PROTOTYPE KEAMANAN LOGIN PAGE ADMIN MENGGUNAKAN TEKNIK OTP BERBASIS EMAIL

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 : **MUHAMMAD HAFIZH RINALDI**
NPM : **1614370281**
PROGRAM STUDI : **SISTEM KOMPUTER**

FAKULTAS SAINS DAN TEKNOLOGI
UNIVERSITAS PEMBANGUNAN PANCA BUDI
MEDAN
2020

LEMBAR PENGESAHAN

PROTOTYPE KEAMANAN *LOGIN PAGE* ADMIN MENGGUNAKAN TEKNIK OTP BERBASIS *EMAIL*

DISUSUN OLEH :

NAMA	**: MUHAMMAD HAFIZH RIŇALDI**
N.P.M	**: 1614370281**
PROGRAM STUDI	**: SISTEM KOMPUTER**

Skripsi Telah Disetujui oleh Dosen
Pembimbing Skripsi PadaTanggal
2020

Dosen Pembimbing I	**Dosen Pembimbing II**
Dian Kurnia, S.Kom., M.Kom	**Supiyandi, S.Kom., M.Kom**

Mengetahui,

Dekan Fakultas Sains Dan Teknologi	**Ketua Frogram Studi**
Hamdani, S.T., M.T	**Eko Hariyanto, S.Kom., M.Kom**

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*

ang bertanda tangan di bawah ini :

Lengkap	: Muhammad Hafizh Rinaldi
t/Tgl. Lahir	: MEDAN / 24 Desember 1998
Pokok Mahasiswa	: 1614370281
m Studi	: Sistem Komputer
trasi	: Keamanan Jaringan Komputer
Kredit yang telah dicapai	: 143 SKS, IPK 3.66
Hp	: 085230715707

ini mengajukan judul sesuai bidang ilmu sebagai berikut :

Judul
Pengamanan login page admin menggunakan notifikasi SMS pada website sekolah Rahmat Islamiyah0

Diisi Oleh Dosen Jika Ada Perubahan Judul

ype keamanan login page admin menggunakan teknik OTP berbasis email

ang Tidak Perlu

Rektor,

Cahyo Pramono, ST., MM

Medan, 19 Juni 2020
Pemohon,

(Muhammad Hafizh Rinaldi)

Tanggal : .....
Disahkan oleh :
Dekan

(Hamdani, ST., MT)

Tanggal : .....
Disetujui oleh :
Dosen Pembimbing I :

(Dian Kurnia, S.Kom., M.Kom)

Tanggal : .....
Disetujui oleh:
Ka. Prodi Sistem Komputer

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

Tanggal : .....
Disetujui oleh:
Dosen Pembimbing II:

(Supiyandi, S.Kom., M.Kom)

ermohonan Meja Hijau

Medan, 27 Agustus 2020
Kepada Yth : Bapak/Ibu Dekan
Fakultas SAINS & TEKNOLOGI
UNPAB Medan
Di -
Tempat

hormat, saya yang bertanda tangan di bawah ini :

	: Muhammad Hafizh Rinaldi
/Tgl. Lahir	: MEDAN / 24 DESEMBER 1998
rang Tua	: JHONI ROSADI
	: 1614370281
s	: SAINS & TEKNOLOGI
Studi	: Sistem Komputer
	: 081375836951
	: Jalan Bunga Teratai XVII No.7 Medan

bermohon kepada Bapak/Ibu untuk dapat diterima mengikuti Ujian Meja Hijau dengan judul **Pengamanan login page admin menggunakan notifikasi SMS pada website** Rahmat Islamiyah, Selanjutnya saya menyatakan :

Melampirkan KKM yang telah disahkan oleh Ka. Prodi dan Dekan
Tidak akan menuntut ujian perbaikan nilai mata kuliah untuk perbaikan indek prestasi (IP), dan mohon diterbitkan ijazahnya setelah lulus ujian meja hijau.
Telah tercap keterangan bebas pustaka
Terlampir surat keterangan bebas laboratorium
Terlampir pas photo untuk ijazah ukuran 4x6 = 5 lembar dan 3x4 = 5 lembar Hitam Putih
Terlampir foto copy STTB SLTA dilegalisir 1 (satu) lembar dan bagi mahasiswa yang lanjutan D3 ke S1 lampirkan ijazah dan transkipnya sebanyak 1 lembar.
Terlampir pelunasan kwintasi pembayaran uang kuliah berjalan dan wisuda sebanyak 1 lembar
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
Soft Copy Skripsi disimpan di CD sebanyak 2 disc (Sesuai dengan Judul Skripsinya)
Terlampir surat keterangan BKKOL (pada saat pengambilan ijazah)
Setelah menyelesaikan persyaratan point-point diatas berkas di masukan kedalam MAP
Bersedia melunaskan biaya-biaya uang dibebankan untuk memproses pelaksanaan ujian dimaksud, dengan perincian sbb :

