RANCANG BANGUN KEAMANAN SISTEM INFORMASI DENGAN AUTHENTIFIKASI MENGGUNAKAN IDENTIFIKASI ONE TIME PASSWORD BERBASIS SMS DENGAN HASH MD5

Disusun dan Diajukan Untuk Memenuhi Persyaratan Ujian Akhir Memperoleh Gelar Sarjana Komputer Pada Fakultas Sains dan Teknologi
Universitas Pembangunan Panca Budi
Medan

SKRIPSI

OLEH :

NAMA	: RIZKY RAHMANSYAH
N.P.M	: 1514370012
PROGRAM STUDI	: SISTEM KOMPUTER

FAKULTAS SAINS DAN TEKNOLOGI
UNIVERSITAS PEMBANGUNAN PANCA BUDI
MEDAN
2019

RANCANG BANGUN KEAMANAN SISTEM INFORMASI DENGAN AUTHENTIFIKASI MENGGUNAKAN IDENTIFIKASI ONE TIME PASSWORD BERBASIS SMS DENGAN HASH MD5

Disusun Oleh :

NAMA	**: RIZKY RAHMANSYAH**
N.P.M	**: 1514370012**
PROGRAM STUDI	**: SISTEM KOMPUTER**

Skripsi telah disetujui oleh Dosen Pembimbing Skripsi

pada tanggal : 06 November 2019

Dosen Pembimbing I	Dosen Pembimbing II
Akhyar Lubis, S.Kom., M.Kom	**Supina Batubara, S.Kom., M.Kom**

Mengetahui,

Dekan Fakultas Sains dan Teknologi	Ketua Program Studi
Siti Shindi Indira, S.T., M.Sc	**Eko Hariyanto, S.Kom., M.Kom**

SURAT PERNYATAAN

Saya yang bertanda tangan di bawah ini :

Nama	: Rizky Rahmansyah
NPM	: 1514370012
Prodi	: Sistem Komputer
Konsentrasi	: Keamanan Jaringan Komputer
Judul Skripsi	: Rancang Bangun Keamanan Sistem Informasi Dengan Authentifikasi Menggunakan Identifikasi One Time Password Berbasis SMS dengan Hash MD5

Dengan ini menyatakan bahwa :

1. Tugas Akhir/Skripsi saya bukan hasil Plagiat
2. Sayat tidak akan menuntut perbaikan nilai indeks Prestasi Kumulatif (IPK) setelah ujian Sidang Meja Hijau
3. Skripsi saya dapat dipublikasikan oleh pihak lembaga, dan saya tidak akan menuntut akibat publikasi tersebut

Demikian pernyataan ini saya perbuat dengan sebenar-benarnya, terima kasih

Medan, 11 November 2019

Yang membuat pernyataan

Rizky Rahmansyah

UNIVERSITAS PEMBANGUNAN PANCA BUDI
FAKULTAS SAINS & TEKNOLOGI

Jl. Jend. Gatot Subroto Km 4,5 Medan Fax. 061-8458077 PO.BOX : 1099 MEDAN

PROGRAM STUDI TEKNIK ELEKTRO	(TERAKREDITASI)
PROGRAM STUDI ARSITEKTUR	(TERAKREDITASI)
PROGRAM STUDI SISTEM KOMPUTER	(TERAKREDITASI)
PROGRAM STUDI TEKNIK KOMPUTER	(TERAKREDITASI)
PROGRAM STUDI AGROTEKNOLOGI	(TERAKREDITASI)
PROGRAM STUDI PETERNAKAN	(TERAKREDITASI)

PERMOHONAN JUDUL TESIS / SKRIPSI / TUGAS AKHIR*

aya yang bertanda tangan di bawah ini :

ama Lengkap	: RIZKY RAHMANSYAH
empat/Tgl. Lahir	: Binjai / 14 Oktober 1997
omor Pokok Mahasiswa	: 1514370012
rogram Studi	: Sistem Komputer
onsentrasi	: Keamanan Jaringan Komputer
umlah Kredit yang telah dicapai	: 141 SKS, IPK 3.56
omor Hp	: 085277010501
engan ini mengajukan judul sesuai bidang ilmu sebagai berikut	:

No.	Judul
1.	Rancang Bangun Keamanan Sistem Informasi dengan Authentifikasi Menggunakan Identifikasi One Time Password Berbasis SMS dengan Hash MD5

atan : Diisi Oleh Dosen Jika Ada Perubahan Judul

oret Yang Tidak Perlu

Rektor I,

(Ir. Bhakti Alamsyah, M.T., Ph.D.)

Medan, 23 September 2019
Pemohon,

(Rizky Rahmansyah)

Tanggal : 30/09/2019
Disahkan oleh :
Dekan

(Sri Shindi Indira, S.T., M.Sc.)

Tanggal : 03/03/2019
Disetujui oleh :
Dosen Pembimbing I :

(Akhyar Lubis, S.Kom., M.Kom)

Tanggal : 30/09/2019
Disetujui oleh:
Ka. Prodi Sistem Komputer

(Eko Hariyanto, S.Kom., M.Kom)

Tanggal : 05/03/2019
Disetujui oleh:
Dosen Pembimbing II:

(Supina Batubara, S.Kom., M.Kom)

UNIVERSITAS PEMBANGUNAN PANCA BUDI
FAKULTAS SAINS & TEKNOLOGI
Jl. Jend. Gatot Subroto Km. 4,5 Telp (061) 8455571
website : www.pancabudi.ac.id email: unpab@pancabudi.ac.id
Medan - Indonesia

Universitas : Universitas Pembangunan Panca Budi
Fakultas : SAINS & TEKNOLOGI
Dosen Pembimbing I : Akhyar Lubis, S.Kom., M.Kom
Dosen Pembimbing II : Supina Batubara, S.Kom., M.Kom
Nama Mahasiswa : RIZKY RAHMANSYAH
Jurusan/Program Studi : Sistem Komputer
Nomor Pokok Mahasiswa : 1514370012
Jenjang Pendidikan : Strata 1
Judul Tugas Akhir/Skripsi : Perancangan keamanan login sistem informasi menggunakan identifikasi one time password berbasis sms dengan hash MD5

TANGGAL	PEMBAHASAN MATERI	PARAF	KETERANGAN
5/3/2019	Acc Bab I Lanjut Seminar Proposal (Acc)		
30/4/2019	Lanjut Bab II & III		
22/8/2019	Acc Bab II tambahkan di Bab III Arsitektur Rancangan		
3/9/2019	Acc Bab III Lanjut Bab IV		
20/9/2019	Acc Bab I, II, III Acc Seminar Hasil		
25/10/2019	Acc Sidang		

Medan, 15 Januari 2019
Diketahui/Disetujui oleh :
Dekan,

Sri Shindi Indira, S.T.,M.Sc.

Coret yang tidak perlu

UNIVERSITAS PEMBANGUNAN PANCA BUDI
FAKULTAS SAINS & TEKNOLOGI
Jl. Jend. Gatot Subroto Km. 4,5 Telp (061) 8455571
website : www.pancabudi.ac.id email: unpab@pancabudi.ac.id
Medan - Indonesia

niversitas	: Universitas Pembangunan Panca Budi
kultas	: SAINS & TEKNOLOGI
osen Pembimbing I	: Akhyar Lubis, S.kom., M.kom
osen Pembimbing II	: Supina Batubara, S.kom., M.kom
ama Mahasiswa	: RIZKY RAHMANSYAH
rusan/Program Studi	: Sistem Komputer
omor Pokok Mahasiswa	: 1514370012
enjang Pendidikan	: Strata 1
dul Tugas Akhir/Skripsi	: Rancang Bangun keamanan sistem informasi dengan authentifikasi menggunakan identifikasi one time Password berbasis SMS dengan Hash MD5

TANGGAL	PEMBAHASAN MATERI	PARAF	KETERANGAN
12-1-2019	Acc Jilid		

Medan, 15 Januari 2019
Diketahui/Disetujui oleh :
Dekan,

Sri Shindi Indira, S.T.,M.Sc.

Coret yang tidak perlu

UNIVERSITAS PEMBANGUNAN PANCA BUDI
FAKULTAS SAINS & TEKNOLOGI
Jl. Jend. Gatot Subroto Km. 4,5 Telp (061) 8455571
website : www.pancabudi.ac.id email: unpab@pancabudi.ac.id
Medan - Indonesia

Universitas : Universitas Pembangunan Panca Budi
Fakultas : SAINS & TEKNOLOGI
Dosen Pembimbing I : Akhyar Lubis, S.Kom., M.Kom
Dosen Pembimbing II : Supina Batubara, S.Kom., M.Kom
Nama Mahasiswa : RIZKY RAHMANSYAH
Jurusan/Program Studi : Sistem Komputer
Nomor Pokok Mahasiswa : 1514370012
Jenjang Pendidikan : strata I
Judul Tugas Akhir/Skripsi : Perancangan Keamanan Login Sistem Informasi menggunakan Identifikasi one time password berbasis SMS dengan Hash MD5

TANGGAL	PEMBAHASAN MATERI	PARAF	KETERANGAN
04/03/2019	ACC Sempro		
30/4/2019	(Perv Bab I, Perv Meto)		
08/08/19	(Perv Bab II, (Tambah tempat-Kutipan)		
	ACC Bab I		
23/08/19	Perv Bab II, lanjut Bab III		
28/08/19	ACC Bab II, lanjut Bab III		
03/08/19	Perv Bab III, (Metode Penelit)		
10/08/2019	Perv Bab III (Tambahkan Rancangan)		
23/09/2019	ACC Seminar Hasil		
13/10/2019	ACC Sidang meja Hijau		

Medan, 15 Januari 2019
Diketahui/Disetujui oleh :
Dekan,

Sri Shindi Indira, S.T.,M.Sc

Coret yang tidak perlu

UNIVERSITAS PEMBANGUNAN PANCA BUDI
FAKULTAS SAINS & TEKNOLOGI
Jl. Jend. Gatot Subroto Km. 4,5 Telp (061) 8455571
website : www.pancabudi.ac.id email: unpab@pancabudi.ac.id
Medan - Indonesia

Universitas	: Universitas Pembangunan Panca Budi
Fakultas	: SAINS & TEKNOLOGI
Dosen Pembimbing I	: Akhyar Lubis, S.Kom., M.Kom
Dosen Pembimbing II	: Supina Batubara, S.Kom., M.Kom
Nama Mahasiswa	: RIZKY RAHMANSYAH
Jurusan/Program Studi	: Sistem Komputer
Nomor Pokok Mahasiswa	: 1514370012
Jenjang Pendidikan	: Strata 1
Judul Tugas Akhir/Skripsi	: Rancang Bangun Keamanan Sistem Informasi dengan autentifikasi menggunakan identifikasi One Time Password Berbasis SMS dengan Hash MD5

TANGGAL	PEMBAHASAN MATERI	PARAF	KETERANGAN
11/11/2019	ACC Judul		

Medan, 15 Januari 2019
Diketahui/Disetujui oleh :
Dekan,

Sri Shindi Indira, S.T.,M.Sc.

*) Coret yang tidak perlu

Plagiarism Detector v. 1092 - Originality Report:

Analyzed document: 29/10/2019 15:37:59

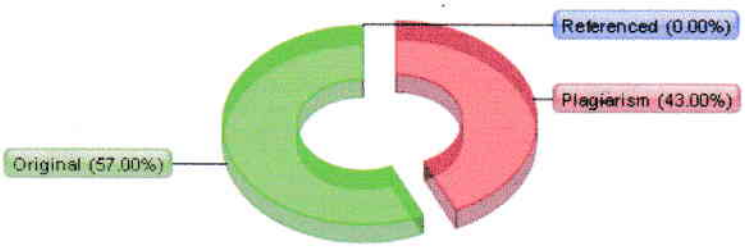
"RIZKY RAHMANSYAH_1514370012_SISTEM KOMPUTER(1).docx"

Licensed to: **Universitas Pembangunan Panca Budi_License4**

UNIVERSITAS PEMBANGUNAN PANCA BUDI
Berimtan, Berilmu, Berkarya

LEMBAGA PENJAMIN MUTU UNIVERSITAS UNPAB UNIVERSITAS PEMBANGUNAN PANCA BUDI
29/10/19

Relation chart:



Distribution graph:

Comparison Preset: Rewrite. Detected language: Indonesian

Top sources of plagiarism:

% 24	wrds: 1718	https://docplayer.info/44662772-Implementasi-algoritma-advanced-encryption-standard-aes-25...
% 10	wrds: 712	https://docplayer.info/47336399-Seminar-nasional-pendidikan-teknik-informatika-senapati.ht...
% 8	wrds: 742	https://webandini.blogspot.com/2016/11/sistem-informasi-e-business.html

[Show other Sources:]

Processed resources details:

211 - Ok / 35 - Failed

[Show other Sources:]

Important notes:

Wikipedia:	Google Books:	Ghostwriting services:	Anti-cheating:
[not detected]	[not detected]	[not detected]	[not detected]

Telah Diperiksa oleh LPMU
dengan Plagiarisme 43 %
Medan, 29 OKTOBER 2019
AN Ka. LPMU
THAMIZI HAKIM
Cahyo Pramono, SE,MM

FM-BPAA-2012-041

Hal : Permohonan Meja Hijau

Medan, 29 Oktober 2019
Kepada Yth : Bapak/Ibu Dekan
Fakultas SAINS & TEKNOLOGI
UNPAB Medan
Di -
Tempat

Telah di terima
berkas persyaratan
dapat di proses
Medan, 30/10/2019
Ka. BPAA
an.

Dengan hormat, saya yang bertanda tangan di bawah ini :

Nama	: RIZKY RAHMANSYAH
Tempat/Tgl. Lahir	: Binjai / 14 Oktober 1997
Nama Orang Tua	: SUMARNO
N. P. M	: 1514370012
Fakultas	: SAINS & TEKNOLOGI
Program Studi	: Sistem Komputer
No. HP	: 085277010501
Alamat	: Jl. Danau Singkarak No. 15

Datang bermohon kepada Bapak/Ibu untuk dapat diterima mengikuti Ujian Meja Hijau dengan judul **rancang bangun keamanan sistem informasi dengan authentifikasi menggunakan identifikasi One Time Password berbasis SMS dengan hash MD5**, Selanjutnya saya menyatakan :

1. Melampirkan KKM yang telah disahkan oleh Ka. Prodi dan Dekan
2. Tidak akan menuntut ujian perbaikan nilai mata kuliah untuk perbaikan indek prestasi (IP), dan mohon diterbitkan ijazahnya setelah lulus ujian meja hijau.
3. Telah tercap keterangan bebas pustaka
4. Terlampir surat keterangan bebas laboratorium
5. Terlampir pas photo untuk ijazah ukuran 4x6 = 5 lembar dan 3x4 = 5 lembar Hitam Putih
6. Terlampir foto copy STTB SLTA dilegalisir 1 (satu) lembar dan bagi mahasiswa yang lanjutan D3 ke S1 lampirkan ijazah dan transkipnya sebanyak 1 lembar.
7. Terlampir pelunasan kwintasi pembayaran uang kuliah berjalan dan wisuda sebanyak 1 lembar
8. Skripsi sudah dijilid lux 2 examplar (1 untuk perpustakaan, 1 untuk mahasiswa) dan jilid kertas jeruk 5 examplar untuk penguji (bentuk dan warna penjilidan diserahkan berdasarkan ketentuan fakultas yang berlaku) dan lembar persetujuan sudah di tandatangani dosen pembimbing, prodi dan dekan
9. Soft Copy Skripsi disimpan di CD sebanyak 2 disc (Sesuai dengan Judul Skripsinya)
10. Terlampir surat keterangan BKKOL (pada saat pengambilan ijazah)
11. Setelah menyelesaikan persyaratan point-point diatas berkas di masukan kedalam MAP
12. Bersedia melunaskan biaya-biaya uang dibebankan untuk memproses pelaksanaan ujian dimaksud, dengan perincian sbb :

1.	[102] Ujian Meja Hijau	: Rp. 100.000
2.	[170] Administrasi Wisuda	: Rp. 1.500.000
3.	[202] Bebas Pustaka	: Rp. 100.000
4.	[221] Bebas LAB	: Rp. 5.000
Total Biaya		: Rp. 1.705.000

30/OKTOBER
2019

5. Admin dropping uang kuliah Rp. 500.000

Total : Rp. 2.205.000

Ukuran Toga : L

Diketahui/Disetujui oleh :
Sri Shindi Indrayani, S.T, M.Sc.
Dekan Fakultas SAINS & TEKNOLOGI

Hormat saya
RIZKY RAHMANSYAH
1514370012

Catatan :

- 1.Surat permohonan ini sah dan berlaku bila ;
  - a. Telah dicap Bukti Pelunasan dari UPT Perpustakaan UNPAB Medan.
  - b. Melampirkan Bukti Pembayaran Uang Kuliah aktif semester berjalan
- 2.Dibuat Rangkap 3 (tiga), untuk - Fakultas - untuk BPAA (asli) - Mhs.ybs.

TANDA BEBAS PUSTAKA
No. 1037/PERP/BP/2019
Tidak ada sangkut paut dengan UPT. Perpustakaan
UNPAB Medan, 29 OCT 2019
an. Kepala UPT Perpustakaan
SALNIA S.IP

UKM CENTER PANCA BUDI
29/10/2019

YAYASAN PROF. DR. H. KADIRUN YAHYA
UNIVERSITAS PEMBANGUNAN PANCA BUDI
LABORATORIUM KOMPUTER
Jl. Jend. Gatot Subroto Km 4,5 Sei Sikambing Telp. 061-8455571
Medan - 20122

KARTU BEBAS PRAKTIKUM

Yang bertanda tangan dibawah ini Ka. Laboratorium Komputer dengan ini menerangkan bahwa :

Nama	:	RIZKY RAHMANSYAH
N.P.M.,	:	1514370012
Tingkat/Semester	:	Akhir
Fakultas	:	SAINS & TEKNOLOGI
Jurusan/Prodi	:	Sistem Komputer

Benar dan telah menyelesaikan urusan administrasi di Laboratorium Komputer Universitas Pembangunan Panca Budi Medan.

Medan, 29 Oktober 2019
Ka. Laboratorium

Fachrid Wadly, S. Kom.

