%% EXTRACT FEATURES FROM AN ARBITRARY FINGERPRINT
filename='101_1.tif';
img = imread(filename);

%BINERIZATION
J=img(:,:,1)>160;
figure, imshow(J)
set(gcf,'position',[1 1 600 600]);

%THINNING
K=bwmorph(~J,'thin','inf');
figure, imshow(~K)
set(gcf,'position',[1 1 600 600]);

if ndims(img) == 3; img = rgb2gray(img); end % Color Images
disp(['Extracting features from ' filename ' ...']);
ffnew=ext_finger(img,1);

%% GET FEATURES OF AN ARBITRARY FINGERPRINT FROM THE TEMPLATE AND
MATCH IT WITH FIRST ONE
load('db.mat'); i=1;
second=['10' num2str(fix((i-1)/8)+1) ' ' num2str(mod(i-1,8)+1)];
disp(['Computing similarity between ' filename ' and ' second ' from
FVC2002']);
S=match(ffnew,ff{i},1);
```

main_calc_fmr.m

```
clear all; clc; addpath(genpath(pwd));

%% BUILDING FMR AND FNMR, THIS WILL TAKE ABOUT 2 HOURS
% build_fmr

%% PLOT FMR & FNMR
load('fmr.mat'); load('fnmr.mat');
figure, hold on;

afmr=mean(fmr,2);
plot(0.01:.01:1,afmr,'LineWidth',2);
text(0.60,0.3,'<-- FNMR','HorizontalAlignment','left');

afnmr=mean(fnmr,2);
plot(0.01:.01:1,afnmr,'r','LineWidth',2);
text(0.27,0.5,'FMR -->','HorizontalAlignment','right');

plot([0.48 0.48],[0.01 0.88],'-.');
text(0.42,0.92,'Zero FMR');

text(0.37,0.09,'EER');
xlabel('Similarity Score'); ylabel('Rate');
```

main_total.m

```
clear all; clc; addpath(genpath(pwd));
%% BUILD FINGERPRINT TEMPLATE DATABASE
% build_db(9,8);           %THIS WILL TAKE ABOUT 30 MINUTES
load('db.mat');

%% EXTRACT FEATURES FROM AN ARBITRARY FINGERPRINT
filename='101_1.tif';
img = imread(filename);
if ndims(img) == 3; img = rgb2gray(img); end % Color Images
disp(['Extracting features from ' filename ' ...']);
ffnew=ext_finger(img,1);

%% FOR EACH FINGERPRINT TEMPLATE, CALCULATE MATCHING SCORE IN
%% COMPARISION WITH FIRST ONE
S=zeros(72,1);
for i=1:72
    second=['10' num2str(fix((i-1)/8)+1) '_' num2str(mod(i-1,8)+1)];
    fprintf(['Computing similarity between ' filename ' and ' second ' from FVC2002 : ']);
    S(i)=match(ffnew,ff{i});
    fprintf([num2str(S(i)) '\n']);
    drawnow
end
%% OFFER MATCHED FINGERPRINTS
Matched_FingerPrints=find(S>0.48)
```

match.m

```
% FINGERPRINT MATCHING SCORE
%
% Usage: [ S ] = match( M1, M2, display_flag );
%
% Argument: M1 - First Minutiae
%            M2 - Second Minutiae
%            display_flag
%
% Returns: S - Similarity Measure

function [ S ] = match( M1, M2, display_flag )
    if nargin==2; display_flag=0; end
    M1=M1(M1(:,3)<5,:);
    M2=M2(M2(:,3)<5,:);
    count1=size(M1,1); count2=size(M2,1);
    bi=0; bj=0; ba=0; % Best i,j,alpha
    S=0; % Best Similarity Score
    for i=1:count1
        T1=transform(M1,i);
        for j=1:count2
            if M1(i,3)==M2(j,3)
                T2=transform(M2,j);
                for a=-5:5 %Alpha
                    T3=transform2(T2,a*pi/180);
                    sm=score(T1,T3);
                    if S<sm
                        S=sm;
                        bi=i; bj=j; ba=a;
                    end
                end
            end
        end
    end
```