1.	[102] Ujian Meja Hijau	: Rp.	
2.	[170] Administrasi Wisuda	: Rp.	
3.	[202] Bebas Pustaka	: Rp.	
4.	[221] Bebas LAB	: Rp.	
Total Biaya		**: Rp.**	**0**

Periode Wisuda Ke :

Ukuran Toga : S

hui/Disetujui oleh :

ni, ST., MT
Fakultas SAINS & TEKNOLOGI

Hormat saya

Muhammad Hafizh Rinaldi
1614370281

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.

SURAT PERNYATAAN

Saya Yang Bertanda Tangan Dibawah Ini :

Nama	:	Muhammad Hafizh Rinaldi
N. P. M	:	1614370281
Tempat/Tgl. Lahir	:	MEDAN / 24 DESEMBER 1998
Alamat	:	Jalan Bunga Teratai XVII No.7 Medan
No. HP	:	081375836951
Nama Orang Tua	:	JHONI ROSADI/RINI KUSRINI
Fakultas	:	SAINS & TEKNOLOGI
Program Studi	:	Sistem Komputer
Judul	:	Pengamanan login page admin menggunakan notifikasi SMS pada website sekolah Rahmat Islamiyah

Bersama dengan surat ini menyatakan dengan sebenar - benarnya bahwa data yang tertera diatas adalah sudah benar sesuai dengan ijazah pada pendidikan terakhir yang saya jalani. Maka dengan ini saya tidak akan melakukan penuntutan kepada UNPAB. Apabila ada kesalahan data pada ijazah saya.

Demikianlah surat pernyataan ini saya buat dengan sebenar - benarnya, tanpa ada paksaan dari pihak manapun dan dibuat dalam keadaan sadar. Jika terjadi kesalahan, Maka saya bersedia bertanggung jawab atas kelalaian saya.

Medan, 27 Agustus 2020

Pernyataan

Muhammad Harizh Rinaldi

1614370281

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

rsitas : Universitas Pembangunan Panca Budi
as : SAINS & TEKNOLOGI
n Pembimbing I : Dian Kurnia, S.Kom, M.Kom
n Pembimbing II : Supiyandi, S.Kom, M.Kom
Mahasiswa : MUHAMMAD HAFIZH RINALDI
an/Program Studi : Sistem Komputer
r Pokok Mahasiswa : 1614370281
g Pendidikan : Strata satu (S1)
Tugas Akhir/Skripsi : Pengamanan Login page admin menggunakan notifikasi SMS pada Website sekolah Rahmat Islamiyah.

NGGAL	PEMBAHASAN MATERI	PARAF	KETERANGAN
2.2019 .2020	· Acc Seminar Proposal Revisi Bab I & II by Email		

Medan, 03 Desember 2019
Diketahui/Disetujui oleh :
Dekan,

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

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

ersitas : Universitas Pembangunan Panca Budi
tas : SAINS & TEKNOLOGI
n Pembimbing I : Dian Kurnia S.Kom., M.Kom
n Pembimbing II : Supiyandi S.Kom., M.Kom
a Mahasiswa : MUHAMMAD HAFIZH RINALDI
an/Program Studi : Sistem Komputer
r Pokok Mahasiswa : 1614370281
ng Pendidikan : Strata satu (S1)
Tugas Akhir/Skripsi : Pengamanan Login page Admin Menggunakan notifikasi SMS pada Website sekolah Rahmat Islamiyah.

ANGGAL	PEMBAHASAN MATERI	PARAF	KETERANGAN
-12-2019	Acc bab 1		
-12-2019	~~perbaiki~~ lengkapi berkas seminar proposal		Acc seminar proposal
03-2020	perbaiki bab 2 tambahkan rumusnya lanjut bab 3		

Medan, 03 Desember 2019
Diketahui/Disetujui oleh :
Dekan,

UNIVERSITAS PEMBANGUNAN PANCA BUDI
UNPAB INDONESIA
FAKULTAS SAINS & TEKNOLOGI

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

ang tidak perlu

YAYASAN PROF. DR. H. KADIRUN YAHYA

UNIVERSITAS PEMBANGUNAN PANCA BUDI

JL. Jend. Gatot Subroto KM 4,5 PO. BOX 1099 Telp. 061-30106057 Fax. (061) 4514808
MEDAN - INDONESIA
Website : www.pancabudi.ac.id - Email : admin@pancabudi.ac.id