ABSTRAK

RIZKY RAHMANSYAH

Rancang Bangun Keamanan Sistem Informasi Dengan Authentifikasi Menggunakan Identifikasi One Time Password Berbasis SMS Dengan Hash MD5

2019

Pengamanan login untuk mengakses aplikasi berbasis *WEB*, berupa pengamanan menggunakan OTP (*One Time Password*) yang di bangkitkan menggunakan *Hash MD5* dan menghasilkan sebuah kode yang dikirimkan lewat *SMS*. Sistem akan mengambil *field email*, *password*, nomor telepon. Hasil dari fungsi *hash* tersebut akan menghasilkan 32 digit bilangan hexadesimal. Selanjutnya diambil empat digit dari bilangan hexadesimal tersebut. Empat angka tersebut yang dikirimkan sebagai *OTP* dengan layanan *Cloud SMS Gateway* dari *Zenziva* dan kode *OTP* akan disimpan sementara didalam *database*. *OTP* yang dikirimkan kepada pengguna akan dicocokkan dengan yang tersimpan dalam tabel *database* untuk mengecek validitasnya. Apabila *OTP* yang dikirimkan dengan yang tersimpan dalam tabel cocok, maka pengguna bisa mengakses aplikasi berbasis *WEB*. *OTP* yang dihasilkan adalah untuk otentifikasi pengamanan akun pengguna *WEB* setelah *Login* dengan memasukkan *username* dan *password*. Pengguna yang salah memasukkan *OTP* sebanyak 3 kali akan diblokir, pembatasan tersebut adalah untuk mempersempit para *hacker* untuk menyadap dan menyusup.

Kata kunci : Keamanan; MD5; *One Time Password*; *SMS Gateway*; *Zenziva*

DAFTAR ISI

Halaman

DAFTAR GAMBAR

Halaman

DAFTAR TABEL

Halaman

KATA PENGANTAR

Puji dan syukur penulis panjatakan kepada Allah SWT atas rahmat dan karunia-Nya yang telah diberikan sehingga penulis dapat menyelesaikan tugas akhir ini.

Penulis mengangkat tema pada tugas akhir ini dengan judul: "Rancang Bangun Keamanan Sistem Informasi dengan Authentifikasi Menggunakan Identifikasi One Time Password Berbasis SMS dengan Hash MD5".

Dalam kesempatan ini, penulis mengucapkan terima kasih yang sebesar-besarnya kepada banyak pihak yang telah membantu dalam penyelesaian penyusunan Tugas Akhir ini. Penulis ingin mengucapkan terima kasih kepada :

1. Orang Tua beserta keluarga yang telah berjasa dalam memberikan dukungan moril dan materil.
2. Bapak Dr. H. Muhammad Isa Indrawan, S.E., M.M., selaku Rektor Universitas Pembangunanan Panca Budi Medan.
3. Rektor I, Bapak Ir. Bhakti Alamsyah, M.T., Ph.D
4. Dekan Fakultas Sains & Teknologi, Ibu Sri Shindi Indira, S.T., M.Sc
5. Ketua Program Studi Sistem Komputer, Bapak Eko Hariyanto, S.Kom., M.Kom
6. Dosen Pembimbing I, Bapak Akhyar Lubis, S.Kom., M.Kom.
7. Dosen Pembimbing II, Ibu Supina Batubara, S.Kom., M.Kom.
8. Seluruh Dosen dan Staf Pegawai Fakultas Sains & Teknologi yang telah banyak membantu dalam kelancaran seluruh aktivitas perkuliahan.
9. Seluruh teman-teman yang telah memberikan berbagai saran, inspirasi, dorongan, doa, motivasi dan moril maupan materil yang diperlukan sehingga penulis dapat menyelesaikan tugas akhir ini.

Penulis juga menyadari bahwa penyusunan Tugas Akhir ini belum sempurna baik dalam penulisan maupun isi disebabkan keterbatasan kemampuan penulis. Oleh karena itu, penulis mengharapkan kritik dan saran yang sifatnya membangun dari pembaca untuk penyempurnaan isi Tugas Akhir ini.

Medan, 20 September 2019
Penulis,

RIZKY RAHMANSYAH
NPM : 1514370012

BAB I

PENDAHULUAN

1.1 Latar Belakang

Kemajuan teknologi dibidang komputer memungkinkan ribuan orang dan komputer diseluruh dunia saling terhubung dalam satu dunia maya yang dikenal sebagai internet. Masalah keamanan merupakan salah satu aspek paling penting dalam dunia teknologi informasi, begitu juga ratusan organisasi seperti perusahaan, pemerintah bahkan pribadi, telah menjadikan informasi sebagai asset yang sangat berharga. Hal ini menyebabkan data dan informasi menjadi sangat penting untuk dilindungi dari manipulasi informasi, pencurian informasi dan serangan terhadap informasi yang secara langsung ataupun tidak. Disatu sisi sistem informasi menguntungkan dan dapat meningkatkan kinerja dari semua komponen organisasi, tetapi dari sisi yang lain terutama dari sisi keamanan sistem informasi yang berbasis web sangat rawan untuk di sadap oleh pihak yang tidak berkepentingan. Banyak metode yang sering digunakan oleh hacker untuk dapat mengetahui username dan password dari sebuah akun. Salah satu cara yang digunakan hacker untuk mengetahui informasi akun seseorang adalah sniffing.

Dengan menggunakan metode *One Time Password* ini pesan dikirimkan dengan cara *Multi-channel* otentikasi, yaitu proses memanfaatkan lebih dari satu saluran komunikasi untuk pengamanan identitas pengguna. Sekarang ini dimungkinkan untuk menggunakan koneksi antara ponsel dan komputer, yang bisa berkomunikasi dengan server otentikasi di Internet misalnya untuk memulai

proses otentikasi. Respon terhadap permintaan otentikasi dapat dikirim ke pengguna dengan menggunakan *Short Message Service (SMS)*. Pengiriman pesan dengan SMS ini lebih mudah diterapkan dibandingkan dengan menerima pesan dengan menggunakan aplikasi pihak ke 3 seperti *Google Authenticator*, dan layanan *Email*. Karena pengguna tidak perlu lagi memasang aplikasi untuk menerima kode otentikasi tersebut. Dari permasalahan tersebut penelitian ini difokuskan untuk merancang aplikasi pengamanan login pada sistem informasi menggunakan otentikasi *One Time Password* berbasis SMS dengan kriptografi *MD5*, yang diintegrasikan pada sistem informasi berbasis website. Kriptografi bertujuan untuk memberikan layanan keamanan, termasuk keamanan untuk menjaga password. Sistem informasi yang baik adalah sistem informasi yang dapat dinilai tingkat keamanannya, sehingga mampu memberikan kenyamanan bagi pengguna (Umar, Riadi, & Handoyo, 2019)

Fungsi kriptografi MD5 digunakan untuk menghasilkan OTP dengan mengambil *field email, password,* nomor *handphone* pengguna yang diambil dari *database* pengguna dan waktu akses pengguna. Perancangan pengamanan login web ini mengunakan pemrograman *PHP: Hypertext PreProcessor* (PHP), dan penyimpanan data menggunakan *MySQL*. Berdasarkan uraian di atas, penulis melakukan penelitian yang lebih mendalam dengan mengambil konsep judul yaitu "Rancang Bangun Keamanan Sistem Informasi dengan Authentifikasi Menggunakan Identifikasi *One Time Password* Berbasis *SMS* dengan *Hash MD5*".

1.2 Rumusan Masalah

Berdasarkan latar belakang masalah diatas maka rumusan masalah adalah sebagai berikut :

a. Bagaimana rancang bangun keamanan halaman login?
b. Bagaimana menerapkan sistem identifikasi login menggunakan *One Time Password* pada sistem informasi yang dibangun?

1.3 Batasan Masalah

Dalam perancangan sistem keamanan login menggunakan *One Time Password* ini penulis membatasi masalah sebagai berikut :

a. Metode yang digunakan pada perancangan sistem informasi ini menggunakan metode *One Time Password* yang menggunakan kriptografi MD5 hash.
b. Menggunakan *Aplication Programming Interface (API)* Zenziva sebagai *Online SMS Gateway*.
c. Bahasa pemrograman yang digunakan untuk merancang sistem ini adalah *PHP* dan menggunakan *Database MySQL*.
d. Analisis difokuskan pada keamanan sistem otentikasi bukan pada keamanan pengiriman token.
e. Pemblokiran *user* akan dilakukan selama 1 jam apabila salah memasukkan *One Time Password* sebanyak 3 kali berturut-turut.
f. Penelitian hanya sebatas penerapan *One Time Password* kedalam sistem, tidak membahas perhitungan manual algoritma MD5.

1.4 Tujuan Penelitian

Tujuan yang ingin dicapai penulis dalam perancangan keamanan halaman login *One Time Password* ini adalah :

a. Menerapkan algoritma kriptografi *MD5* untuk merancang dan membangun keamanan halaman *login website*.
b. Untuk menerapkan sistem enkripsi menggunakan metode *One Time Password* kedalam sebuah sistem informasi yang dibangun.

1.5 Manfaat Penelitian

Perancangan sistem keamanan login menggunakan metode *One Time Password* ini bermanfaat bagi pengguna sistem informasi antara lain :

a. Sebagai penambahan wawasan melindungi data informasi pada sistem dengan implementasi algoritma kriptografi.
b. Meningkatkan keamanan data *login* pada *website.*

BAB II

LANDASAN TEORI

2.1 Sistem

Menurut (Ariawan & Wahyuni, 2015) “sistem adalah kumpulan dari sub-sub sistem baik sistem abstrak maupun fisik yang saling terintegrasi dan berkolaborasi untuk mencapai tujuan tertentu. Sistem adalah setiap sesuatu yang terdiri dari obyek-obyek, atau unsur-unsur, atau komponen - komponen yang bertata kaitan dan bertata hubungan satu sama lain, sedemikian rupa sehingga unsur-unsur tersebut merupakan satu kesatuan pemrosesan atau pengolahan yang tertentu”.

Dengan demikian dapat disimpulkan bahwa sistem merupakan seperangkat elemen yang saling berhubungan yang bersama-sama mencapai suatu tujuan tertentu dalam proses yang teratur yang dapat mendukung sistem yang lebih besar dan saling memiliki ketergantungan untuk mencapai tujuan tertentu.

2.2 Informasi

Menurut (Marshall B. Romney & Steinbart, 2015) “informasi adalah data yang telah dikelola dan di proses untuk memberikan arti dan memperbaiki proses pengambilan keputusan”.

Dengan demikian dapat disimpulkan bahwa informasi adalah data yang diproses menjadi suatu bentuk yang lebih berguna dan berarti bagi yang menerimanya dalam aktivitas pembuatan keputusan.

2.3 Sistem Informasi

Secara garis besar sistem merupakan suatu kumpulan komponen dan elemen yang saling terintegrasi, komponen yang terorganisir dan bekerja sama dalam mewujudkan suatu tujuan tertentu.

Menurut (Djahir & Pratita, 2014) mengemukakan bahwa "sistem adalah kumpulan/grup dari subsistem/bagian/komponen apapun, baik fisik ataupun nonfisik yang saling berhubungan satu sama lain dan bekerja sama secara harmonis untuk mencapai satu tujuan tertentu". Sedangkan menurut (Mulyani, 2017) menyatakan bahwa "sistem bisa diartikan sebagai sekumpulan sub sistem, komponen yang saling bekerja sama dengan tujuan yang sama untuk menghasilkan output yang sudah ditentukan sebelumnya". Selain itu menurut (HUTAHAEAN, 2017) mengemukakan bahwa "sistem adalah suatu jaringan kerja dari prosedur-prosedur yang saling berhubungan, berkumpul bersama-sama untuk melakukan kegiatan atau untuk melakukan sasaran tertentu".

Berdasarkan pendapat dari para ahli diatas, dapat disimpulkan bahwa sistem merupakan suatu kumpulan komponen dari subsistem yang saling bekerja sama dari prosedur-prosedur yang saling berhubungan untuk menghasilkan output dalam mencapai tujuan tertentu.

2.4 Keamanan Sistem Informasi

Menurut G. J. Simons, keamanan sistem informasi adalah bagaimana kita dapat mencegah penipuan (*cheating*) atau, paling tidak, mendeteksi adanya

penipuan di sebuah sistem yang berbasis informasi, dimana informasinya sendiri tidak memiliki arti fisik.

Selain itu keamanan sistem informasi bisa diartikan sebagai kebijakan, prosedur, dan pengukuran teknis yang digunakan untuk mencegah akses yang tidak sah, perubahan program, pencurian, atau kerusakan fisik terhadap sistem informasi. Sistem pengamanan terhadap teknologi informasi dapat ditingkatkan dengan menggunakan teknik-teknik dan peralatan-peralatan untuk mengamankan perangkat keras dan lunak komputer, jaringan komunikasi, dan data.

2.5 Autentikasi

Autentikasi adalah metode untuk menyatakan bahwa informasi betul-betul asli, atau orang yang mengakses atau memberikan informasi adalah betul-betul orang yang dimaksud.

2.6 OTP (One Time Password)

Password atau kata sandi dapat digunakan untuk layanan otentikasi, yaitu layanan yang berhubungan dengan identifikasi, baik mengidentifikasi kebenaran pihak-pihak yang berkomunikasi (*user authentication* atau *entity authentication*) maupun mengidentifikasi kebenaran sumber pesan. Dua pihak yang saling berkomunikasi harus dapat mengotentikasi satu sama lain sehingga ia dapat memastikan sumber pesan. Otentikasi sumber pesan secara implisit juga memberikan kepastian integritas data, sebab jika pesan telah dimodifikasi berarti sumber pesan sudah tidak benar. *One Time Password* (OTP) adalah sebuah

password yang hanya berlaku untuk sesi login tunggal atau transaksi tunggal. Berbeda dengan penggunaan password statis, OTP tidak menggunakan password yang sama untuk setiap login atau transaksi, sehingga jika pihak yang tidak berkepentingan berhasil merekam password OTP yang sudah digunakan maka dia tidak akan dapat menyalahgunakan password tersebut karena sudah tidak berlaku lagi. Untuk dapat membuat sebuah password OTP, digunakan salah satu metode kriptografi, yaitu fungsi hash, dan untuk pemilihan karakternya dipilih secara acak dengan Pseudo Random Number Generator. (Sakti, Agani, & Hardjianto, 2016)

2.7 Kriptografi

Kriptografi adalah ilmu mengenai teknik enkripsi dimana data diacak menggunakan suatu kunci enkripsi menjadi sesuatu yang sulit dibaca oleh seseorang yang tidak memiliki kunci dekripsi. Dekripsi menggunakan kunci dekripsi mendapatkan kembali data asli. Proses enkripsi dilakukan menggunakan suatu algoritma dengan beberapa parameter. Biasanya algoritma tidak dirahasiakan, bahkan enkripsi yang mengandalkan kerahasiaan algoritma dianggap sesuatu yang tidak baik. Rahasia terletak di beberapa parameter yang digunakan, jadi kunci ditentukan oleh parameter. Parameter yang menentukan kunci dekripsi itulah yang harus dirahasiakan. (Agung & Prasta, 2018)

Proses yang dilakukan untuk mengubah plaintext menjadi ciphertext disebut enkripsi (*encryption*) atau *encipherment* sedangkan proses untuk mengubah *ciphertext* kembali ke *plaintext* disebut dekripsi (*decryption*) atau decipherment. Kriptografi memerlukan parameter untuk proses konversi yang dikendalikan oleh

sebuah kunci atau beberapa kunci. Kriptografi saat ini telah menjadi salah satu syarat penting dalam keamanan teknologi informasi terutama dalam pengiriman pesan rahasia. Pengiriman pesan rahasia sangat rentan terhadap serangan yang dilakukan oleh pihak ketiga, seperti penyadapan, pemutusan komunikasi, pengubahan pesan yang dikirim dan lain-lain. Kriptografi dapat meningkatkan keamanan dalam pengiriman pesan atau komunikasi data dengan cara menyandikan pesan tersebut berdasarkan algoritma dan kunci tertentu yang hanya diketahui oleh pihak-pihak yang berhak atas data, informasi dan dokumen tersebut.

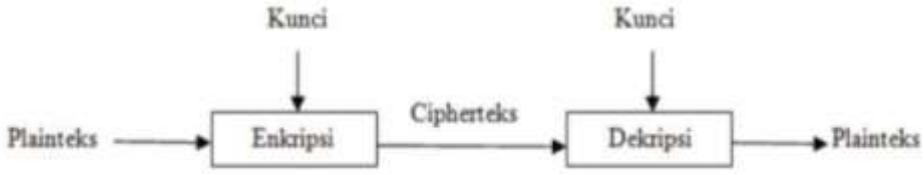
Di dalam kriptografi akan sering menemukan berbagai istilah atau terminologi. Beberapa istilah yang harus diketahui yaitu :

a. Enkripsi dan Dekripsi

   Proses menyandikan plaintext menjadi *ciphertext* disebut enkripsi (*encryption*) atau *enciphering*. Sedangkan proses mengembalikan *ciphertext* menjadi plaintext disebut dekripsi (*decryption*) atau *deciphering*.

b. Cipher dan Kunci

   Algoritma kriptogarfi disebut juga *cipher*, yaitu aturan untuk enkripsi dan dekripsi, atau fungsi matematika yang digunakan untuk enkripsi dan dekripsi. Beberapa *cipher* memerlukan algoritma yang berbeda untuk *enciphering* dan *deciphering*, dapat dilihat pada Gambar 2.1.



Gambar 2.1 Skema Enkripsi dan Dekripsi Dengan Menggunakan Kunci
Sumber : Triase (2016)

c. Sistem Kriptografi

Kriptografi membentuk sebuah sistem yang dinamakan sistem kriptografi. Sistem kriptografi (*cryptosystem*) adalah kumpulan yang terdiri dari algoritma kriptografi, semua plaintext dan ciphertext yang mungkin, dan kunci. Di dalam kriptografi, cipher hanyalah salah satu komponen saja.

d. Penyadap

Penyadap (*eavesdropper*) adalah orang yang mencoba menangkap password selama ditransmisikan. Tujuan penyadap adalah untuk mendapatkan username dan password pada website informasi mengenai sistem kriptografi yang digunakan untuk berkomunikasi dengan maksud untuk memecahkan ciphertext. Nama lain penyadap : enemy, adversary, intruder, interceptor, bad guy.

e. Kriptanalisis dan Kriptologi

Kriptografi berkembang sedemikian rupa sehingga melahirkan bidang yang berlawanan yaitu kriptanalisis. Kriptanalisis (*cryptanalysis*) adalah ilmu dan seni untuk memecahkan ciphertext menjadi plaintext tanpa mengetahui kunci yang digunakan. Pelakunya disebut kriptanalis. Jika seorang kriptografer (*cryptographer*) mentransformasikan plaintext menjadi ciphertext dengan suatu algoritma dan kunci maka sebaliknya seorang kriptanalis berusaha untuk memecahkan ciphertext tersebut untuk menemukan plaintext atau kunci. Kriptologi (*cryptology*) adalah studi mengenai kriptografi dan kriptanalisis.