```

        end
    end
end
if display_flag==1
    figure, title(['Similarity Measure : ' num2str(S)]);
T1=transform(M1,bi);
T2=transform(M2,bj);
T3=transform2(T2,ba*pi/180);
plot_data(T1,1);
plot_data(T3,2);
end
end

```

score.m

```

% TRANSFORMED MINUTIAE MATCHING SCORE
%
% Usage: [ si ] = score( T1, T2 );
%
% Argument: T1 - First Transformed Minutiae
%             T2 - Second Transformed Minutiae
%             d
% Returns: sm - Similarity Measure

function [ sm ] = score( T1, T2 )
Count1=size(T1,1); Count2=size(T2,1); n=0;
T=15; %Threshold for distance
TT=14; %Threshold for theta
for i=1:Count1
    Found=0; j=1;
    while (Found==0) && (j<=Count2)
        dx=(T1(i,1)-T2(j,1));
        dy=(T1(i,2)-T2(j,2));
        d=sqrt(dx^2+dy^2); %Euclidean Distance between T1(i) &
T2(i)
        if d<T
            DTheta=abs(T1(i,3)-T2(j,3))*180/pi;
            DTheta=min(DTheta,360-DTheta);
            if DTheta<TT
                n=n+1; %Increase Score
                Found=1;
            end
        end
        j=j+1;
    end
    sm=sqrt(n^2/(Count1*Count2)); %Similarity Index
end

```

plot_data.m

```

% PLOT DATA
%
% Usage: plot_data( X,y );
%
% Argument: X - Data Points
%             y - Plot Style (1 for blue, 2 for red, ...)

```

```

% Vahid. K. Alilou
% Department of Computer Engineering
% The University of Semnan
%
% July 2013

function plot_data( X,y )
N=size(X,1); r=15;
hold on; axis equal;
pale={'b+' 'r.' 'g.' 'y.' 'm.' 'c.'};
color={'b' 'r' 'g' 'y' 'm' 'c'};
for i=1:N
    plot(X(i,1),X(i,2),pale{y});
    MyX=[X(i,1) X(i,1)+r*cos(X(i,3))];
    MyY=[X(i,2) X(i,2)+r*sin(X(i,3))];
    plot(MyX,MyY,color{y});
end
hold off;
end

```

ext_finger.m

```

% EXTRACTING FEATURE FROM A FINGERPRINT IMAGE
%
% Usage: [ ret ] = ext_finger( img, display_flag );
%
% Argument:   img - FingerPrint Image
%             display_flag
%
% Returns:     ret - Minutiae

function [ ret ] = ext_finger( img, display_flag )
if nargin==1; display_flag=0; end
block_size_c = 24; YA=0; YB=0; XA=0; XB=0;
% Enhancement -----
-----
if display_flag==1; fprintf(' >> enhancement '); end
yt=1; xl=1; yb=size(img,2); xr=size(img,1);
for x=1:55
    if numel(find(img(x,:)<200)) < 8
        img(1:x,:) = 255;
        yt=x;
    end
end
for x=225:size(img,1)
    if numel(find(img(x,:)<200)) < 3
        img(x-17:size(img,1),:) = 255;
        yb=x;
        break
    end
end
for y=200:size(img,2)
    if numel(find(img(:,y)<200)) < 1
        img(:,y:size(img,2)) = 255;
        xr=y;
        break
    end
end
end

```