LEMBAR BUKTI BIMBINGAN SKRIPSI

swa : Muhammad Hafizh Rinaldi
: 1614370281
: Sistem Komputer
dikan : Strata Satu
mbing : Dian Kurnia, S.Kom., M.Kom
: Pengamanan login page admin menggunakan notifikasi SMS pada website sekolah Rahmat Islamiyah0

	Pembahasan Materi
	Baik, saya akan tinjau judul skripsi kamu kembali dan saya koordinasikan dengan pembimbing 2 kamu, segera saya kabarin kamu kembali
	Revisilah judul mu menjadi "Prototype keamanan page login website menggunakan teknik OTP berbasis email"
	lengkapi bab 3 kamu, buat keterangan lengkap antar muka aplikasi nya
	ACC Bab 3 lanjut Bab 4
	ACC Bab 4, *Lanjut Penulisan Kesimpulan dan Saran, lengkapi daftar pustaka*
	ACC Bab 5, Lengkapi berkas seminar hasil, ACC seminar Hasil
0	Lengkapi berkas meja hijau, Acc sidang

Medan, 26 Agustus 2020
Dosen Pembimbing,

Dian Kurnia, S.Kom., M.Kom

YAYASAN PROF. DR. H. KADIRUN YAHYA

UNIVERSITAS PEMBANGUNAN PANCA BUDI

Jl. Jend. Gatot Subroto KM 4,5 PO. BOX 1099 Telp. 061-30106057 Fax. (061) 4514808
MEDAN - INDONESIA
Website : www.pancabudi.ac.id - Email : admin@pancabudi.ac.id

LEMBAR BUKTI BIMBINGAN SKRIPSI

iswa : Muhammad Hafizh Rinaldi
: 1614370281
di : Sistem Komputer
didikan : Strata Satu
mbing : Supiyandi, S.Kom., M.Kom
: Pengamanan login page admin menggunakan notifikasi SMS pada website sekolah Rahmat Islamiyah0

	Pembahasan Materi
	Apa yang mau di tinjau kembali ya.. apabila Doping 1 sudah ACC . Silahkan lanjutkan...terimakasih...
	- Bab 1 dan 2 masih kosong..tidak ada Teks apa yang mau diperiksa - Bab 3 untuk diagram dan tabel jangan di buat berwarna - Teks yang asing (Inggris) harus di cetak miring
	Lanjutkan BAB IV dan V sekalian lengkapi keseluruhan
	ACC Seminar Hasil
20	Lengkapi Berkas, ACC Sidang Meja Hijau.

Medan, 26 Agustus 2020
Dosen Pembimbing,

Supiyandi, S.Kom., M.Kom

SURAT KETERANGAN PLAGIAT CHECKER

ni saya Ka.LPMU UNPAB menerangkan bahwa saurat ini adalah bukti pengesahan
IU sebagi pengesah proses plagiat checker Tugas Akhir/ Skripsi/Tesis selama masa
Covid-19 sesuai dengan edaran rektor Nomor : 7594/13/R/2020 Tentang
huan Perpanjangan PBM Online.

disampaikan.

a penyalahgunaan/pelanggaran atas surat ini akan di proses sesuai ketentuan yang
ku UNPAB.

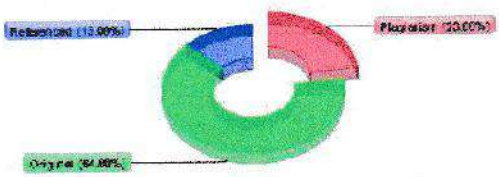
Ka.LPMU

Cahyo Pramono, SE.,MM

Plagiarism Detector v. 1460 - Originality Report 27-Aug-20 08:07:19

MUHAMMAD HAFIZH RINALDI_1614370281_SISTEM KOMPUTER.docx Universitas Pembangunan Panca Budi_License03

Comparison Preset: Rewrite. Detected language: Indonesian



[Show other Sources]

133 - Ok / 28 - Failed

[Show other Sources]

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
Nomor. 1393/BL/LAKO/2022

tanda tangan dibawah ini Ka. Laboratorium Komputer dengan ini menerangkan bahwa :

	: Muhammad Hafizh Rinaldi
	: 1614370281
t/Semester	: Akhir
is	: SAINS & TEKNOLOGI
n/Prodi	: Sistem Komputer