2.7.1 Prinsip Dasar Kriptografi

Kriptografi adalah ilmu dan seni untuk menjaga kerahasiaan pesan dengan cara menyandikannya ke dalam bentuk yang tidak dapat dimengerti lagi maknanya (Pabokory, Astuti, & Kridalaksana, 2016). Prinsip-prinsip yang mendasari kriptografi yakni :

a. *Secrecy* (kerahasiaan) layanan yang digunakan untuk menjaga isi dari informasi dari siapapun kecuali yang memiliki otoritas atau kunci rahasia untuk membuka maupun menghapus informasi yang telah disandi.
b. *Authentication* berhubungan dengan identifikasi atau pengenalan, baik secara kesatuan sistem maupun informasi itu sendiri. Dua pihak yang saling berkomunikasi harus saling memperkenalkan diri. Dimana informasi yang dikirimkan melalui kanal harus di *autentifikasi* keaslian, isi datanya, waktu pengiriman dan lain-lain.
c. Hak Akses terhadap suatu *file* atau fasilitas lain dalam sebuah sistem pemrosesan informasi masih dalam area lain dimana gagasan kriptografi telah diterapkan.

2.7.2 Algoritma MD5

MD5 adalah salah satu fungsi *hash* yang paling banyak digunakan. MD5 merupakan versi perbaikan dari MD4 yang dirancang oleh Ron Rivest pada tahun 1991. MD5 umumnya digunakan sebagai *checksum* untuk verifikasi integritas file yang didownload dari internet.

MD5 memproses teks masukan ke dalam blok-blok 512 bit, kemudian dibagi menjadi 16 buah sub blok sebesar 32 bit. Keluaran dari algoritma MD5 adalah sebuah set dari 4 buah blok masing-masing 32 bit, yang kemudian menghasilkan nilai *hash* 128 bit (Agung & Linda, 2016).

2.8 SMS Gateway

SMS Gateway adalah komunikasi menggunakan SMS yang mengandung informasi berupa nomor telepon seluler pengirim, penerima, waktu dan pesan. Informasi tersebut dapat diolah dan bisa melakukan aktivasi transaksi tergantung kode-kode yang sudah disepakati. Untuk dapat mengelola semua transaksi yang masuk dibutuhkan sebuah sistem yang mampu menerima kode SMS dengan jumlah tertentu, mengolah informasi yang terkandung dalam pesan SMS dan melakukan transaksi yang dibutuhkan (Afrina & Ibrahim, 2015). Penulis akan menggunakan Zenziva sebagai penyedia layanan *Cloud SMS gateway*.

2.8.1 Zenziva

Zenziva adalah layanan online *SMS Center* & *SMS Masking*. Untuk menggunakan layanan Zenziva *user* harus melakukan registrasi terlebih dulu. Ada beberapa pilihan paket SMS yang disediakan oleh Zenziva dan bisa dipilih oleh *user* tergantung dari kebutuhan masing-masing user. Dengan memanggil *web service* dari Zenziva, secara sistem sudah dapat menggunakan layanan *SMS gateway* Zenziva.

2.9 Basis Data

Dalam pembuatan aplikasi, para pembuat aplikasi atau *programmer* menggunakan basis data yang digunakan untuk pengolahan data atau penataan file-file yang ada dan digunakan kembali sesuai dengan kebutuhan aplikasi tersebut.

2.9.1 Pengertian Basis Data

Basis data merupakan tempat pengolahan informasi yang sangat penting dalam upaya menciptakan suatu aplikasi yang terintegrasi.

Menurut (Shalahuddin & Sukamto, 2018) sistem basis data adalah sistem terkomputerisasi yang tujuan utamanya adalah memelihara data yang sudah diolah atau informasi dan membuat informasi tersedia saat dibutuhkan. Sedangkan Menurut (Suharyanto, Chandra, & Gunawan, 2017) menjelaskan, *database* adalah kumpulan data terstruktur. Agar dapat menambahkan, mengakses, dan memproses data yang tersimpan dalam *database* komputer, dibutuhkan sistem manajemen basis data (*database management system*).

Menurut (Swara & Pebriadi, 2016) Basis data atau *database* adalah kumpulan informasi yang disusun dan merupakan suatu kesatuan yang utuh yang disimpan di dalam perangkat keras (komputer) secara sistematis sehingga dapat diolah menggunakan perangkat lunak. Dengan sistem tersebut data yang terhimpun dalam suatu *database* dapat menghasilkan informasi yang berguna.

Dapat ditarik kesimpulan bahwa basis data merupakan sekumpulan data yang diolah menjadi informasi dan dapat digunakan kembali jika suatu saat dibutuhkan.

2.9.2 Aplikasi Basis Data

Aplikasi basis data sering digunakan oleh para pembuat aplikasi sebagai media pengolahan basis data. Aplikasi basis data yang sering digunakan dalam pengolahan basis data yaitu MySQL dan phpMyAdmin.

a. *My*SQL

Salah satu aplikasi basis data yang sering digunakan untuk mengolah dan menata file-file yaitu *MySQL*. Menurut (Madcoms, 2016b) "*MySQL* adalah sistem manajemen *database SQL* yang bersifat *Open Source* dan paling populer saat ini. Sistem *Database MySQL* mendukung beberapa fitur seperti *multithreaded*, *multi-user*, dan *SQL database management system* (DBMS). *Database* ini dibuat untuk keperluan sistem *database* yang cepat, handal, dan mudah digunakan". Sedangkan Menurut (Raharjo, Heryanto, & Rosdiana, 2015), "*MySQL* merupakan software RDBMS (atau *server database*) yang dapat mengelola *database* dengan sangat cepat, dapat menampung data dalam jumlah sangat besar, dapat diakses oleh banyak user (*multi-user*), dan dapat melakukan suatu proses secara sinkron atau berbarengan *(multi-threaded).*". Penulis menyimpulkan bahwa *MySQL* merupakan aplikasi pengolahan database

yang sering digunakan untuk membuat sebuah aplikasi yang memiliki data-data sebagai sumber pengolahannya.

b. phpMyAdmin

Selain *MySQL*, aplikasi yang dapat mengolah basis data yaitu *phpMyAdmin*. *phpMyAdmin* memiliki fungsi yang sama dengan *MySQL*, namun untuk pengaksesan aplikasi menggunakan browser. Menurut (Sukmaindrayana & Sidik, 2017) "*PhpMyadmin* adalah sebuah aplikasi open source yang berfungsi untuk memudahkan manajemen *MySQL*".

Sedangkan menurut (Madcoms, 2016b) "*phpMyAdmin* adalah salah satu aplikasi yang digunakan untuk memudahkan dalam melakukan pengelolaan database *MySQL"*. *phpMyAdmin* merupakan aplikasi web yang bersifat opensource." yang diperlukan. Manipulasi data tersebut berupa menambah, mengubah, dan menghapus data yang berada dalam database".

Maka dari itu, dapat disimpulkan bahwa *phpMyAdmin* merupakan aplikasi yang digunakan untuk melakukan pengolahan basis data dengan browser sebagai medianya.

2.9.3 XAMPP

Menurut (Madcoms, 2016) berpendapat bahwa "*Xampp* adalah sebuah paket kumpulan *software* yang terdiri dari *Apache, MySQL, PhpMyAdmin, PHP, Perl, Filezilla*, dan lain.".

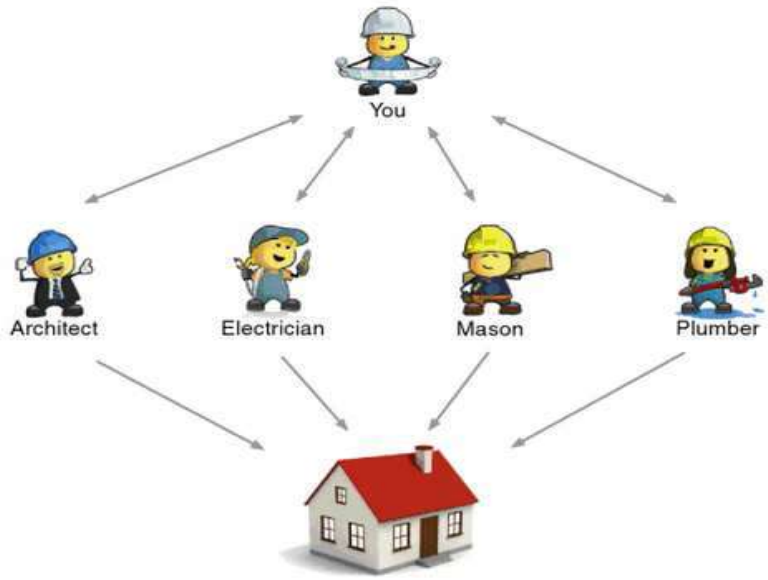
Menurut (Rahman & Santoso, 2015) "*Xampp* merupakan paket *PHP* dan *MySQL* berbasis *open source*, yang dapat digunakan sebagai tool pembantu pengembangan aplikasi berbasis *PHP*".

Dari pendapat diatas dapat ditarik kesimpulan *XAMPP* merupakan paket *PHP* dan *MySQL* berbasis *open source*, yang dapat digunakan sebagai tool pembantu pengembangan aplikasi berbasis *PHP*.

2.10 API (*Application Programming Interface*)

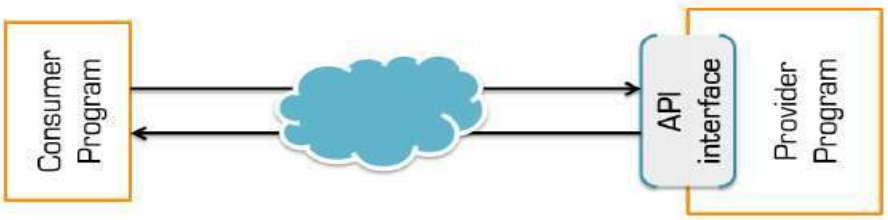
API merupakan software *interface* yang terdiri atas kumpulan instruksi yang disimpan dalam bentuk library dan menjelaskan bagaimana agar suatu *software* dapat berinteraksi dengan *software* lain. Menurut (Rama & Kak, 2015) "Secara umum *API* merupakan ekspresi terfokus keseluruhan fungsional dalam suatu modul *software* yang dapat diakses oleh orang yang membutuhkan dengan cara yang telah ditentukan layanan".

Penjelasan ini dapat dicontohkan dengan analogi apabila akan dibangun suatu rumah. Dengan menyewa kontraktor yang dapat menangani bagian yang berbeda, pemilik rumah dapat memberikan tugas yang perlu dilakukan oleh kontraktor tanpa harus mengetahui bagaimana cara kontraktor menyelesaikan pekerjaan tersebut. Dari analogi tersebut, rumah merupakan software yang akan dibuat, dan kontraktor merupakan *API* yang mengerjakan bagian tertentu dari software tersebut tanpa harus diketahui bagaimana prosedur dalam melakukan pekerjaan tersebut.



Gambar 2.2 Analogi API pada Pembangunan Rumah
Sumber: Reddy (2015)

Interface pada *software* merupakan suatu entry points yang digunakan untuk mengakses seluruh resources yang terdapat di dalam *software* tersebut. Dengan adanya *API*, maka terdapat aturan bagaimana *software* dapat berinteraksi dengan *software* lain untuk mengakses *resources* melalui *interface* yang telah tersedia.



Gambar 2.3 Skema Konektivitas API Antar Software
Sumber: 3Scale Networks (2015)

Secara struktural, *API* merupakan spesifikasi dari suatu data *structure*, *objects*, *functions*, beserta parameter-parameter yang diperlukan untuk mengakses *resource* dari aplikasi tersebut. Seluruh spesifikasi tersebut membentuk suatu *interface* yang dimiliki oleh aplikasi untuk berkomunikasi dengan aplikasi lain, dan *API* dapat digunakan dengan berbagai bahasa *programming*, ataupun hanya

dengan menggunakan *URL (Uniform Resource Locator)* yang telah disediakan oleh suatu *website*.

API dapat diklasifikasikan menjadi beberapa kategori, hal ini dilihat dari abstraksi apa yang dideskripsikan di dalam sistem. Kategori-kategori ini diantaranya:

Tabel 2.1 Kategori API

Kategori API	Deskripsi	Contoh
Operating System	Api yang digunakan untuk fungsi dasar yang dapat dilakukan oleh komputer. Seperti proses I/O, eksekusi program.	API for MS Windows
Programming Languages	Api yang digunakan untuk memperluas kapabilitas dalam melakukan eksekusi terhadap suatu bahasa pemrograman.	Java API
Application Service	API yang digunakan untuk mengakses data dan layanan yang disediakan dari suatu aplikasi.	API for mySAP (BAPI/*Bussines Application Programming Interfaces)*
Infrastructure Service	Digunakan untuk mengakses infrastruktur dari suatu komputer. Infrastruktur disini	Amazon EC2 (Elastic Compute Cloud) untuk akses untuk virtual computing dan Amazon

	adalah komputer beserta *peripheral* seperti *storage*, aplikasi dan lain-lain	S3 (Simple Storage Service) untuk menyimpan data dalam jumlah besar.
Web Services	API yang digunakan untuk mengakses content dan layanan yang disediakan oleh suatu web application.	Facebook Graph API yang digunakan untuk mengakses informasi yang dapat dibagikan.

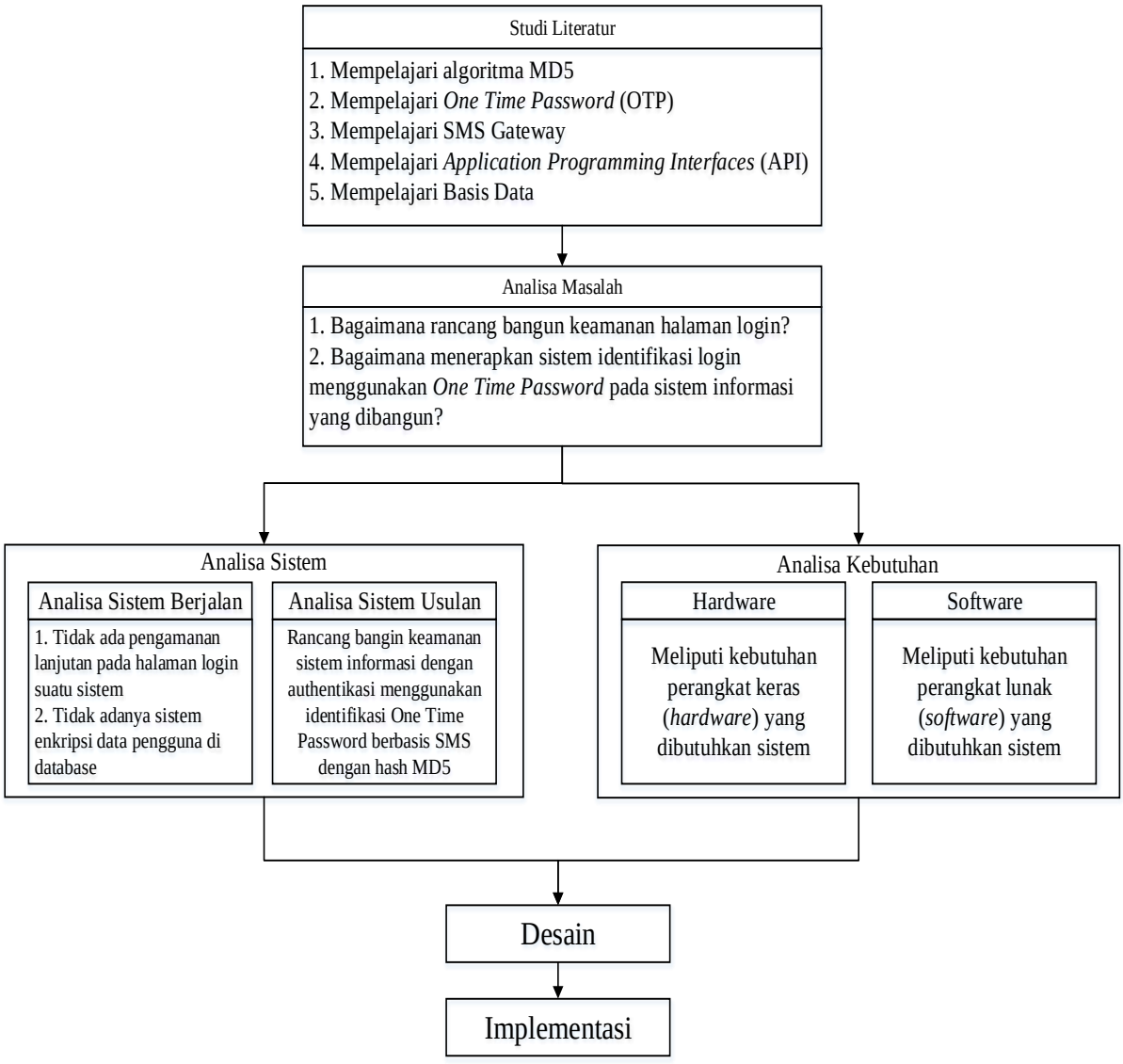
Sumber: Gumelar (2018)

BAB III

METODE PENELITIAN

3.1 Tahapan Penelitian

Tahapan penelitian mencakup langkah-langkah pelaksanaan penelitian dari awal sampai akhir. Masing-masing Langkah penelitian diuraikan secara rinci sebagai berikut:



Gambar 3.1 Tahapan Penelitian

Dari gambar 3.1 Tahapan Penelitian diatas dapat dijelaskan secara terperinci adalah sebagai berikut :

1. Studi Literatur

Pada tahapan ini penulis melakukan pengumpulan semua informasi yang diperlukan untuk membangun sistem. Informasi tersebut dapat diperoleh penulis dari berbagai sumber dengan cara membaca literatur yang terdapat pada jurnal, artikel, buku-buku dan skripsi. Pada tahapan ini akan dilakukan beberapa pembelajaran, seperti mempelajari algoritma MD5, *One Time Password* (OTP), SMS Gateway, *Application Programming Interfaces* (API), dan basis data.

2. Analisa Masalah

Pada tahap ini penulis akan menganalisis masalah dan mengumpulkan data yang ada pada sistem sebelumnya, lalu penulis akan mengusulkan beberapa metode untuk menyempurnakan sistem sebelumnya, metode yang diusulkan penulis diharapkan dapat mengurangi penyusupan hacker untuk masuk kedalam sistem, beberapa metode yang penulis usulkan seperti, bagaimana rancang bangun keamanan halaman login? bagaimana menerapkan sistem identifikasi login menggunakan *One Time Password* pada sistem informasi yang dibangun?

3. Analisa Sistem Berjalan

Pada tahapan ini penulis akan menganalisa keamanan sistem informasi yang berjalan serta mengumpulkan masalah-masalah yang ada pada sistem sebelumnya. Penulis melakukan eksperimen terhadap sistem yang berjalan sehingga penulis dapat mengumpulkan kelemahan apa saja yang terdapat pada sistem yang ada saat ini.

4. Analisa Sistem Usulan

Pada tahapan ini penulis akan mengusulkan sistem keamanan yang lebih baik dari sebelumnya yang hanya mengandalkan *username* dan *password* untuk masuk kedalam sistem informasi. Sistem usulan penulis adalah rancang bangun keamanan sistem informasi dengan authentikasi menggunakan identifikasi *One Time Password* berbasis *SMS* dengan *hash MD5*.