```

for y=1:75
    if numel(find(img(:,y)<200)) < 1
        img(:,1:y) = 255;
        xl=y;
    end
end
[ binim, mask, cimg, cimg2, orient_img, orient_img_m ] =
f_enhance(img);
% Making Mask -----
-----
if display_flag==1; fprintf('done.\n >>> making mask '); end
mask_t=mask;
for y=19:size(mask,1)-block_size_c*2
    for x=block_size_c:size(mask,2)-block_size_c*2
        n_mask = 0;
        for yy=-1:1
            for xx=-1:1
                y_t = y + yy *block_size_c;
                x_t = x + xx *block_size_c;
                if y_t > 0 && x_t > 0 && (y_t ~= y || x_t ~= x) &&
mask(y_t,x_t) == 0
                    n_mask = n_mask + 1;
                end
            end
        end
        if n_mask == 0
            continue
        end
        if mask(y,x) == 0 || y > size(mask,1) - 20 || y < yt || y
> yb || x < xl || x > xr
            cimg2(ceil(y/(block_size_c)), ceil(x/(block_size_c))) =
255;
            mask_t(y,x) = 0;
            continue;
        end
        for i = y:y+1
            for j = x-9:x+9
                if i > 0 && j > 0 && i < size(mask,1) && j <
size(mask,2) && mask(i,j) > 0
                else
                    cimg2(ceil(y/(block_size_c)), ceil(x/(block_size_c))) =
255;
                    mask_t(y,x)=0;
                    break
                end
            end
        end
    end
end
end
end
mask=mask_t;
inv_binim = (binim == 0);
thinned = bwmorph(inv_binim, 'thin',Inf);
mask_t=mask;
if numel(find(mask(125:150,150:250)>0)) > 0 &&
numel(find(mask(250:275,150:250)>0)) > 0
    mask(150:250,150:250)=1;
end
method=-1; core_y = 0; core_x = 0; core_val=0; lc=0;
o_img=sin(orient_img); o_img(mask == 0) = 1;

lower_t=0.1;

```

```

[v,y]=min(cimg);
[dt1,x]=min(v);
delta1_y=y(x)*block_size_c/2; delta1_x=x*block_size_c/2;

v(x)=255; v(x+1)=255;
[dt2,x]=min(v);
delta2_y=y(x)*block_size_c/2; delta2_x=x*block_size_c/2;

v(x)=255; v(x+1)=255;
[dt3,x]=min(v);
delta3_y=y(x)*block_size_c/2; delta3_x=x*block_size_c/2;

db=60;
if dt1 < 1 && delta1_y+db < core_y && delta1_y > 15 || dt2 < 1 &&
delta2_y+db < core_y && delta2_y > 15 || dt3 < 1 && delta3_y+db <
core_y && delta3_y > 15
    core_val=255;
end
for y=10:size(o_img,1)-10
    for x=10:size(o_img,2)-10
        s1=0; t=10; %few of bad cores here
        if y < 50 && x > 250
            t=11;
        end
        if y > 38
            yt=20;
        else
            yt=5;
        end
        if lc > 0.41 && (core_y + 60 < y)
            break;
        end
        if mask(y,x)==0 || mask(max(y-t,1),x)==0 ||
mask(y,min(x+t, size(o_img,2)))==0 || mask(y,max(x-t,1))==0 ||
mask(max(y-t,1),min(x+t,size(o_img,2)))==0 || mask(max(y-t,1),max(x-
t,1))==0 || o_img(y,x) < lc || o_img(y,x) < 0.1
            continue
        end
        if dt1 < 1 && delta1_y+db < y && delta1_y > 15 || dt2 < 1
&& delta2_y+db < y && delta2_y > 15 || dt3 < 1 && delta3_y+db < y
&& delta3_y > 15
            continue
        end
        test_m=min(o_img(1:y-yt,max((x-
10),1):min(x+10,size(o_img,2)) ));
        if numel(test_m)>0 && min(test_m) >= 0.17
            continue
        end
        for a=y:y+2
            for b=x:x+1
                s1=s1+o_img(a,b);
            end
        end
        s1=s1/6; s2=[]; i=1;
        for a=y-3:y-1
            for b=x:x+1
                s2(i)=o_img(a,b);
                i=i+1;
            end
        end
    end

```