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

Medan, 27 Agustus 2020
Ka. Laboratorium

Fachrid Wadly, S. Kom., M.Kom.

men : FM-LAKO-06-01	Revisi : 01	Tgl. Efektif : 04 Juni 2015

YAYASAN PROF. DR. H. KADIRUN YAHYA
PERPUSTAKAAN UNIVERSITAS PEMBANGUNAN PANCA BUDI
Jl. Jend. Gatot Subroto KM. 4,5 Medan Sunggal, Kota Medan Kode Pos 20122

SURAT BEBAS PUSTAKA
NOMOR: 2932/PERP/BP/2020

erpustakaan Universitas Pembangunan Panca Budi menerangkan bahwa berdasarkan data pengguna perpustakaan
a saudara/i:

: Muhammad Hafizh Rinaldi
: 1614370281
Semester : Akhir
: SAINS & TEKNOLOGI
Prodi : Sistem Komputer

nnya terhitung sejak tanggal 27 Agustus 2020, dinyatakan tidak memiliki tanggungan dan atau pinjaman buku
tidak lagi terdaftar sebagai anggota Perpustakaan Universitas Pembangunan Panca Budi Medan.

Medan, 27 Agustus 2020
Diketahui oleh,
Kepala Perpustakaan,

UNPAB INDONESIA

Sugiarjo, S.Sos., S.Pd.I

SURAT PERNYATAAN

Saya yang bertanda tangan dibawah ini :

Nama : **MUHAMMAD HAFIZH RINALDI**

NPM : **1614370281**

Fakultas : SAINS DAN TEKNOLOGI

Program Studi : SISTEM KOMPUTER

Judul Skripsi **PROTOTYPE KEAMANAN LOGIN PAGE ADMIN MENGGUNAKAN TEKNIK OTP BERBASIS EMAIL**

Dengan Ini Menyatakan Bahwa :

1. Skripsi Ini Merupakan Hasil Karya Tulis Saya Sendiri Dan Bukan Merupakan Hasil Karya Orang Lain (Plagiat).
2. Skripsi Saya Bersedia Dipulikasikan Oleh Lembaga
3. Terdapat Revisi/Perbaikan Dalam Skripsi Saya.

Demikian Surat Pernyataan Ini Saya Buat Untuk Memenuhi Persyaratan Pengambilan Hasil Plagiat Cheker Saya, Atas Perhatiannya Saya Ucapkan Terimakasih.

Medan, 27 Agustus 2020

Pernyataan

Muhammad Hafizh Rinaldi

1614370281

ABSTRAK

MUHAMMAD HAFIZH RINALDI

PROTOTYPE KEAMANAN *LOGIN PAGE ADMIN* MENGGUNAKAN TEKNIK OTP BERBASIS *EMAIL*

Keamanan jaringan merupakan suatu tindakan yang berhubungan dengan deteksi dan pencegahan terhadap tindakan yang merugikan. Demi keamanan sebuah jaringan komputer, maka dibutuhkan sebuah sistem yang dapat memberikan peringatan dini terhadap tindak penyusupan yang dilakukan pengguna yang tidak bertanggung jawab.Dalam keamanan *Login Page Admin*masih secara manualdan membutuhkan waktu yang cukup lama. Sehingga dengan menggunakan teknik OTP berbasis *email* dapat mempermudah pihak pengguna untuk lebih cepat *login* kedalam *website* tersebut.

Pembuatan sistem dilakukan dengan cara membuka halaman *admin* pada *prototype website* yang di bangun, user memasukkan kode OTP yang dikirim ke *emailadmin* yang didapat dari *website prototype*. Setelah user memasukkan *username* dan *password*, maka kode OTP akan dikirim ke *email admin*, kemudian kode dimasukkan ke halaman *login web prototype* untuk masuk ke halaman admin *prototype website* dan akan diproses oleh sistem untuk menentukan informasi apa yang diperlukan admin.

Hasil penelitian ini menunjukkan bahwa sistem *prototype Login* dengan pengamanan OTP berbasis *website* berjalan sesuai dengan algoritma yang dirancang, danpengiriman kode OTP dilakukan menggunakan *email*ke *email admin* yang mengakses *login* portal *admin*, dengan syarat *email* yang diinputkan sesuai dengan *email* yang terdaftar pada *databasesystem*.