5. Analisa Kebutuhan Sistem

Pada tahapan ini penulis akan menganalisa kebutuhan dari perangkat keras (*hardware*) dan kebutuhan dari perangkat lunak (*software*) yang akan digunakan untuk membangun sistem.

3.2 Metode Pengumpulan Data

Studi literatur adalah tahap dalam mengumpulkan semua informasi yang diperlukan penulis untuk membangun sistem. Informasi tersebut dapat diperoleh penulis dari berbagai sumber dengan cara membaca literatur yang terdapat pada jurnal, artikel, buku-buku dan skripsi.Dari literatur tersebut dapat diketahui persamaan ataupun perbedaan terhadap penelitian yang dilakukan oleh penulis maupun dengan peneliti lainya. Sumber tersebut dijadikan sebagai landasan teori untuk proses pengembangan Rancang Bangun Keamanan Sistem Informasi dengan Autentikasi Menggunakan Identifikasi *One Time Password* Berbasis *SMS* dengan *Hash MD5*.

3.2.1 Studi Kepustakaan

Studi kepustakaan dilakukan dengan cara membaca, mengutip dan membuat catatan yang bersumber pada bahan-bahan pustaka yang mendukung dan berkaitan dengan rancang bangun keamanan sistem informasi. Selanjutnya dengan cara mempelajari dan memahami sistem yang berhubungan dengan masalah yang akan dibahas dalam karya ilmiah ini. Hal ini dimaksudkan agar penulis memiliki landasan teori yang kuat dalam menarik kesimpulan.

3.2.2 Eksperimen

Setelah mendapatkan data secara studi kepustakaan, proses penelitian akan dilakukan eksperimen atau percobaan. Dalam eksperimen ini pengumpulan data dapat diambil secara langsung, sehingga akan lebih mendalami dalam melakukan penelitian. Penulis juga melakukan percobaan berulang-ulang untuk menghindari dan meminimalkan kesalahan dalam penelitian ini.

3.3 Analisa Sistem

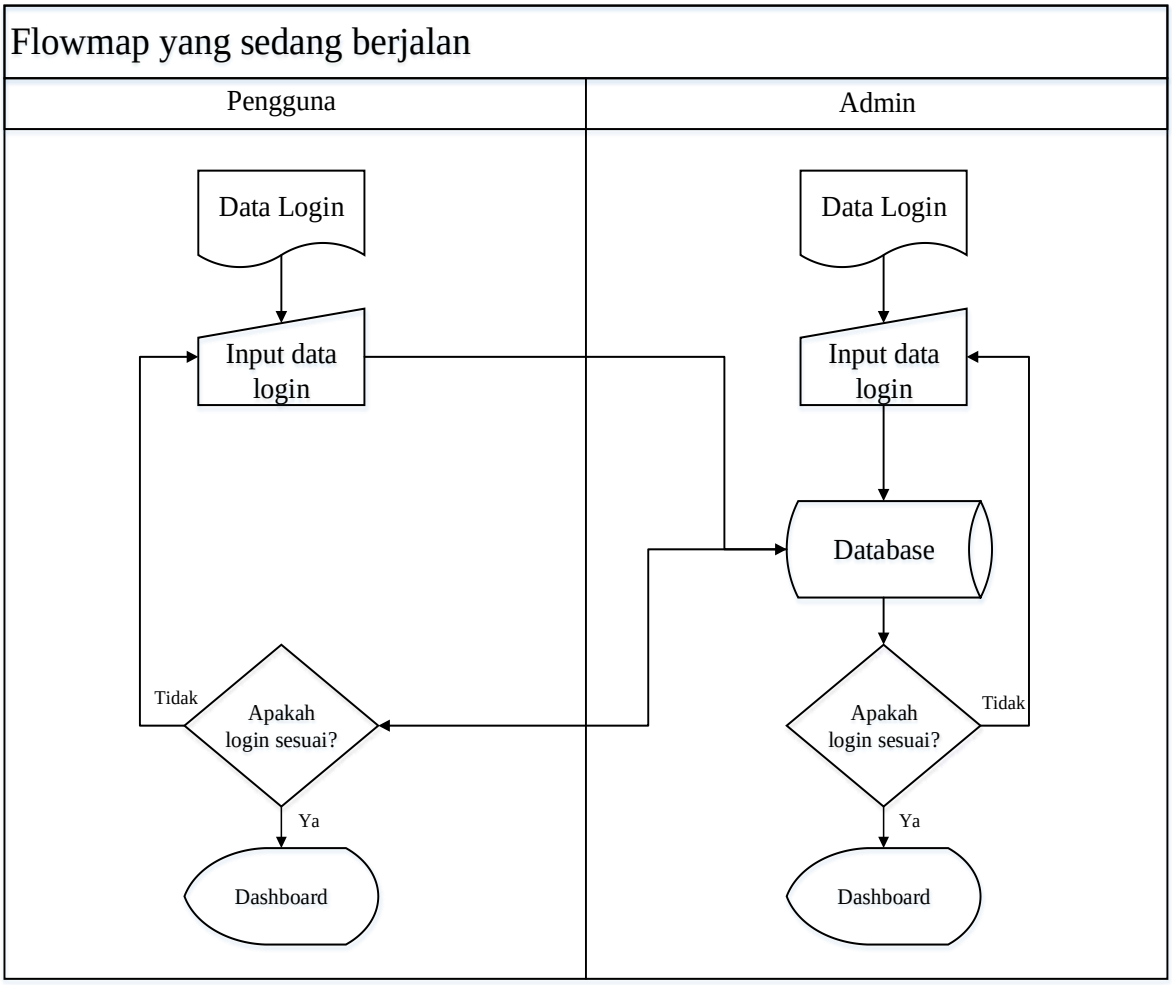
3.3.1 Analisa Sistem Berjalan

Pada tahapan ini akan dianalisis mengenai prosedur-prosedur yang sedang berjalan dan diperoleh beberapa prosedur diantaranya :

a. Kata sandi yang diinputkan pengguna kedalam sistem tidak terenkripsi.
b. Kata sandi yang disimpan di *database* tidak terenkripsi.
c. Untuk login kedalam sistem pengguna hanya diminta memasukkan *username* dan *password*.

d. Tidak ada sistem keamanan tambahan berupa *Two Factor Authentication.*

Adapun flowmap sistem yang sedang berjalan sebagai berikut:



Gambar 3.2 Flowmap yang sedang berjalan

3.3.2 Analisa Sistem Usulan

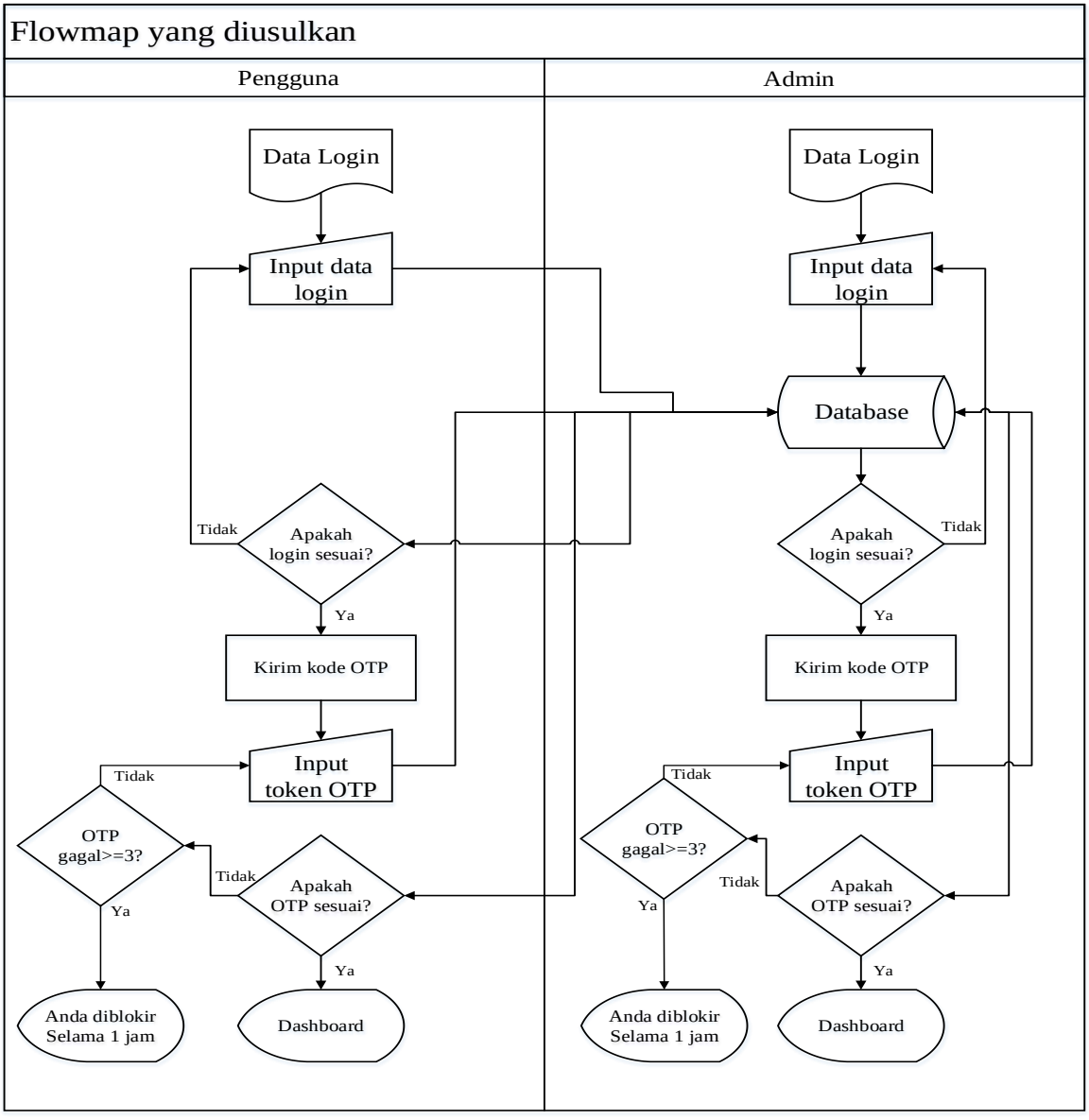
a. Kata sandi yang diinput pengguna akan dienkripsi menggunakan *hash MD5.*

b. Kata sandi yang disimpan di *database* akan dienkripsi menggunakan *hash MD5.*

c. Selain username dan password pengguna akan diminta kode *token* yang akan dikirimkan ke ponsel sebagai kemananan.

d. Sebelum masuk kehalaman utama (*dashboard*) pengguna akan diarahkan ke form *Two Factor Authentication* untuk dimintai memasukkan kode *OTP* yang dikirimkan keponsel pengguna melalui *SMS*.

Adapun flowmap yang diusulkan penulis adalah sebagai berikut :

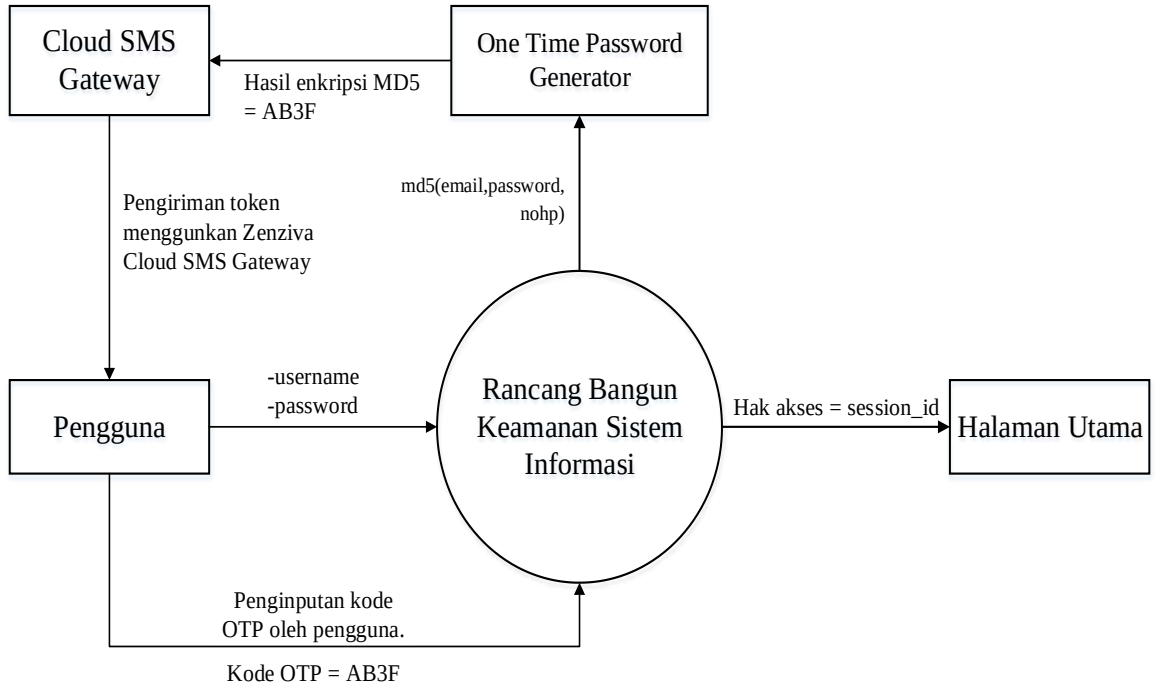


Gambar 3.3 Flowmap yang akan diterapkan

3.4 Diagram Konteks

Diagram konteks adalah diagram yang terdiri dari suatu proses dan menggambarkan ruang lingkup suatu sistem. Diagram konteks merupakan level tertinggi dari DFD yang menggambarkan seluruh input ke dalam sistem atau output dari sistem yang memberi gambaran tentang keseluruhan sistem. Sistem dibatasi oleh boundary (Digambarkan dengan garis putus - putus). Dalam diagram konteks hanya ada satu proses, tidak boleh ada store dalam diagram konteks.

Adapun diagram konteks pada keamanan sistem informasi dapat digambarkan sebagai berikut:



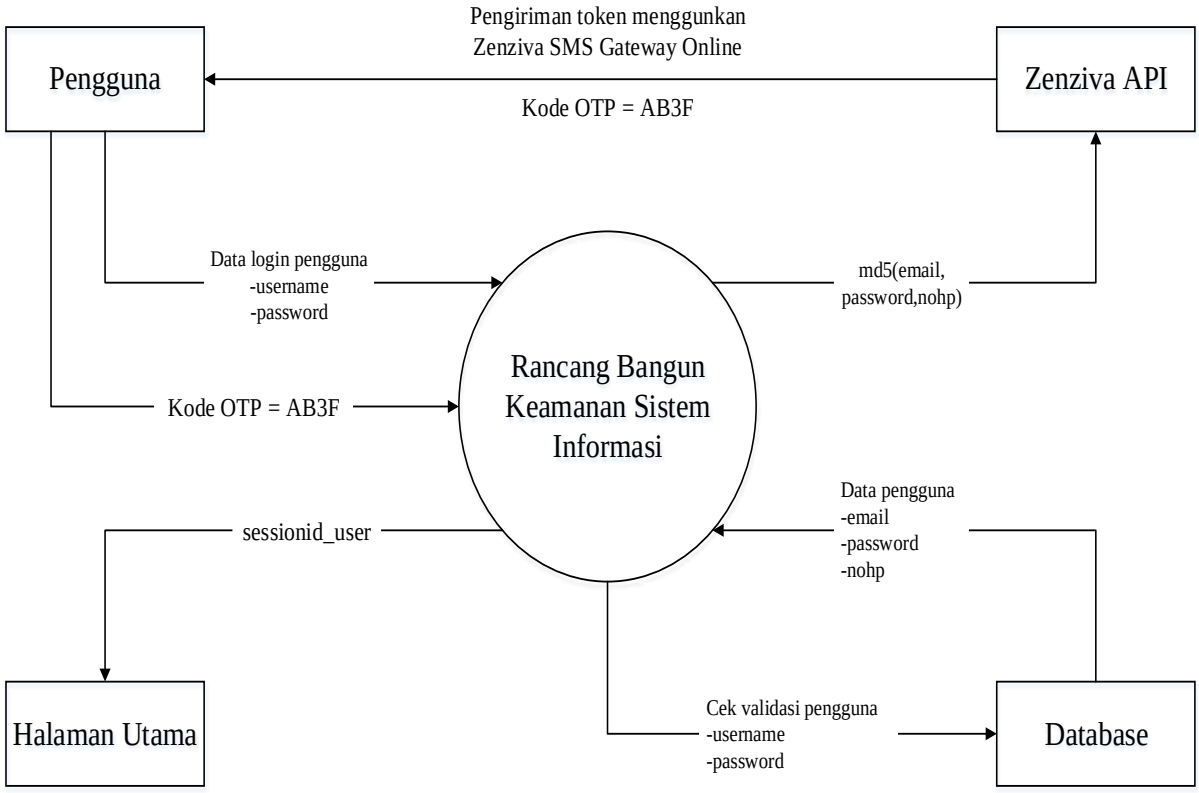
Gambar 3.4 Diagram Konteks

3.5 Data Flow Diagram

Pada Data Flow Diagram dibawah ini penulis merepresentasi graphis dari sistem yang menggambarkan komponen-komponen sistem yang penulis bangun, aliran-aliran data diantara komponen-komponen tersebut beserta asal, tujuan dan penyimpanan datanya.