```

        if min(s2) < lower_t
            s2=sum(s2)/6;
        else
            s2=s1;
        end
        s3=[]; i=1;
        for a=y:y+2
            for b=x+2:x+3
                s3(i)=o_img(a,b);
                i=i+1;
            end
        end
        if min(s3) < lower_t
            s3=sum(s3)/6;
        else
            s3=s1;
        end
        s4=[]; i=1;
        for a=y:y+2
            for b=x-2:x-1
                s4(i)=o_img(a,b);
                i=i+1;
            end
        end
        if min(s4) < lower_t
            s4=sum(s4)/6;
        else
            s4=s1;
        end
        s5=[];
        i=1;
        for a=y-3:y-1
            for b=x-2:x-1
                s5(i)=o_img(a,b);
                i=i+1;
            end
        end
        if min(s5) < lower_t
            s5=sum(s5)/6;
        else
            s5=s1;
        end
        s6=[];
        i=1;
        for a=y-3:y-1
            for b=x+2:x+3
                s6(i)=o_img(a,b);
                i=i+1;
            end
        end
        if min(s6) < lower_t
            s6=sum(s6)/6;
        else
            s6=s1;
        end
        if s1-s2 > core_val
            core_val=s1-s2;
            core_x=x;
            core_y=y;
            lc=o_img(y,x);
            method=1;
        end
    end

```

```

        if s1-s3 > core_val
            core_val=s1-s3;
            core_x=x;
            core_y=y;
            lc=o_img(y,x);
            method=2;
        end
        if x < 300 && s1-s4 > core_val
            core_val=s1-s4;
            core_x=x;
            core_y=y;
            lc=o_img(y,x);
            method=3;
        end
        if x < 300 && s1-s5 > core_val
            core_val=s1-s5;
            core_x=x;
            core_y=y;
            lc=o_img(y,x);
            method=4;
        end
        if s1-s6 > core_val
            core_val=s1-s6;
            core_x=x;
            core_y=y;
            lc=o_img(y,x);
            method=5;
        end
    end
end
if core_y > 37
    yt=20;
else
    yt=5;
end
test_smooth = 100;
if core_y > 0
    test_smooth= sum(sum(o_img(core_y-yt-5:core_y-yt+5,core_x-
5:core_x+5)));
end
if lc > 0.41 && (test_smooth < 109.5 && method~=2 || test_smooth <
100) %&& min(min(o_img(1:core_y-yt,core_x-10:core_x+10))) < 0.17
    start_t=0;
    core_val=1/(core_val+1);
else
    core_x=0;
    core_y=0;
    core_val = 255;
end
mask=mask_t; path_len = 45;

% Finding Minutiae -----
if display_flag==1; fprintf('done.\n >> finding minutiae '); end
minu_count = 1;
minutiae(minu_count, :) = [0,0,0,0,0,1];
min_path_index = [];
% loop through image and find minutiae, ignore certain pixels for
border
for y=20:size(img,1)-14
    for x=21:size(img,2)-21

```

```

if (thinned(y, x) == 1) % only continue if pixel is white
    % calculate CN from Raymond Thai
    CN = 0; sx=0; sy=0;
    for i = 1:8
        t1 = p(thinned, x, y, i);
        t2 = p(thinned, x, y, i+1);
        CN = CN + abs (t1-t2);
    end
    CN = CN / 2;
    if ((CN == 1) || (CN == 3)) %&& mask(y,x) > 0
        skip=0;
        for i = y-5:y+5
            for j = x-5:x+5
                if i>0 && j>0 && mask(i,j) == 0
                    skip=1;
                end
            end
        end
        if skip == 1
            continue;
        end
        t_a=[];
        c = 0;
        for e=y-1:y+1
            for f=x-1:x+1
                c = c + 1;
                t_a(c) = orient_img_m(e,f);
            end
        end
        m_o = median(t_a); m_f = 0;
        if CN == 3
            [CN, prog, sx, sy,ang]=test_bifurcation(thinned,
x,y, m_o, core_x, core_y);
            if prog < 3
                continue
            end
            if ang < pi
                m_o = mod(m_o+pi,2*pi);
            end
        else
            progress=0;
            xx=x; yy=y; pao=-1; pos=0;
            while progress < 15 && xx > 1 && yy > 1 &&
yy<size(img,1) && xx<size(img,2) && pos > -1
                pos=-1;
                for g = 1:8
                    [ta, xa, ya] = p(thinned, xx, yy, g);
                    [tb, xb, yb] = p(thinned, xx, yy,
g+1);
                    if (ta > tb) && pos== -1 && g ~= pao
                        pos=ta;
                        if g < 5
                            pao = 4 + g;
                        else
                            pao = mod(4 + g, 9) + 1;
                        end
                        xx=xa; yy=ya;
                    end
                end
                progress=progress+1;
            end

```