Kata Kunci :*Keamanan Jaringan,Login Page, Notifikasi Email,.*

ABSTRACT

MUHAMMAD HAFIZH RINALDI

PROTOTYPE SECURITY LOGIN PAGE ADMIN USING EMAIL-BASED OTP

Network security is an action related to detection and prevention of harmful actions. For the security of a computer network, we need a system that can provide early warning of intrusions by irresponsible users. In security, Admin Login Page is still manual and takes a long time. So that using the email-based OTP technique can make it easier for users to log into the website more quickly.

Making the system is done by opening the admin page on the prototype website that is built, the user enters the OTP code which is sent to the admin email which is obtained from the prototype website. After the user enters the username and password, the OTP code will be sent to the admin email, then the code is entered into the prototype web login page to enter the website prototype admin page and will be processed by the system to determine what information the admin needs.

The results of this study indicate that the login prototype system with website-based OTP security runs according to the designed algorithm, and the sending of the OTP code is carried out using an email to the admin email who accesses the admin portal login, provided that the email entered is in accordance with the email registered in the database system.

Keywords: *Network Security, Login Page, Email Notification,*

KATA PENGANTAR

بِسْمِ اللَّهِ الرَّحْمَٰنِ الرَّحِيمِ

يَٰٓأَيُّهَا ٱلَّذِينَ ءَامَنُواْ هَلۡ أَدُلُّكُمۡ عَلَىٰ تِجَٰرَةٖ تُنجِيكُم مِّنۡ عَذَابٍ أَلِيمٖ ۝ تُؤۡمِنُونَ بِٱللَّهِ وَرَسُولِهِۦ وَتُجَٰهِدُونَ فِي سَبِيلِ ٱللَّهِ بِأَمۡوَٰلِكُمۡ وَأَنفُسِكُمۡۚ ذَٰلِكُمۡ خَيۡرٞ لَّكُمۡ إِن كُنتُمۡ تَعۡلَمُونَ ۝

Artinya:Hai orang-orang yang beriman, sukakah kamu aku tunjukkan suatu perniagaan yang dapat menyelamatkan kamu dari azab yang pedih? (Yaitu) kamu beriman kepada Allah dan Rasul-Nya dan berjihad di jalan Allah dengan harta dan jiwamu. Itulah yang lebih baik bagi kamu jika kamu mengetahui.**(QS. Ash-Shaff : 10 – 11)**

Syukur Alhamdulillah penulis ucapkan kehadirat Allah SWT yang senantiasa melimpahkan rahmat dan hidayah-Nya sehingga dapat menyelesaikan penulisan skripsi dengan judul **Prototype Keamanan Page Login Website Menggunakan Teknik OTP Berbasis Email.** Skripsi ini diajukan sebagai salah satu syarat memperoleh gelar sarjana Komputer di Program Studi Sistem Komputer Universitas Pembangunan Pancabudi.

Pada kesempatan ini penulis mengucapkan terima kasih yang sebesar-besarnya kepada Orang Tua, Bapak Jhoni Rosadi dan Ibu Rini Kusrini yang sangat penulis sayangi dengan tulus dan ikhlas memberikan kasih sayang serta senantiasa memberikan motivasi, bimbingan, doa dan nasehat selama ini sehingga penulis dapat menyelesaikan skripsi ini.

Penulis juga menyampaikan terima kasih yang sebesar besarnya kepada Bapak Dian Kurnia, S.Kom., M.Kom selaku Dosen Pembimbing I, Bapak

Supiyandi, S.Kom., M.Kom selaku Dosen Pembimbing II, dan Bapak Eko Hariyanto, S,Kom., M.Kom selaku Penguji skripsi yang telah banyak memberikan masukan, saran, bimbingan selama skripsi ini selesai.

Pada kesempatan ini penulis juga mengucapkan terima kasih yang sebesar besarnya kepada:

1. Bapak Dr. H. Muhammad Isa Indrawan, SE.,MM selaku rektor Universitas Pembangunan Panca Budi Medan.
2. Ibu Sri Shindi Indira, ST., M.Sc selaku Dekan Fakultas Sains & Teknologi Universitas Pembangunan Panca Budi Medan.
3. Bapak Eko Hariyanto, S,Kom., M.Kom selaku Ketua Program Studi Sistem Komputer Fakultas Sains & Teknologi Universitas Pembangunan Pancabudi.
4. Bapak / Ibu Staff pengajar Program Studi Sistem Komputer Fakultas Sains & Teknologi Universitas Pembangunan Pancabudi.
5. Penulis juga mengucapkan terima kasih Adik Ahmad Fadhil, sepupu Nur Kartika, partner berjuang Inggit Dayu Ramadhan S.Farm, sahabat-sahabat Hafni Fadhillah, Rahmawati, Nur Indahyani, Mriki Surya Ningrad, Ahmad Karel, Fauzi Syahputra, Muhammad Budi, Irwansyah putra, Kristiansyah, Alpi suhri, Febri, Aseng, Julian, Noel dan teman-teman seperjuangan stambuk 2016 lainnya, terima kasih telah membantu dan memberikan semangat selama penyusunan skripsi ini.