3.5.1 Data Flow Diagram Level 1

Pada diagram level 1 ini menggambarkan pecahan data dari diagram konteks. Berikut adalah data flow diagram level 1:



Gambar 3.5 Data Flow Diagram Level 1

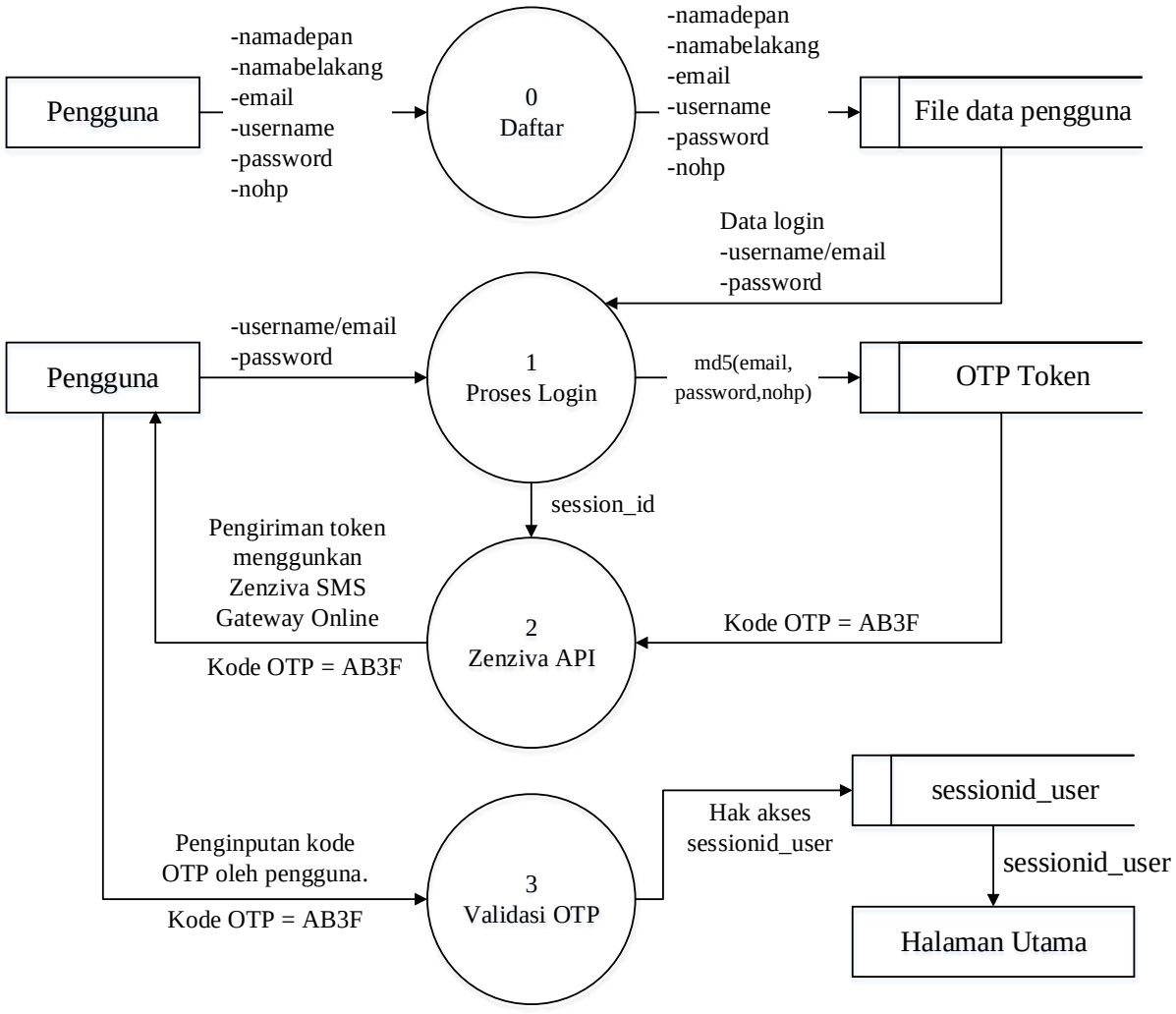
Adapun penjelasan dari data flow diagram level 1 diatas adalah sebagai berikut:

a. Pengguna menginputkan data *login* seperti, *username* dan *password*.
b. Lalu sistem akan melakukan validasi dari data yang diinputkan pengguna. Sistem akan mencocokkan dengan data yang ada di *database*.
c. Ketika validasi selesai dan data *login* dinyatakan cocok maka selanjutnya sistem ada men-*generate* kode OTP dari gabungan *email*, *password*, dan nomor *handphone* pengguna.
d. Output dari hasil *generate* tadi akan disimpan di *database* kemudian dikirimkan ke *Zenziva API Server* guna untuk dikirim ke nomor handphone pengguna.
e. Setelah kode *OTP* diterima, *Zenziva API Server* akan mengirimkan kode *OTP* ke nomor handphone pengguna.
f. Pengguna akan menerima *SMS* masuk berupa kode *OTP*.
g. Pengguna akan diarahkan ke form verifikasi kode *OTP* untuk diminta menginputkan kode *OTP* yang diterima dari *SMS*.
h. Kode *OTP* yang dikirimkan pengguna akan dicocokkan dengan kode *OTP* yang ada di *database*.
i. Kode *OTP* dinyatakan cocok maka pengguna akan diarahkan ke halaman utama (*dashboard*).

3.5.2 Data Flow Diagram Level 2

Pada diagram level 2 ini menggambarkan pecahan data dari *data flow diagram* level 1 dimana proses yang dijalankan adalah daftar, proses *login*, *zenziva API*, dan validasi *OTP*.

Berikut adalah *data flow diagram* level 2 yang penulis usulkan:



Gambar 3.6 Data Flow Diagram Level 2

Adapun penjelasan dari data flow diagram level 2 diatas adalah sebagai berikut :

a. Pengguna menginputkan data-data yang dibutuhkan untuk *registrasi* seperti nama depan, nama belakang, *email*, *username*, *password*, nomor *handphone*.

b. Sistem akan menginputkan data registrasi pengguna kedalam database MySQL.

c. Setelah registrasi dinyatakan sukses selanjutnya pengguna akan diarahkan ke halaman *login*.

d. Pengguna menginputkan data-data login seperti *username* dan *password*, pengguna juga bisa menggunakan *email* sebagai pengganti *username* pada saat *login*.

e. Sistem akan memvalidasi *username* dan *password* yang diinputkan pengguna pada saat *login* dan akan mencocokkan dengan data yang ada di dalam *database*.

f. Setelah validasi selesai dan data *login* cocok dengan ada yang ada di *database* kemudian sistem akan men-*generate* kode OTP menggunakan algoritma MD5 dengan menggabungkan *email*, *password*, dan nomor *handphone* pengguna.

g. Sistem akan mengirimkan *OTP* hasil enkripsi tersebut ke *server Zenziva* melalui teknologi API (*Application Programming Interfaces*).

h. *OTP* diterima oleh *Zenziva* dan setelah itu kode *OTP* akan dikirimkan kepada mengguna melalui *SMS*.

i. Pengguna menerima *SMS* masuk berisi kode *OTP*.

j. Pengguna akan diarahkan ke form verifikasi kode *OTP* untuk diminta menginputkan kode *OTP* yang diterima dari *SMS*.

k. Kode *OTP* yang dikirimkan pengguna akan dicocokkan dengan kode *OTP* yang ada di *database*.

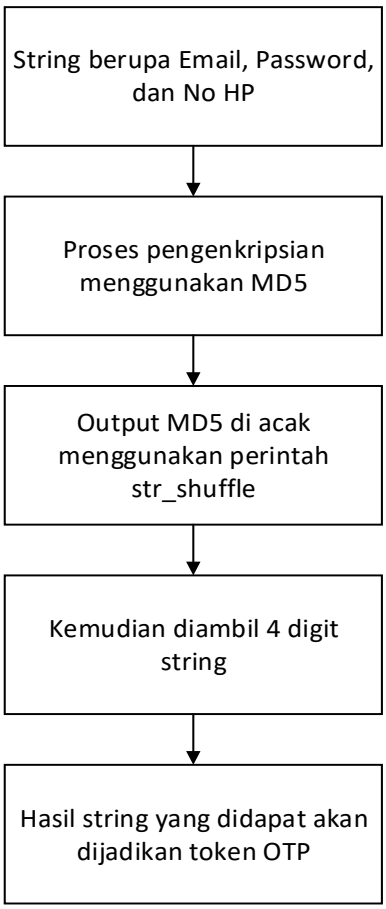
l. Kode *OTP* dinyatakan cocok maka pengguna akan diarahkan ke *dashboard*.

3.6 Flowchat Prosedur Enkripsi yang Diusulkan

Pesan awal atau Plainteks akan dienkripsi menggunakan algoritma One Time Password (OTP) sehingga menghasilkan *cipherteks*. *Chipertext* ini dihasilkan dari gabungan *email, password,* nomor *handphone* yang diambil dari *database. Email, password,* nomor *handphone* tersebut kemudian digabungkan menjadi satu *string* lalu dilakukan enkripsi MD5 pada *string* itu yang kemudian menghasilkan *output* berupa *hash MD5.*

Dari *hash* yang didapatkan tersebut diambil secara 6 karakter untuk yang nantinya akan digunakan sebagai kode *token* atau *One Time Password* (OTP) yang akan dikirimkan melalui SMS ke nomor *handphone* pemilik akun.

Berikut adalah gambaran prosedur enkripsi :

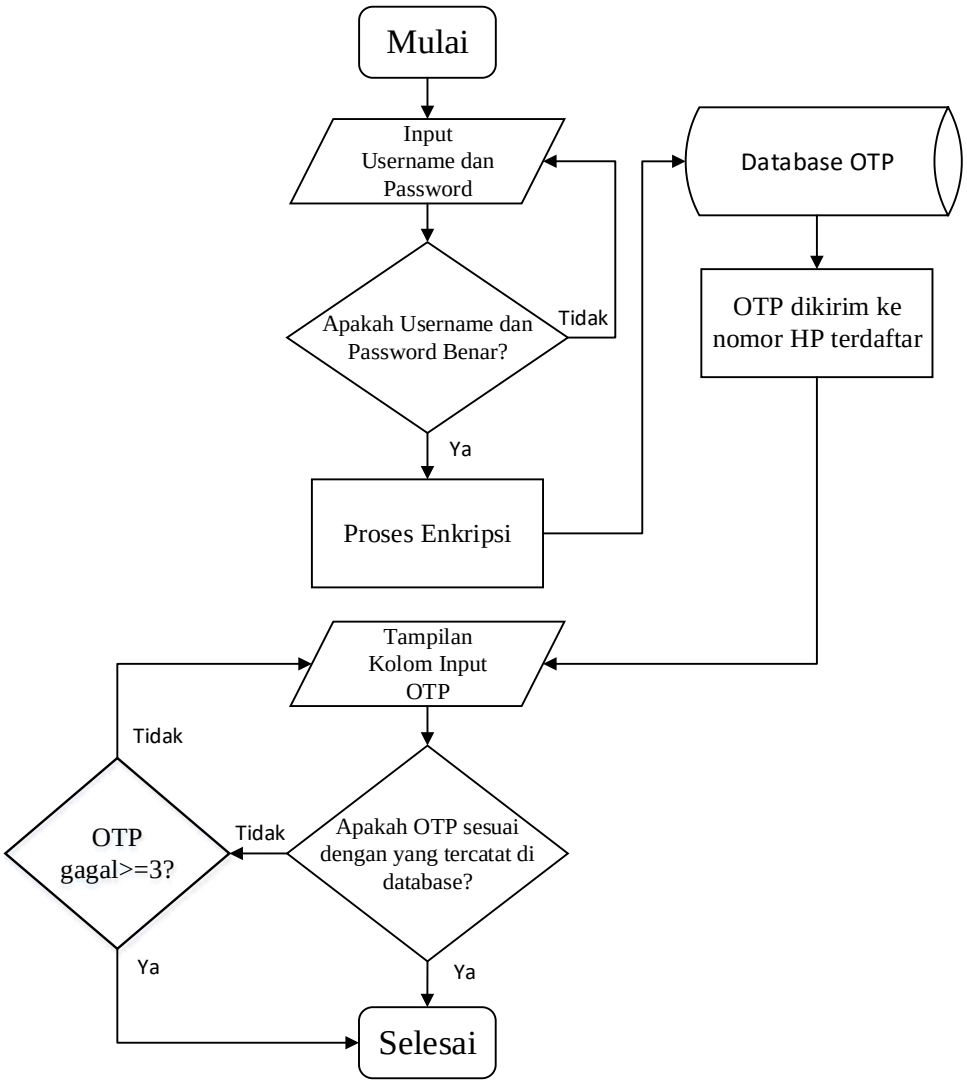


Gambar 3.7 Flowchart Prosedur Enkripsi

3.7 Flowchart Prosedur Sistem Login

Prosedur sistem loginnya yaitu pengguna menginputkan *username*/*email* dan *password* kemudian sistem akan mencocokkan dengan *username*/*email* dan password yang tercatat didalam *database MySQL*, setelah user diverifikasi oleh sistem maka *token* akan dikirimkan ke nomor ponsel akun terdaftar, lalu *token* itu digunakan sebagai *password* kedua untuk masuk kedalam sistem.

Berikut adalah flowchart prosedur sistem :

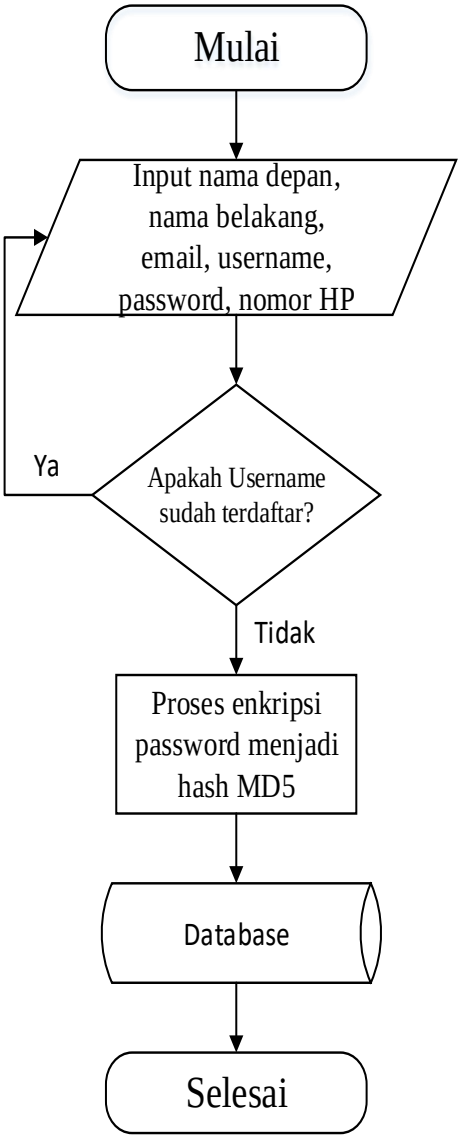


Gambar 3.8 Flowchart Prosedur Login

3.8 Flowchart Prosedur Registrasi

Prosedur sistem registrasinya yaitu pengguna menginputkan nama depan, nama belakang, *username*, *email* dan *password* dan nomor handphone kemudian setelah pengguna mengklik tombol submit maka sistem akan mengecek ketersediaan *username*, bila *username* yang diinputkan pengguna telah terdaftar maka pengguna akan ditampilkan kembali *form* registrasi, namun jika *username* tersedia dan dapat digunakan maka data yang diinputkan pengguna akan diinput

kedalam *database* dengan *password* yang diproses dahulu menjadi *hash MD5* guna untuk kepentingan keamanan. Berikut adalah *flowmap* prosedur sistem registrasi :



Gambar 3.9 Flowchart Prosedur Registrasi

3.9 Struktur Tabel

Berikut ini adalah struktur setiap tabel yang ada pada *database:*

3.9.1 Tabel *Member*

Fungsi : Untuk menyimpan data *Member* / User

Jumlah *Field* : 7

Primary Key : id (auto_increment)

Tabel data *member* ini menampung informasi tentang data *member* yang digunakan untuk proses *login* aplikasi. Hanya *member* yang memiliki *username* dan *password* yang bisa mengakses halaman ini. Berisi **id** (Primary Key) dengan tipe data integer, **namadepan** dengan tipe data varchar dan memiliki panjang 32 karakter, **namabelakang** dengan tipe data varchar dan memiliki panjang 32 karakter, **email** dengan tipe data varchar dan memiliki panjang 50 karakter, **username** dengan tipe data varchar dan memiliki panjang 32 karakter, **password** dengan tipe data varchar dan memiliki panjang 32 karakter, dan yang terakhir tipe data **nohp** dengan tipe data integer dan memiliki panjang 15 karakter.

Tabel 3.1 Tabel *member*

Nama Field	**Tipe Data**	**Panjang**	**Keterangan**
id	Integer	11	Kode User, Prymary Key
namadepan	Varchar	32	Nama Depan User
namabelakang	Varchar	32	Nama Belakang User
email	Varchar	50	Email User
username	Varchar	32	Nama Pengguna (Unix)
password	Varchar	32	Kata Sandi User
nohp	Integer	15	Nomor HP Pengguna

3.9.2 Tabel *Authentication*

Fungsi : Untuk menyimpan *token OTP*.

Jumlah *Field* : 5

Primary Key : id (auto_increment)

Tabel *authentication* ini menampung informasi tentang *token* OTP *(One Time Password)*. Berisi **id** dengan tipe data integer dan memiliki panjang 11 karakter, **otp** dengan tipe data varchar dan memiliki panjang 10, **expired** dengan tipe data varchar dan memiliki panjang 11 karakter, **created** dengan tipe data date time dan memiliki panjang 19 karakter, **nohp** dengan tipe data integer dan memiliki panjang 15 karakter.

Tabel 3.2 Tabel *authentication*

Nama Field	Tipe Data	Panjang	Keterangan
Id	Integer	11	Kode User, Prymary Key
otp	Varchar	10	Kode Token OTP
expired	Integer	11	Status OTP
created	Date Time	19	Tanggal dan waktu dibuat
nohp	Integer	15	Nama Pengguna (Unix)

3.9.3 Tabel *Status*

Fungsi : Untuk mencatat riwayat *login*.

Jumlah *Field* : 5

Primary Key : id (auto_increment)

Tabel *status* ini menampung informasi tentang riwayat login pengguna. Dimana pada tabel inilah riwayat login pengguna dicatat, fungsi utama tabel ini adalah untuk mencatat informasi berapa kali pengguna salah menginputkan token

OTP (*One Time Password*) yang nantinya akan dicatat pada kolom *login_attempt*. Pada kasus ini pengguna diberi batasan hingga 3 kali salah memasukkan OTP maka pengguna akan langsung diblokir oleh sistem selama 1 jam. Tabel *status* berisi **id** dengan tipe data integer dan memiliki panjang 11 karakter, **email** dengan tipe data varchar dan memiliki panjang 50, **ip** dengan tipe data varchar dan memiliki panjang 10 karakter, **login_attempt** dengan tipe data integer dan memiliki panjang 10 karakter, dan **timestamp** dengan tipe data integer.