```

        if progress < 10
            continue
        end
        if mod(atan2(y-yy,xx-x), 2*pi) > pi
            m_o=m_o+pi;
        end
    end
    minutiae(minu_count, :) = [ x, y, CN, m_o, m_f, 1];
    min_path_index(minu_count, :) = [sx sy];
    minu_count = minu_count + 1;
end
end % if pixel white
end % for y
end % for x

% Filtering False Minutiae -----
-----
if display_flag==1; fprintf('done.\n >> filtering false minutiae
'); end
minu_count = minu_count -1;
t_minutiae = [];
t_minu_count = 1;
t_mpi = [];
for i=1:minu_count
    X = minutiae(i,1); Y = minutiae(i,2);
    rc=0;
    for y=max(Y-2,1):min(Y+2, size(binim,1))
        if rc > 0
            break
        end
        for x=max(X-2,1):min(X+2, size(binim,2))
            if mask(y,x) == 0
                rc = rc + 1;
                break
            end
        end
    end
    if rc > 0
        continue;
    else
        t_minutiae(t_minu_count, :) = minutiae(i, :);
        t_mpi(t_minu_count, :) = min_path_index(i, :);
        t_minu_count = t_minu_count + 1;
    end
end
minutiae = t_minutiae;
min_path_index = t_mpi;
minu_count = size(minutiae,1);
t_minu_count = 1; t_minutiae = [];
dist_m = dist2(minutiae(:,1:2), minutiae(:,1:2));
dist_test=49;
for i=1:minu_count
    reject_flag = 0;
    P_x = minutiae(i,1); P_y = minutiae(i,2);
    for j = i + 1 : minu_count
        if dist_m(i,j) <= dist_test
            reject_flag = 1;
        end
    end
    if reject_flag == 0 && mask(P_y, P_x) > 0
        reverse_p = 0;
    end
end

```

```

if min_path_index(i,1) == 0
    x = P_x;
    y = P_y;
else
    x = min_path_index(i,1);
    y = min_path_index(i,2);
end
p1x=P_x; p1y=P_y;
x1=x; y1=y;
iter = 0;
for m=1:path_len
    iter = iter + 1;
    cn = 0;
    for ii = 1:8
        t1 = p(thinned, x1, y1, ii);
        t2 = p(thinned, x1, y1, ii+1);
        cn = cn + abs (t1-t2);
    end
    cn = cn / 2;
    if cn ~= 3 && cn ~= 4 || m == 1
        for n=1:8
            if reverse_p == 0 || iter > 1
                [ta, xa, ya] = p(thinned, x1, y1, n);
            else
                [ta, xa, ya] = p(thinned, x1, y1, 9-n);
            end
            if ta == 1 && (xa ~= p1x || ya ~= p1y) && (xa ~= x || ya ~= y)
                p1x = x1; p1y = y1;
                x1 = xa; y1 = ya;
                break;
            end
        end
    end
end
t_minutiae(t_minu_count, :) = minutiae(i, :);
t_minu_count = t_minu_count + 1;
end
minutiae = t_minutiae;
minu_count = t_minu_count-1;
tmpvec1 = size(img,1).*ones(minu_count,1);
tmpvec2 = ones(minu_count,1);
minutiae_for_sc = [minutiae(:,1)/size(img,2) (tmpvec1 -
minutiae(:,2) + tmpvec2)/size(img,1)];
dist_m = sqrt(dist2(minutiae_for_sc(:,1:2),
minutiae_for_sc(:,1:2)));
for i=1:minu_count
    [d,ind] = sort(dist_m(i,:));
    for j = 1 : minu_count
        if dist_m(i,ind(j)) == 0
            continue
        end
        theta_t = mod(atan2(minutiae(i,2) - minutiae(ind(j),2),
minutiae(i,1) - minutiae(ind(j),1)), 2*pi);
        ridge_count = 0;
        p_y = minutiae(i,2); p_x = minutiae(i,1);
        t_x = 0; t_y = 0;
        current=1; radius = 1;
        while p_y ~= minutiae(ind(j),2)

```