Penulis menyadari bahwa skripsi ini masih banyak kekurangan, oleh karena itu dengan segala kerendahan hati, penulis menerima kritik dan saran yang bersifat membangun demi kesempurnaan skripsi ini.

Akhirnya penulis ucapkan terima kasih kepada semua pihak yang telah membantu yang tidak disebutkan satu persatu dalam penulisan skripsi ini. Semoga skripsi ini bermanfaat bagi ilmu pengetahuan pada umumnya dan bidang Sistem Komputer khususnya.

Medan, 2020

Muhammad Hafizh Rinaldi
NPM. 1614370281

DAFTAR ISI

Halaman

DAFTAR GAMBAR

Halaman

DAFTAR TABEL

BAB I

PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi terutama di bidang jaringan komputer dan internet berkembang sangat pesat. Komputer yang dulu bersifat bediri sendiri, sekarang sudah jarang ditemukan. Kebutuhan akan transfer data yang cepat dan praktis membuat jaringan komputer sangat dibutuhan. Hal ini mengakibatkan berbagai macam resiko terutama dalam bidang keamanan jaringan komputer.

Keamanan jaringan merupakan suatu tindakan yang berhubungan dengan deteksi dan pencegahan terhadap tindakan yang merugikan. Pada tahun 2014, kejahatan pada bidang jaringan komputer di Indonesia mencapai angka 48,4 juta. Seorang administrator bertugas untuk mengelola dan menjamin bahwa jaringan komputer yangdijaga terhindar dari tindakan penyusupan serta menjamin ketersediaan layanan bagi penggunanya. Kendala yang dialami oleh administrator adalah tindakan penyusupan yang terjadi kapan saja, bila administrator tidak segera melakukan tindak pencegahan karena telat mendeteksi penyerangan maka dapat berakibat fatal. Demi keamanan jaringan komputer, maka dibutuhkan sistem yang dapat memberikan peringatan dini terhadap tindak penyusupan yang dilakukan pengguna yang tidak bertanggung jawab(Radhito et al., 2019)

Pada umumnya sebuah aplikasi berbasis web tidak mempunyai fasilitas notifikasi atau pemberitahuan terbaru kepada pengguna, sehingga proses penyampaian informasi terutama informasi penting tidak diketahui secara langsung. Hal tersebut tentunya menjadi permasalahan, terutama pada sistem

Login Page Admin pada *website*. Jika tidak segera diamankan *Login Page Admin* terhadap maka kondisi server dan jaringan dapat terganggu. Permasalahan tersebut dapat diatasi dengan menerapkan sistem notifikasi*email* secara otomatis tanpa harus membuka dan memperhatikan aplikasi terus menerus. Teknik dalam penyajian data secara realtime yang telah dilakukan pada aplikasi *web* dapat menggunakan notifikasi *Email*(Rahmatulloh et al., 2019).

Di era globalisasi saat ini banyak orang yang menggunakan *email* untuk berkomunikasi, setiap orang yang memiliki minimal satu akun *email* atau bahkan beberapa akun dibeberapa fasilitas penyedia *email*. *Email* bukan sekedar pengganti surat menyurat konvensional, namun banyak sekali manfaat yang dihasilkan. *Elektronic Mail* atau popular disebut *email* adalah perangkat lunak sistem korespondensi antara satu komputer dengan komputer lain dengan menggunakan sistem jaringan komputer atau internet. Di era modern dan serba teknologi sekarang ini, keberadaan *email* adalah suatu hal yang sangat penting. Hampir seluruh kegiatan, seperti pertemuan diskusi, menyebar surat undangan dapat dilakukan dimana saja dan kapan saja dalam satu waktu dan virtual, yaitu dengan memanfaatkan jaringan internet.*Email* sangat mendukung proses-proses komunikasi, kolaborasi, dan kordinasi secara elektronis dalam satu waktu.

Penggunaan *email* sebagai komunikasi formal secara individual ataupun secara kelompok terbukti efektifdapat memangkas biaya-biaya seperti transportasi, sewa ruangan, komunikasi dan penginapan (untuk kegiatan rapat). Keamanan *email* harus direncanakan dan dikoordinasikan dengan baik agar dapat melindungi sumber daya *(resource)* dan investasi di dalamnya(Ismaredah, 2015).