Tabel 3.3 Tabel *status*

Nama Field	**Tipe Data**	**Panjang**	**Keterangan**
id	Integer	11	Kode User, Prymary Key
email	Varchar	50	Email User
ip	Varchar	10	Alamat IP User
login_attempt	Integer	10	Riwayat batasan login User
timestamp	Integer	15	Tanggal dan waktu dibuat

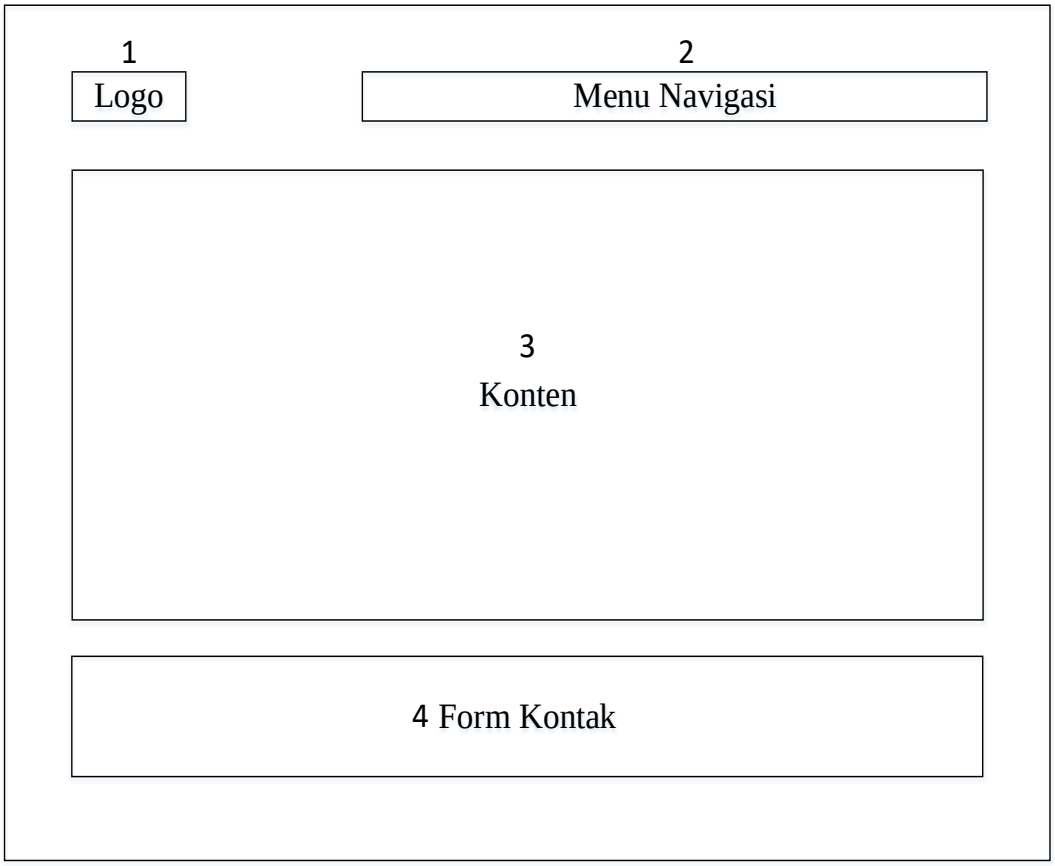
3.10 Rancangan Antarmuka Aplikasi

Perancangan Antarmuka meliputi perancangan struktur menu dan perancangan tampilan pada tampilan user.

3.10.1 Rancangan Tampilan Halaman Awal

Rancangan tampilan halaman utama dibagi menjadi empat bagian, di bagian atas terdapat header yang berisi logo dan menu navigasi, di bagian tengah terdapat area konten, sedangkan di bagian bawah terdapat area footer yang berupa form kontak.

Berikut adalah rancangan tampilan halaman awal:



Gambar 3.10 Rancangan Tampilan Halaman Awal

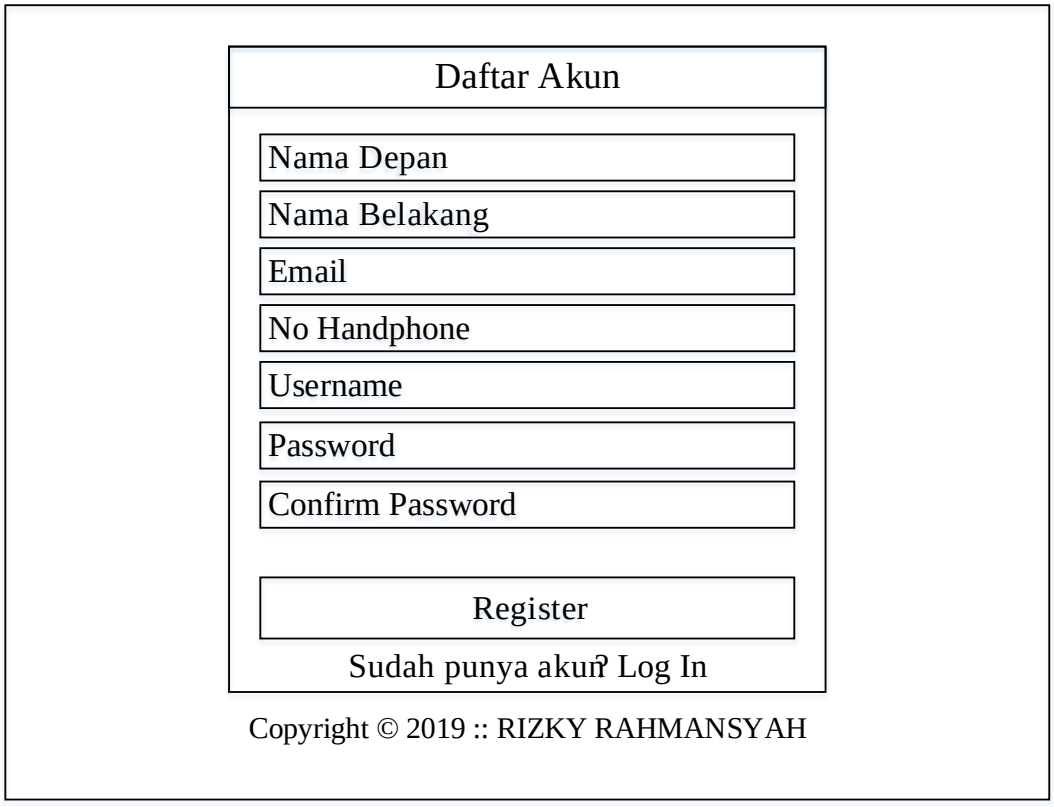
Keterangan :

1. Merupakan tempat penempatan logo website.
2. Merupakan tempat dimana menu navigasi akan dibuat, menu nasvigasi meliputi home, login, registrasi, contact form.
3. Tempat dimana penulis meletakkan konten-konten yang bertujuan memaparkan fitur-fitur dari website yang dibangun.
4. Tempat dimana alamat website serta tempat dimana pengguna dapat mengirimkan masukkan terkait website yang penulis bangun.

3.10.2 Rancangan Tampilan Form Registrasi

Rancangan Form Registrasi berfungsi bagi pengguna untuk mendaftarkan diri kedalam sistem informasi, pada tahapan ini pengguna diminta untuk menginputkan nama depan, nama belakang, email, username, password, dan nomor handphone. Setelah pengguna menginputkan data-data kemudian data-data itu akan disimpan kedalam database MySQL.

Berikut adalah rancangan form registrasi member:



Gambar 3.11 Rancangan Tampilan Form Registrasi

3.10.3 Rancangan Tampilan Form Login

Rancangan *Form Login* berfungsi bagi pengguna untuk masuk kedalam sistem informasi dengan cara memasukkan *username*/*email* atau *password*.

Setelah pengguna memasukkan *username* dan *password* maka nantinya pengguna akan diarahkan ke halaman verifikasi ke dua dengan cara menginputkan kode *token* yang dikirimkan ke nomor *handphone* pengguna.

Berikut adalah rancangan tampilan login:

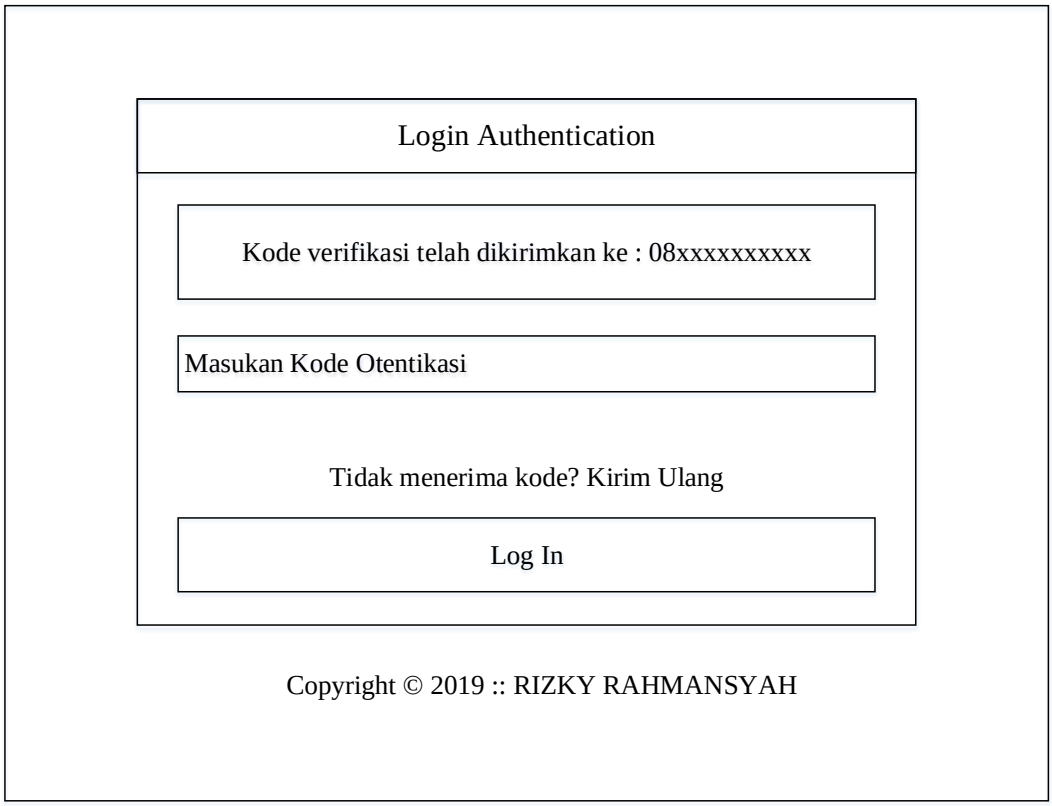
Gambar 3.12 Rancangan Tampilan Form Login

3.10.4 Rancangan Tampilan Form Input OTP

Rancangan form input OTP adalah sebuah tampilan antarmuka yang menampilkan kolom penginputan kode *token* OTP yang dikirimkan ke nomor *handphone.* Pada langkah ini pengguna diminta untuk memasukan kode *token* dan kemudian sistem aja mencocokkan dengan kode *token* yang ada di

database jika kode *token* sama dengan yang ada di *database* maka pengguna akan diarahkan ke tampilan selanjutnya.

Berikut adalah tampilan rancangan *form input* OTP:

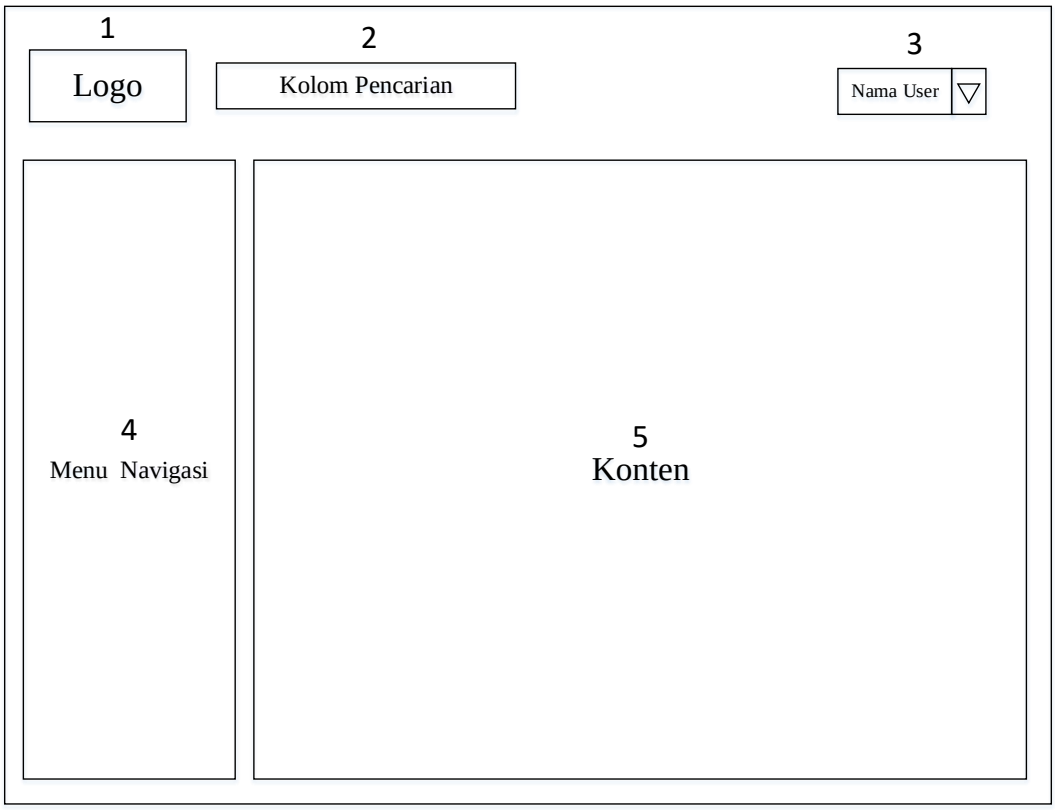


Gambar 3.13 Rancangan Tampilan Form Input OTP

3.10.5 Rancangan Tampilan Halaman Utama

Rancangan tampilan halaman utama ini adalah sebuah tampilan jika pengguna telah melewati proses verifikasi OTP dengan nomor ponsel maka pengguna akan diarahkan kehalaman utama ini. Halaman ini berisi tentang menu-menu yang terdapat pada website yang pengguna buat.

Berikut adalah rancangan tampilan halaman utama:



Gambar 3.14 Rancangan Tampilan Halaman Utama

Keterangan:

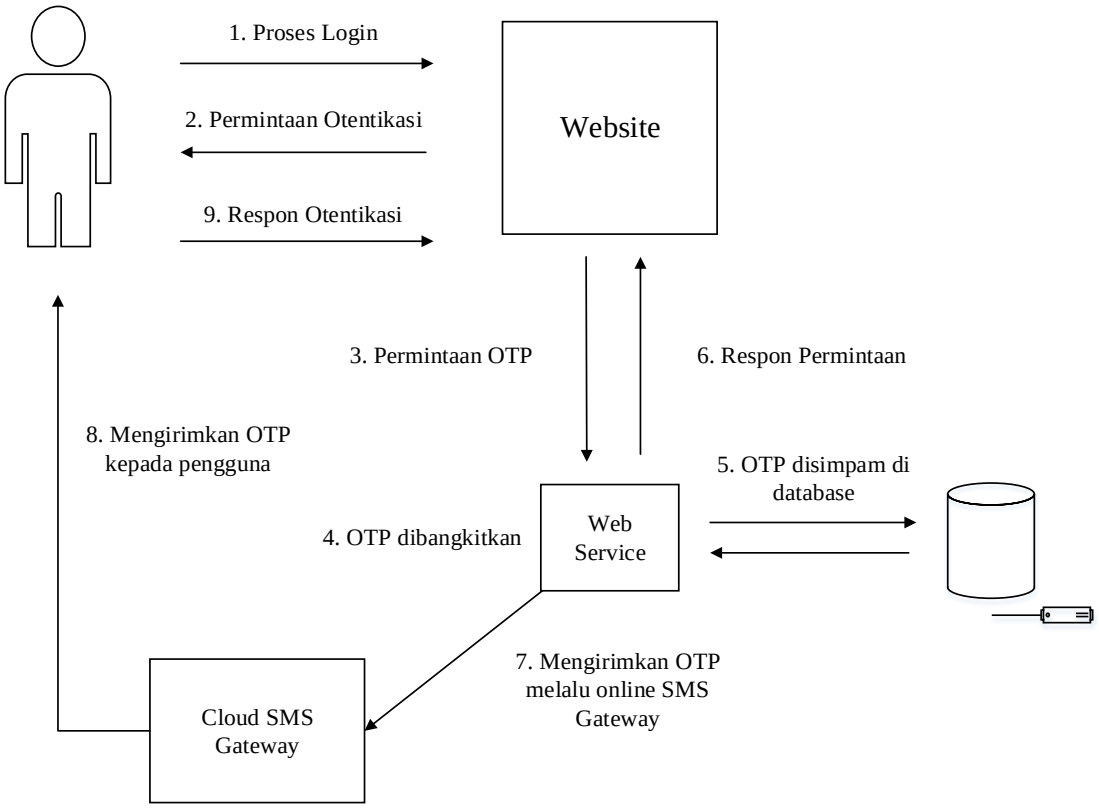
1. Merupakan penempatan logo website.
2. Kolom pencarian untuk mencari sebuah menu didalam halaman utama.
3. Merupakan menu *dropdown* yang berisi keteragan nama pengguna yang login.
4. Menu navigasi yang berisi tentang link-link fitur wesbsite yang dibangun.
5. Merupakan tempat konten utama website.

3.11 Arsitektur Rancangan

Pada tahapan ini dilakukan arsitektur perancangan dengan tujuan untuk mendefinisikan tujuan utama dari sistem keamanan yang dibangun yang

dibutuhkan untuk mendukung aplikasi dalam menangani data. Arsitektur rancangan ini akan menjelaskan secara umum bagaimana sebuah sistem keamanan menggunakan *One Time Password* berjalan.

Berikut ini adalah arsitektur rancangan dari sistem keamanan menggunakan *token One Time Password:*



Gambar 3.15 Arsitektur Rancangan

Keterangan :

1. Pengguna melakukan *login* mengguanakan alamat *email* dan kata sandi.
2. *Website* akan menampilkan halaman verifikasi *OTP* kepada pengguna.
3. Permintaan *OTP* ke *web service*.
4. *OTP* akan dibangkitkan.

5. Setelah *OTP* dibangkitkan maka *OTP* akan disimpan kedalam database *MySQL*.
6. Respon permintaan setelah pembangkitan *OTP*.
7. *OTP* yang berhasil dibangkitkan dan disimpan di-*database MySQL* akan dikirimkan ke penyedia *Cloud SMS Gateway* (*Zenziva*) melalui teknologi *API* (*Application Programming Interfaces*).
8. *OTP* diterima oleh penyedia *Cloud SMS Gateway* kemudian akan dikirimkan ke pengguna melalui *SMS*.
9. Pengguna menerima *SMS* yang berisi kode *OTP* kemudian merespon otentikasi dengan memasukkan kode *OTP* kedalam form verifikasi *OTP*.

BAB IV

HASIL DAN PEMBAHASAN

4.1 Implementasi Sistem

Dalam implemtasi sistem yang sudah dirancang, maka dibutuhkan beberapa perangkat yang sangat penting agar sistem yang sudah dirancang dapat berjalan pada saat diimplementasikan, berikut ini adalah beberapa perangkat yang dibutuhkan:

4.2.1 Spesifikasi Perangkat Lunak

Kebutuhan perangkat lunak merupakan faktor yang harus dipenuhi dalam penelitian ini, sehingga perangkat lunak tersebut sesuai dengan maksud dan tujuan dalam penelitian.