```

        if thinned(p_y, p_x) > 0 && current == 0 && (t_x ~= p_x
|| t_y ~= p_y)
            current = 1;
            ridge_count = ridge_count + 1;
        else
            if thinned(p_y, p_x) == 0
                current = 0;
            end
        end
        t_x = p_x; t_y = p_y;
        p_x = round(minutiae(i,1) - radius*cos(theta_t));
        p_y = round(minutiae(i,2) - radius*sin(theta_t));
        radius = radius + 1;
    end
end
if core_val < 1
    minutiae(minu_count+1, :) = [core_x, core_y, 5, start_t, 0,1];
    minu_count = minu_count + 1;
end
if dt1 < 1
    minutiae(minu_count+1, :) = [delta1_x, delta1_y, 7, 0, 1,1];
    minu_count = minu_count + 1;
end
if dt2 < 1
    minutiae(minu_count+1, :) = [delta2_x, delta2_y, 7, 0, 1,1];
    minu_count = minu_count + 1;
end
if dt3 < 1
    minutiae(minu_count+1, :) = [delta3_x, delta3_y, 7, 0, 1,1];
    minu_count = minu_count + 1;
end

% Return Minutiae -----
-----
if display_flag == 1
    fprintf('done.\n');
    minutiae_img = uint8(zeros(size(img, 1),size(img, 2), 3));
    for i=1:minu_count
        x1 = minutiae(i, 1); y1 = minutiae(i, 2);
        if minutiae(i, 3) == 1 %Termination
            if minutiae(i, 4) > pi
                for k = y1-2: y1 + 2
                    for l = x1-2: x1 + 2
                        minutiae_img(k, l,:) = [255, 0, 0];
                    end
                end
            else
                for k = y1-2: y1 + 2
                    for l = x1-2: x1 + 2
                        minutiae_img(k, l,:) = [205, 100, 100];
                    end
                end
            end
        elseif minutiae(i, 3) == 2
            for k = y1-2: y1 + 2
                for l = x1-2: x1 + 2
                    minutiae_img(k, l,:) = [255, 0, 255];
                end
            end
        elseif minutiae(i, 3) == 3 %Bifurcation

```

```

        if minutiae(i, 4) > pi
            for k = y1-2: y1 + 2
                for l = x1-2: x1 + 2
                    minutiae_img(k, l,:) = [0, 0, 255];
                end
            end
        else
            for k = y1-2: y1 + 2
                for l = x1-2: x1 + 2
                    minutiae_img(k, l,:) = [255, 0, 255];
                end
            end
        end
    elseif minutiae(i, 3) == 5
        for k = y1-4: y1 + 4
            for l = x1-4: x1 + 4
                minutiae_img(k, l,:) = [0, 255, 0];
            end
        end
    elseif minutiae(i, 3) > 5
        for k = y1-2: y1 + 2
            for l = x1-2: x1 + 2
                minutiae_img(k, l,:) = [128, 128, 0]; % gold for
delta
            end
        end
    end
combined = uint8(minutiae_img);
for x=1:size(binim,2)
for y=1:size(binim,1)
    if mask(y,x) == 0
        combined(y,x,:)= [0,0,0];
        continue
    end
    if (thinned(y,x)) % binim(y,x)
        combined(y,x,:)= [255,255,255];
    else
        combined(y,x,:)= [0,0,0];
    end % end if
    if ((minutiae_img(y,x,3) ~= 0) || (minutiae_img(y,x,1) ~=
0) ) || (minutiae_img(y,x,2) ~= 0)
        combined(y,x,:)= minutiae_img(y,x,:);
    end
end % end for y
end % end for x
if core_val < 1 && YA > 0
    for k = YA-2: YA + 2
        for l = XA-2: XA + 2
            combined(k,l,:)= [20, 255, 250];
        end
    end
    for k = YB-2: YB + 2
        for l = XB-2: XB + 2
            combined(k,l,:)= [20, 255, 250];
        end
    end
end
subplot(1,2,1), subimage(img), title('Original image')
subplot(1,2,2), subimage(combined), title('Minutiae')
end

```

```
    ret=minutiae;  
end
```