Berdasarkan latar belakang tersebut saya mengangkat judul skripsi yaitu**“ Prototype Keamanan Page Login Website Menggunakan Teknik OTP Berbasis Email “**

1.2Rumusan Masalah

Berdasarkan latar belakang penelitian, rumusan masalah pada penelitian ini adalah sebagai berikut:

1. Apakah sistem *prototype login* dengan pengamanan OTP berbasis *website* dapat berjalan sesuai algoritma ?
2. Bagaimana membuat *Prototype Keamanan Login Page Admin* menggunakan Teknik OTP berbasis *Email*?
3. Keamanan apa yang digunakan pada saat pengiriman kode OTP melalui *email* ?

1.3 Batasan Masalah

Agar dalam penelitian ini tidak terjadi pembahasan diluar judul skripsi perlu adanya batasan-batasan terhadap ruang lingkup yang diteliti yaitu:

1. Keamanan *login page admin* pada *Prototype* ini menggunakan notifikasi *Email*
2. Media aplikasi keamanan *login page admin* ini menggunakan *Framework* / *Bookstrap* dan *Dreamweaver*
3. Pola pengamanan dengan *Character random* pada *Prototype* ini.

1.4 Tujuan Penelitian

Berikut ini beberapa tujuan penelitian yang akan dibahas dalam penelitian ini yaitu sebagai berikut :

1.Untuk mengetahui sistem *prototype login* dengan pengamanan OTP berbasis *website* dapat berjalan sesuai algoritma.

2. Untuk mengetahui cara pembuatan *prototype* keamanan *login page admin* menggunakan Teknik OTP berbasis Email.

3. Untuk mengetahui keamanan yang digunakan pada saat pengiriman kode OTP melalui *email*.

1.5 Manfaat Penelitian

1. Berguna untuk meningkatkan sistem keamanan jaringan terhadap serangan dari luar.
2. Dapat digunakan untuk mengetahui secara akurat kondisi *server* dan jaringan tidak terganggu, tanpa berada di depan *monitor* setiap saat.

BAB II

LANDASAN TEORI

2.1 Kriptografi

Kriptografi adalah ilmu dan seni untuk menjaga keamanan pesan. Pesan dapat berbentuk data atau informasi yang dikirim melalui saluran telekomunikasi atau yang disimpan didalam media rekam. Pesan yang tersimpan dapat berupa gambar, suara, video, atau berkas digital lainnya. Kriptografi terdiri beberapa elemen yang membentuk sebuah sistem yang disebut sistem kriptografi yang terdiri dari algoritma kriptografi, plainteks, cipherteks, dan kunci.

Sesuai defenisinya kriptografi bertujuan untuk memberikan layanan keamanan yang juga disebut aspek-aspek keamanan yang terdiri dari:

1. Kerahasiaan *(confidetiality)*

Kerahasiaan bertujuan untuk menjaga agar pesan tidak dapat dibaca oleh pihak-pihak yang berhak. Dalam kriptografi layanan ini diwujudkan dengan menyandikan pesan menjadi cipherteks

2. Integrasi Data *(Data Integrity)*

Integrasi data bertujuan untuk menjamin keaslian pesan atau belum dimanipulasi selama pengiriman. Dalam kriptografi layanan ini diwujudkan dengan menggunakan tanda tangan digital.

3. Otentikasi

Bertujuan untuk memastikan identitas pihak-pihak yang berkomunikasi maupun kebenaran sumber pesan dalam kriptografi layanan ini berwujud tanda tangan digital.

4. Nirpenyangkalan

Bertujuan untuk mencegah pihak yang berkomunikasi melakukan penyangkalan. Penyangkalan ini bisa terjadi dari pihak pengirim yang menyangkal telah malakukan pengiriman pesan atau dari pihak penerima yang menyangkal telah menerima pesan.

Berdasarkan sejarahnya, kriptografi dibagi menjadi kriptografi klasik dan modern. Berdasarkan kunci enkripsi dan dekripsi, kriptografi dibedakan menjadi kriptografi kunci simetris dan asimetris. Kriptografi kunci simteris menggunakan kunci yang sama untuk mengenkripsi dan mendekripsi. Sedangkan kriptografi kunci asimetris menggunakan kunci yan berbeda. Semua kriptografi klasik merupakan kriptografi kunci simetris. Sedangkan kriptografi modern sebagian merupakan kriptografi kunci simetris DES dan AES (Lalang Erawan, 2018).