Perangkat lunak yang dibutuhkan dalam penelitian ini adalah sebagai berikut :

a. Sistem Operasi

   Sistem operasi yang dapat digunakan dalam penelitian ini adalah Windows 10 Home 64-bit. Alasan menggunakan sistem operasi ini adalah terdapat beberapa fitur yang dapat membantu penulis.

b. Notepad++

   Software ini digunakan sebagai *tool* untuk men-*coding* bahasa pemrograman yang penulis gunakan untuk merancang aplikasi.

c. Microsoft Office Word 2013

Software ini digunakan untuk menyusun laporan hasil dari penelitian. Proses penulisan menggunakan *Microsoft Office Word*, karena *software* tersebut sudah dikenal dan digunakan secara luas. *Microsoft Office Word* merupakan pengolah data yang dianjurkan sebagai spesifikasi minimal, karena ekstensi yang sering digunakan adalah format *.docx* dan *.doc* yang dapat dijalankan pada *software* ini.

d. Microsoft Visio 2013

Software ini digunakan untuk menyusun laporan hasil dari penelitian. Proses penulisan menggunakan *Microsoft Visio 2013*, karena *software* tersebut sudah dikenal dan digunakan secara luas. *Microsoft Visio 2013* merupakan aplikasi yang sering digunakan untuk membuat diagram, diagram alir (*flowchart*), dengam menggunakan *software* ini membuat diagram akan semakin mudah.

e. Browser

Aplikasi *browser* yang digunakan untuk menjalankan program ini adalah *Google Chrome*, dan aplikasi ini masih bisa berjalan dengan baik pada aplikasi browser lainnya seperti *Mozilla Firefox*, dan *Microsoft Edge*.

4.1.2 Spesifikasi Perangkat Keras

Perangkat keras juga dibutuhkan pada penelitian ini. Perangkat keras yang dibutuhkan dalam penelitian ini adalah laptop dengan spesifikasi berikut ini :

a. Processor : Intel Core i7-8750H @4.1 GHz

b. RAM : 8.00 GB DDR4

c. SSD : Adata XPG SX8200 PRO 256GB

d. Hardisk : 1 TB SSHD 7200RPM

e. Graphics : NVIDIA GEFORCE GTX 1050Ti

4.2 Tampilan Antar Muka

Implementasi antarmuka rancang bangun keamanan sistem informasi dengan autentikasi menggunakan identifikasi *one time password* berbasis *sms* dengan *hash md5* merupakan implementasi dari perancangan antarmuka yang telah dijelaskan pada bab sebelumnya dimana implementasi tersebut dapat dilihat pada gambar dibawah ini

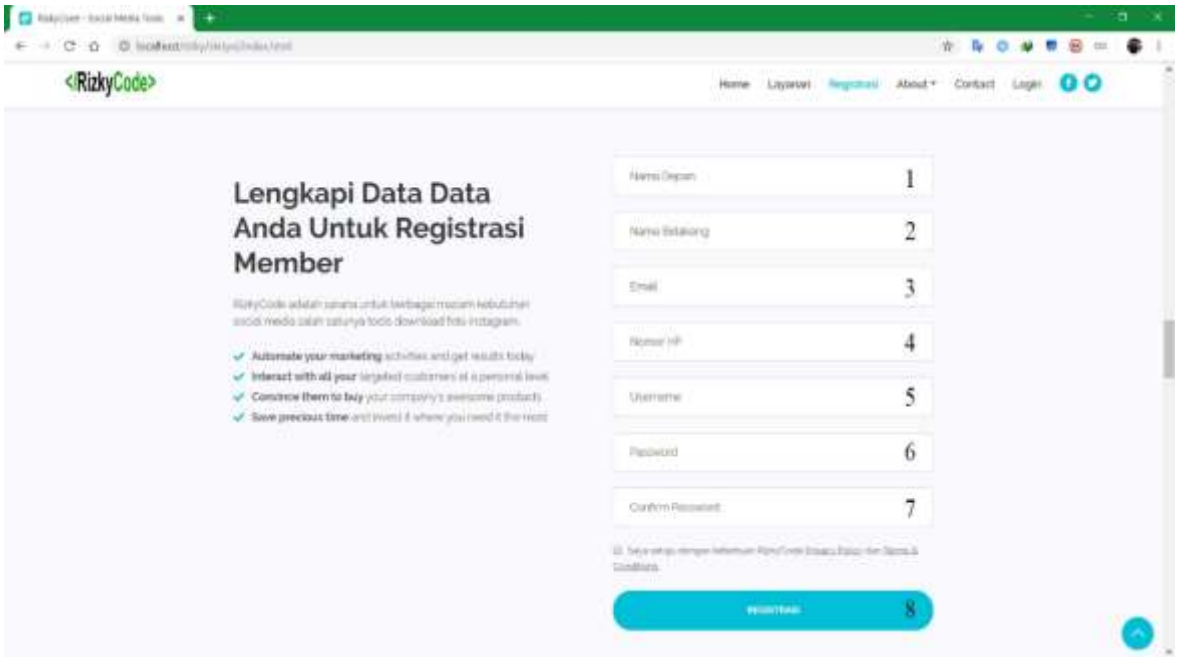
4.2.1 Tampilan Halaman Awal

Tampilan halaman awal merupakan tampilan yang pertama kali muncul ketika pengguna membuka suatu situs web. Pada tampilan ini penulis akan mempromosikan jasa maupun fitur-fitur dari website yang dibuat.

Gambar 4.1 Tampilan Halaman Awal

4.2.2 Tampilan Halaman Registrasi

Tampilan halaman registrasi merupakan tampilan dimana pengguna bisa mendaftarkan diri sebagai member suatu website.



Gambar 4.2 Tampilan Halaman Registrasi

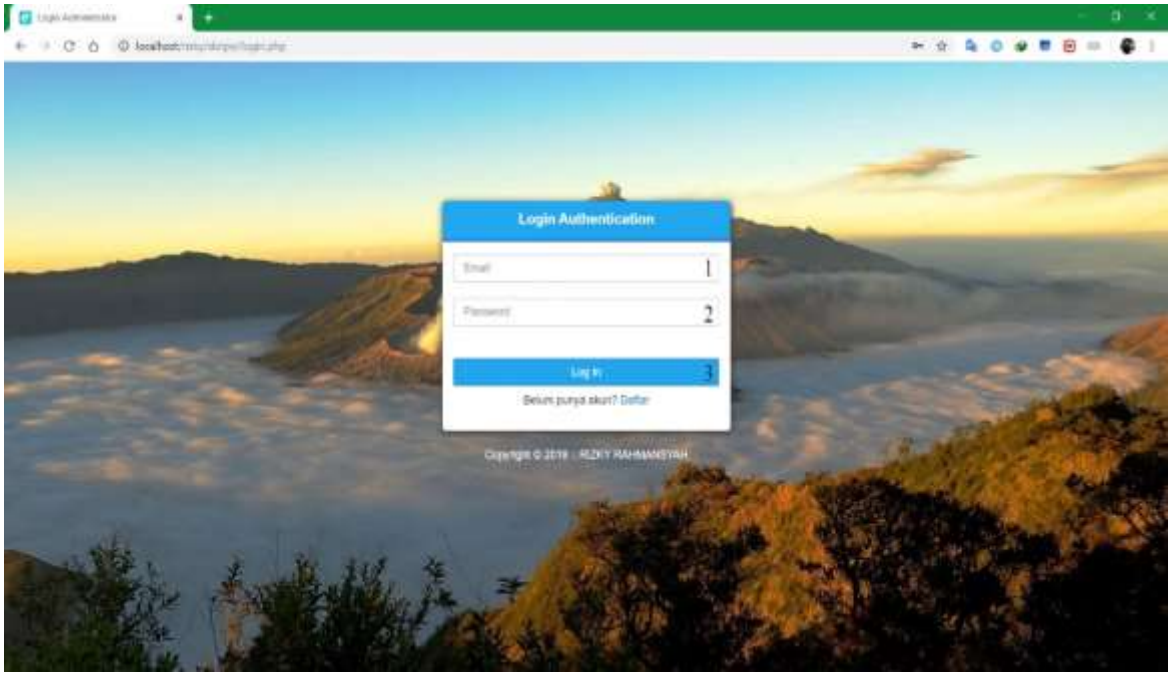
Keterangan:

1. Merupakan kolom *text area* dimana pengguna diwajibkan memasukkan nama depan.
2. Merupakan kolom *text area* dimana pengguna diwajibkan memasukkan nama belakang.
3. Merupakan kolom *text area* dimana pengguna diwajibkan memasukkan alamat *email* yang aktif, *email* ini nantinya akan digunakan sebagai identitas untuk *login* kedalam sistem.

4. Merupakan kolom *text area* dimana pengguna diwajibkan memasukkan nomor *handphone* yang aktif, nomor *handphone* ini nantinya akan digunakan sistem untuk mengirimkan kode *one time password (OTP).*
5. Merupakan kolom *text area* dimana pada kolom ini pengguna diwajibkan memasukkan nama pengguna atau *username*.
6. Merupakan kolom *text area* dimana pengguna dapat menginputkan *password* sebagai identitas ketika *login* kedalam sistem.
7. Tidak jauh berbeda dengan *text area* nomor 6, pada *text area* nomor 7 ini pengguna juga diwajibkan memasukkan *password* seperti pada nomor 6. Kolom ini hanya bertujuan untuk memastikan apakah pengguna telah memasukkan *password* dengan benar.
8. Apabila semua data-data yang dibutuhkan untuk registrasi maka pengguna diminta untuk menekan tombol registrasi.

4.2.3 Tampilan Halaman Login

Tampilan halaman login bisa diibaratkan pintu gerbang masuk kedalam sistem halaman *login* merupakan tampilan dimana pengguna dapat memasukkan data-data yang dibutuhkan untuk masuk kedalam sistem seperti *email* dan kata sandi.



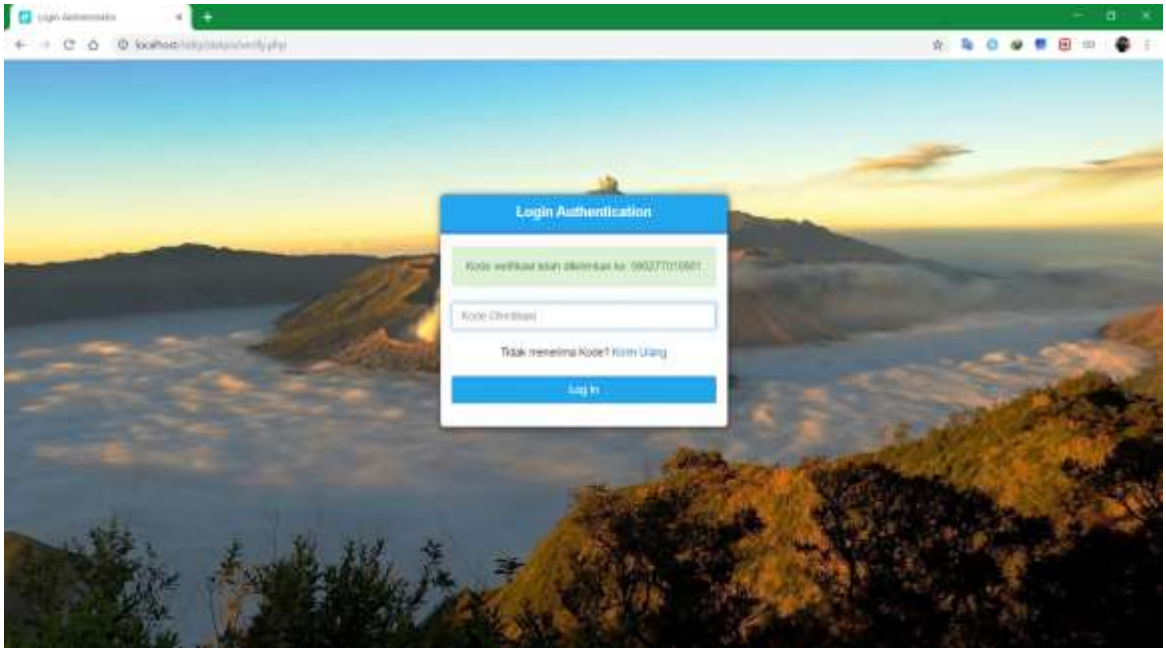
Gambar 4.3 Tampilan Halaman Login

Keterangan :

1. Merupakan *text area* dimana pengguna menginputkan *email* yang telah didaftarkan sebelumnya.
2. Merupakan *text area* dimana pengguna menginputkan *password* yang telah didaftarkan sebelumnya.
3. Merupakan sebuah tombol *login* yang berfungsi apabila pengguna telah menginputkan *email* dan *password*.

4.2.4 Tampilan Halaman Verifikasi *OTP*

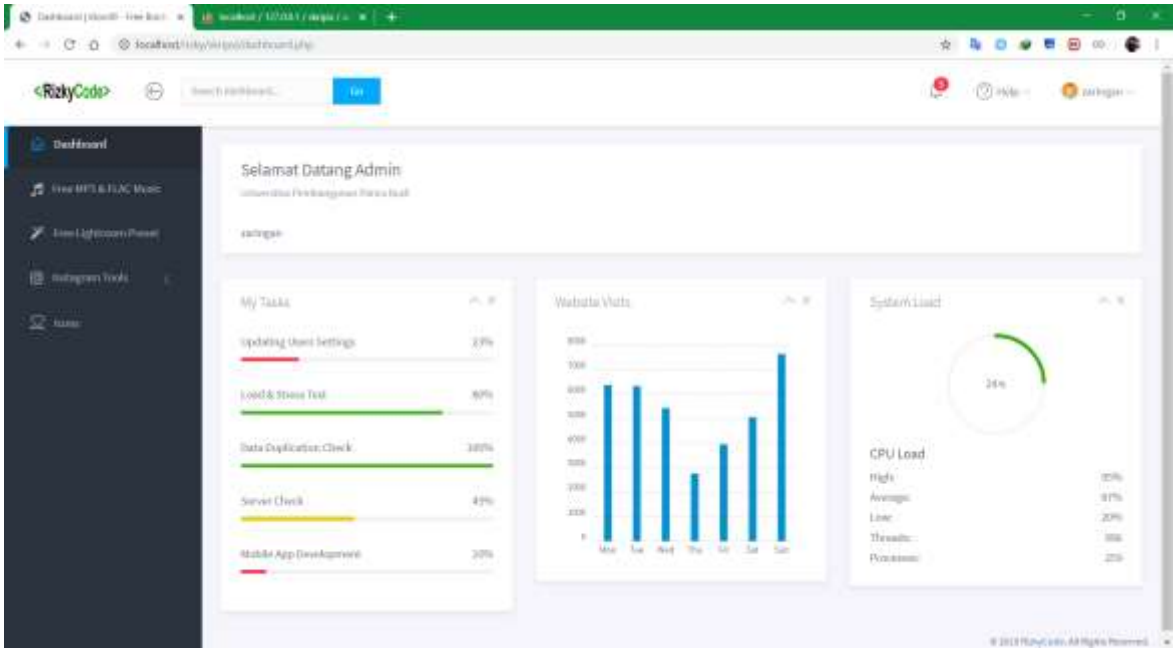
Tampilan halaman verifikasi *OTP* adalah tampilan yang muncul ketika pengguna telah melewati halaman *login*, pada saat ini pengguna diminta menginputkan kode *OTP* yang terkirim ke nomor handphone.



Gambar 4.4 Tampilan Halaman Verifikasi OTP

4.2.5 Tampilan Halaman Utama

Tampilan halaman utama merupakan sebuah halaman dimana pengguna telah sukses melewati halaman verifikasi *OTP*. Pada halaman ini berisi fitur-fitur dari sistem yang dibangun, pada saat ini penulis menyediakan fitur *instagram photo downloader*, dan beberapa menu lainnya.



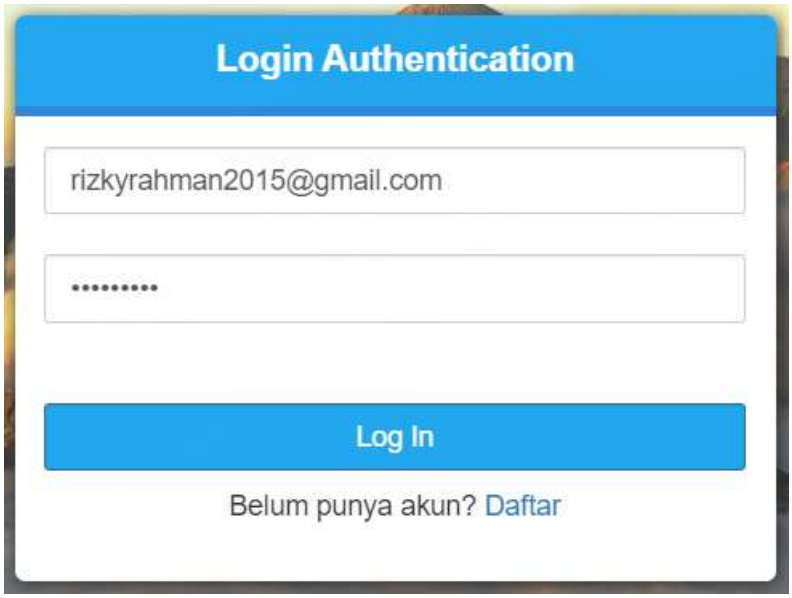
Gambar 4.5 Tampilan Halaman Utama

4.3 Pengujian Program

Pada tahapan ini penulis akan melakukan pengujian terhadap keamanan sistem informasi yang dibangun.

4.3.1 Pengujian Pada Halaman Login Website

Pada tahapan ini akan menggambarkan pengujian akses *login* menggunakan alamat *email* rizkyrahman2015@gmail.com dan *password* ***pancabudi***. Pada pengujian ini alamat *email* dan *password* yang dimasukkan pengguna ke halaman login sesuai dengan *email* dan *password* yang tertera didalam *database.* Login dinyatakan sukses dan pengguna akan dialihkan ke *form* verifikasi *OTP*.



Gambar 4.6 Tampilan Pengujian Login Website

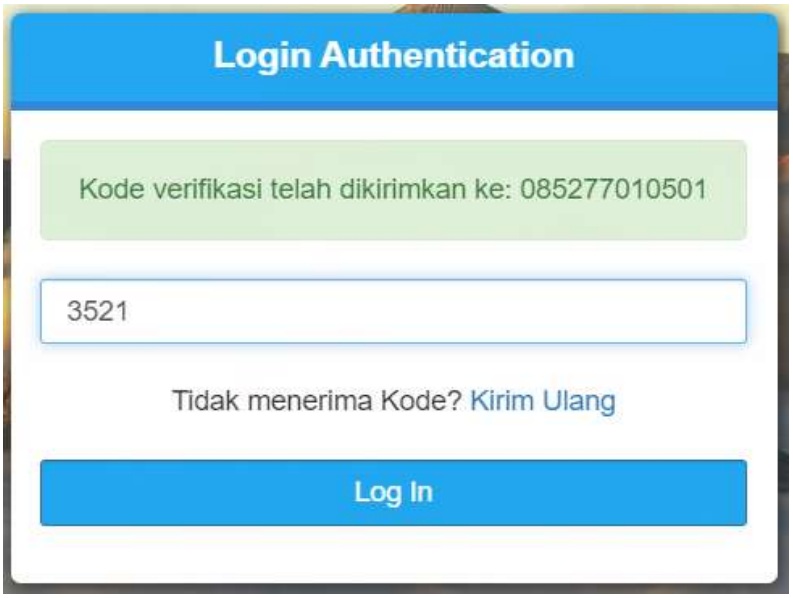
4.3.2 Pengujian Pada Pengiriman OTP Melalui SMS

Pada pengujian ini akan digambarkan tampilan isi SMS yang berisi kode OTP. Kode inilah yang nantinya dimasukkan kedalam form input OTP yang sudah dijelaskan pada Gambar 4.8.

Gambar 4.7 Tampilan Isi Pesan SMS

4.3.3 Pengujian Pada Halaman Verifikasi OTP

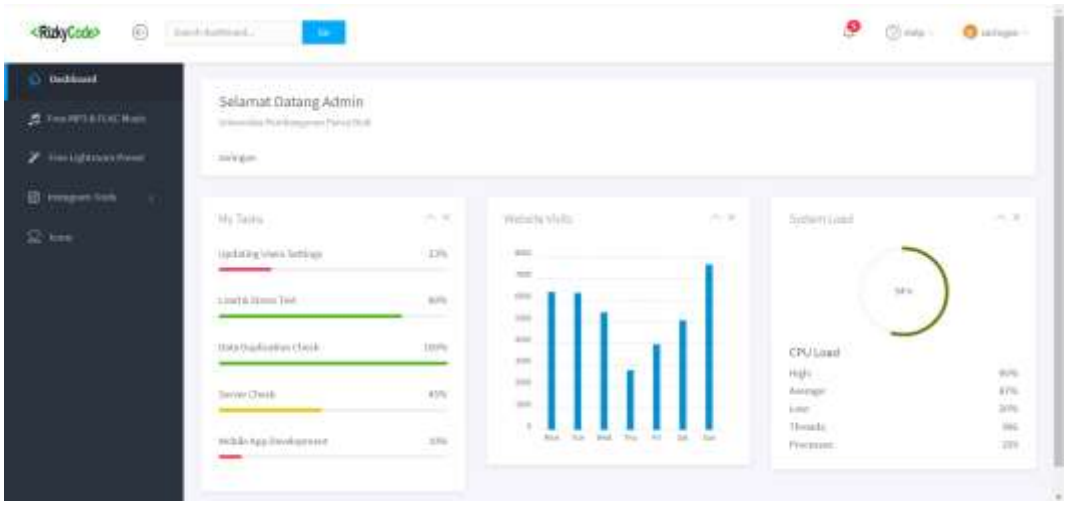
Pada pengujian ini memperlihatkan email dan password tersedia dan valid dalam database dan pengguna akan dialihkan ke form input OTP. Pada Gambar 4.6 berikut ini terdapat form input OTP, pengguna akan diminta untuk memasukkan kode OTP yang dikirimkan ke nomor ponsel. Pada pengujian ini kode OTP-nya adalah: 3521.



Gambar 4.8 Tampilan Halaman Verifikasi OTP

4.3.4 Tampilan Hasil Pengujian Halaman Utama Website

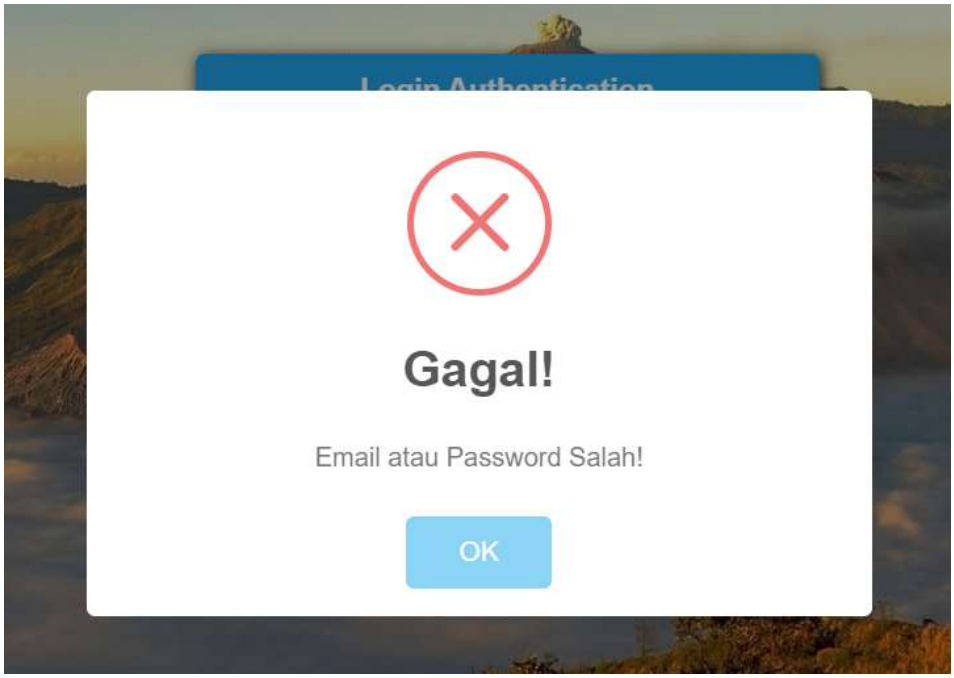
Pada Gambar 4.9 berikut ini membuktikan bahwa kode OTP yang terkirim melalui SMS singkron dengan kode OTP yang ada didalam database website.



Gambar 4.9 Tampilan *Website* Setelah berhasil *login* dengan kode OTP

4.3.5 Pengujian Data Login Email dan Password Salah

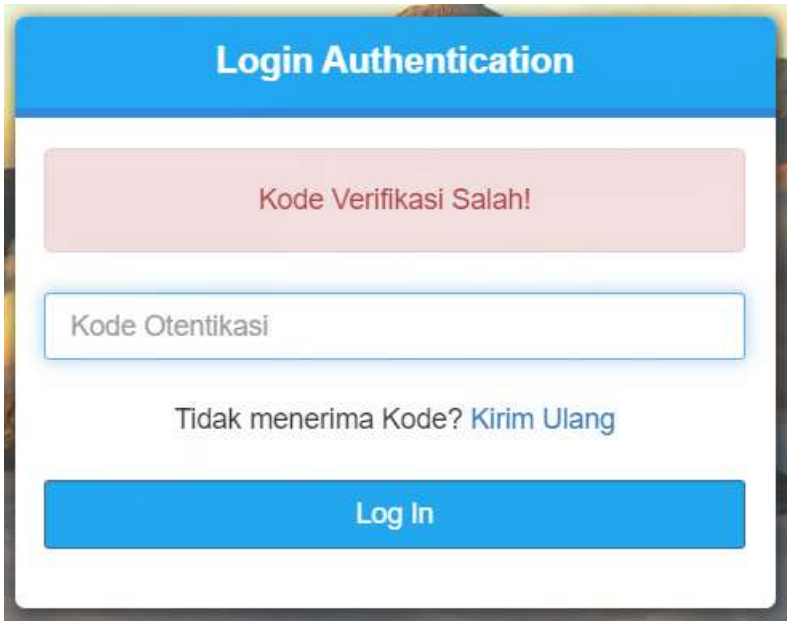
Pada Gambar 4.10 berikut ini akan muncul *popup* "Email atau Passowrd Salah!" ketika pengguna salah memasukkan *email* atau *password* pada halaman *login website*.



Gambar 4.10 Tampilan Ketika Email atau Password Salah

4.3.6 Pengujian Kode OTP Salah

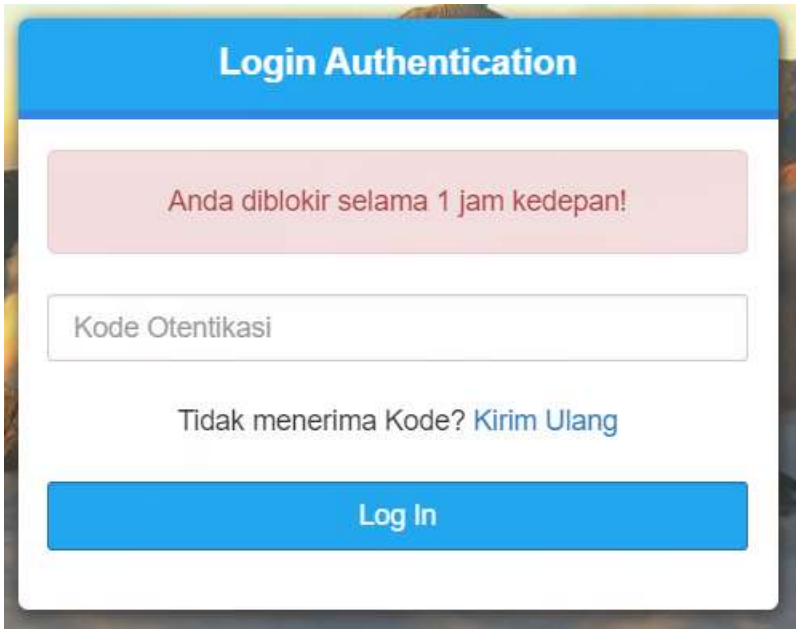
Pada Gambar 4.11 berikut ini akan muncul text notifikasi berwarna merah yang bertuliskan “Kode Verifikasi Salah!”. Notifikasi ini muncul apabila pengguna salah memasukkan kode OTP.



Gambar 4.11 Tampilan Ketika Kode Verifikasi Salah

4.3.7 Pengujian Pemblokiran Pengguna

Pada tahapan ini akan diuji memasukkan kode OTP yang salah sebanyak 3 kali maka akan muncul text notifikasi berwarna merah yang bertuliskan “Anda diblokir selama 1 jam kedepan!”. Pengguna akan diblokir dan tidak bisa login selama waktu yang telah ditentukan.



Gambar 4.12 Tampilan ketika pengguna diblokir

4.4 Kelebihan dan Kekurangan Sistem

4.4.1 Kelebihan Sistem

1. Aplikasi menggunakan enkripsi MD5 sehingga string yang sudah dienkripsi tidak dapat didekripsi oleh hacker.
2. Pengiriman kode *token* menggunakan teknologi *API* dari *zenziva* yaitu sebuah penyedia layanan *online SMS gateway* sehingga biaya operasional jauh lebih murah daripada menggunakan modem.
3. Dirancang menggunakan bahasa pemrograman PHP sehingga mempercepat pemrosesan data.

4.4.2 Kekurangan Sistem

1. Membutuhkan hosting karena sistem yang penulis rancang berbasis web, sehingga memerlukan biaya tambahan untuk menyewa hosting.
2. Waktu pengiriman yang sangat tergantung pada jaringan.

BAB V

PENUTUP

5.1 Kesimpulan

Kesimpulan yang didapatkan dari rancang bangun perangkat lunak ini adalah:

1. Konsep *One Time Password* dengan menggunakan *SMS Gateway* dapat diterapkan pada perbankkan, *payment account*, dan toko online dimana keamanan merupakan hal yang vital dibidang tersebut.
2. Konsep ini lebih aman daripada sistem login biasa dikarenakan *password* yang selalu berganti dan dikirimnya *password* melalui jaringan lain langsung kepada user. Kelemahan dari konsep ini terdapat pada waktu pengiriman yang sangat tergantung pada jaringan.
3. Hal yang perlu diperhatikan dalam penerapan konsep ini adalah *delay* antara saat pengguna meminta *password* dengan saat pengguna mendapatkan *password* via *SMS* (*Short Message Service*).

5.2 Saran

Saran dan perbaikkan dari pembangunan perangkat lunak ini adalah konsep ini dapat diterapkan menggunakan alat atau media lain untuk mempercepat waktu pengiriman (Contoh: *email*, alat khusus semacam *pager*, dan lainya).

DAFTAR PUSTAKA

Afrina, M., & Ibrahim, A. (2015). Pengembangan Sistem Informasi SMS Gateway Dalam Meningkatkan Layanan Komunikasi Sekitar Akademika Fakultas Ilmu Komputer Unsri. *Jurnal Sistem Informasi*, *7*(2), 852–864.

Aryza, S., Irwanto, M., Lubis, Z., Siahaan, A. P. U., Rahim, R., & Furqan, M. (2018). A Novelty Design Of Minimization Of Electrical Losses In A Vector Controlled Induction Machine Drive. In IOP Conference Series: Materials Science and Engineering (Vol.300, No. 1, p. 012067). IOP Publishing.

Agung, H., & Linda. (2016). *Aplikasi Laporan Keuangan Akuntansi Bulog-Jakarta Menggunakan Algoritma MD5 dan RSA*.

Agung, H., & Prasta, I. (2018). *Implementasi Algoritma Rivest , Shamir , Adleman Untuk File Sharing Pada PT . Sumber Makmur Pangan Sejahtera Berbasis Web*. *5*(2), 96–102.

Andrian, Yudhi, and Purwa Hasan Putra. "Analisis Penambahan Momentum Pada Proses Prediksi Curah Hujan Kota Medan Menggunakan Metode Backpropagation Neural Network." *Seminar Nasional Informatika (SNIf)*. Vol. 1. No. 1. 2017

Ariawan, J., & Wahyuni, S. (2015). Aplikasi Pengajuan Lembur Karyawan Berbasis Web. *Jurnal Algoritma Sekolah Tinggi Teknologi Garut*, *5*(1), 62–66.

Djahir, Y., & Pratita, D. (2014). Bahan Ajar Sistem Informasi Manajemen. In *Bahan Ajar Sistem Informasi Manajemen*. Bandung: Informatika.

Fachri, barany. Perancangan sistem informasi iklan produk halal mui berbasis mobile web menggunakan multimedia interaktif. Jurasik (jurnal riset sistem informasi dan teknik informatika), 2018, 3: 98-102.

Fachri, barany. "aplikasi perbaikan citra efek noise salt & papper menggunakan metode contraharmonic mean filter." seminar nasional royal (senar). Vol. 1. No. 1. 2018.

Ginting, G., Fadlina, M., Siahaan, A. P. U., & Rahim, R. (2017). Technical approach of TOPSIS in decision making. Int. J. Recent Trends Eng. Res, 3(8), 58-64.

HUTAHAEAN, J. (2017). Konsep Sistem Informasi. *Jurnal Administrasi Pendidikan*.

Indra permana, a. M. I. N. U. D. D. I. N. "sistem pakar mendeteksi hama dan penyakit tanaman kelapa sawit pada pt. Moeis kebun sipare-pare kabupaten batubara." (2013)

Madcoms. (2016a). *PEMROGRAMAN PHP dan MySQL untuk pemula*. Yogyakarta: Andi.

Madcoms. (2016b). *Sukses Membangun Toko Online dengan PHP & MySQL*. Yogyakarta: Andi.

Marshall B. Romney, & Steinbart, P. J. (2015). Accounting Information Systems 9th Edition. In *African Journal of Microbiology Research*. https://doi.org/10.5897/AJMR12.475

Mayasari, Nova. "Comparison of Support Vector Machine and Decision Tree in Predicting On-Time Graduation (Case Study: Universitas Pembangunan Panca Budi)." *Int. J.Recent Trends Eng. Res* 2.12 (2016): 140-151.

Mulyani, S. (2017). *Metode Analisis dan Perancangan Sistem*. Bandung: Abdi Sistematika.

Pabokory, F. N., Astuti, I. F., & Kridalaksana, A. H. (2016). Implementasi Kriptografi Pengamanan Data Pada Pesan Teks, Isi File Dokumen, Dan File Dokumen Menggunakan Algoritma Advanced Encryption Standard. *Informatika Mulawarman : Jurnal Ilmiah Ilmu Komputer*, *10*(1), 20. https://doi.org/10.30872/jim.v10i1.23

Puspita, Khairani, and Purwa Hasan Putra. "Penerapan Metode Simple Additive Weighting (SAW) Dalam Menentukan Pendirian Lokasi Gramedia Di Sumatera Utara." Seminar Nasional Teknologi Informasi Dan Multimedia, ISSN. 2015.

Putera, A., Siahaan, U., & Rahim, R. (2016). Dynamic key matrix of hill cipher using genetic algorithm. Int. J. Secur. Its Appl, 10(8), 173-180.

Raharjo, B., Heryanto, I., & Rosdiana. (2015). *Modul Pemrograman Web HTML, PHP & MySQL Revisi Kedua*. Bandung: Modula.

Rahman, F., & Santoso. (2015). Aplikasi pemesanan undangan online. *Aplikasi Pemesanan Undangan Online*, *1*(2), 78–87.

Rama, G. M., & Kak, A. (2015). Some structural measures of API usability. *Software - Practice and Experience*. https://doi.org/10.1002/spe.2215

Sakti, D. V. S. Y., Agani, N., & Hardjianto, M. (2016). Pengamanan Sistem Menggunakan One Time Password Dengan Pembangkit Password Hash SHA-256 dan Pseudo Random Number Generator (PRNG) Linear Congruential Generator (LCG) di Perangkat Berbasis Android. *Conference: Budi Luhur Information Technology, At Budi Luhur University, Volume: 13 No. 1*, *13*(1), 1–3.

Shalahuddin, M., & Sukamto, R. A. (2018). Rekayasa Perangkat Lunak Terstruktur dan Berorientasi Objek Edisi Revisi. In *Jurnal Pilar Nusa Mandiri*.

Suharyanto, C. E., Chandra, J. E., & Gunawan, F. E. (2017). Perancangan Sistem Informasi Penggajian Terintegrasi Berbasis Web (Studi Kasus di Rumah Sakit St. Elisabeth). *Jurnal Nasional Teknologi Dan Sistem Informasi*, *3*(2), 225–232. https://doi.org/10.25077/teknosi.v3i2.2017.225-232

Sukmaindrayana, A., & Sidik, R. (2017). Aplikasi Grosir Pada Toko Rsidik Bungursari Tasikmalaya. *Jurnal Manajemen Informatika*, *4*(2), 1–158. https://doi.org/10.1017/CBO9781107415324.004

Swara, G. Y., & Pebriadi, Y. (2016). REKAYASA PERANGKAT LUNAK PEMESANAN TIKET BIOSKOP BERBASIS WEB. *Jurnal TEKNOIF*, *4*(2), 27–39.

Umar, R., Riadi, I., & Handoyo, E. (2019). Analisis Keamanan Sistem Informasi Berdasarkan Framework COBIT 5 Menggunakan Capability Maturity Model Integration (CMMI). *JURNAL SISTEM INFORMASI BISNIS*. https://doi.org/10.21456/vol9iss1pp47-54

Wahyuni, Sri. "Implementasi Rapidminer Dalam Menganalisa Data Mahasiswa Drop Out." *Jurnal Abdi Ilmu* 10.2 (2018): 1899-1902