2.2 *Prototype*

Prototype adalah suatu metode yang memperkenalkan *stakeholder* yang berinteraksi untuk membayangkan sebuah produk, bertujuan untuk mendapatkan beberapa pengalaman realistis dan dapat mengeksplorasi untuk membayangkan penggunaan dari sebuah produk. *Fidelity* adalah ukuran untuk membedakan tingkat interaksi, tampilan visual, dan detail dari suatu *prototype*. *Prototype* dibagi menjadi dua sifat yaitu *low-fidelityprototype* dan *high prototype.* Ciri-ciri *low-fidelity protoype* adalah prototype hasil rancangan tidak mempresentasikan produk final. Ada beberapa cara untuk menerapkan *low-fidelity* dengan menggunakan *story boarding, skeching, prototyp with index card* dan *wizard of Oz*. *High fidelity prototype* adalah produk yang diharapkan menjadi produk dan lebih mempresentasikan produk seperti produk akhir(Ismawan, 2018).

2.3 *Unified Modelling Language* (UML)

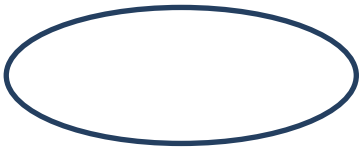
Unified Modelling Language (UML) adalah bahasa spesifikasi *standard* yang dipergunakan untuk mendokumentasikan, menspesifikasikan, dan membangun perangkat lunak. UML merupakan metodologi dalam mengembangkan sistem berorientasi objek dan juga merupakan alat untuk mendukung pengembangan sistem.

Unified Modelling Language (UML) adalah sebuah bahasa yang berdasarkan grafik atau gambar untuk memvisualisasi, menspesifikasikan, membangun pendokumentasian dari sebuah sistem pengembangan *software* berbasis OO *(Object-Oriented)*. UML sendiri juga memberikan *standard* penulisan sebuah sistem *blue print,* yang meliputi konsep bisnis proses, penulisan kelas-kelas dalam bahasa program yang spesifik, skema *database*, dan komponen–komponen yang diperlukan dalam sistem *software.* Diagram *Unified Modelling Language* (UML) antara lain sebagai berikut:

1. *Use Case Diagram*

Use Case menggambarkan *external view* dari sistem yang akan dibuat modelnya. Model *use case* dapat dijabarkan dalam diagram *use case*, tetapi perlu diingat, diagram tidak identik dengan model karena model lebih luas dari *diagram*.*Use case* harus mampu menggambarkan urutan aktor yang menghasilkan nilai terukur(Suendri, 2018).

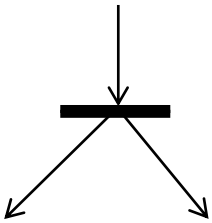
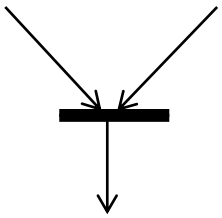
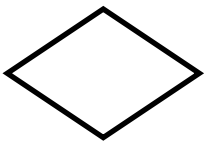
Tabel 2.1*Use Case diagram* (Hendini, 2016)

Gambar	Keterangan
	*Use Case* menggambarkan fungsionalitas yang disediakan sistem sebagai unit-unit yang bertukar pesan antar unit dengan aktif, yang dinyatakan dengan menggunakan kata kerja.
	*Actor* atau Aktor adalah *Abstraction* dari orang atau sistem yang lain yang mengaktifkan fungsi dari target sistem. Untuk mengidentifikasikan aktir, harus ditentukan pembagian tenaga kerja dan tugas-tugas yang berkaitan dengan peran pada konteks target sistem. Orang atau sistem bisa muncul dalam beberapa peran. Perlu dicatat bahwa aktor berinteraksi dengan *Use Case*, tetapi tidak memiliki kontrol terhadap *use case.*
	Asosiasi antara aktor dan *use case*, digambarkan dengan garis tanpa panah yang mengindikasikan siapa atau apa yang meminta interaksi secara langsung dan bukannya mengindikasikan data.
	Asosiasi antara aktor dan *use case* yang menggunakan panah terbuka untuk mengindikasikan bila aktor berinteraksi secara pasif dengan sistem .
	Include, merupakan di dalam *use case* lain (*required*) atau pemanggilan *use case* oleh *use case* lain, contohnya adalah pemanggilan sebuah
	Extend, merupakan perluasan dari *use case* lain jika kondisi atau syarat terpenuhi.

2. *Activity Diagram*

Activity Diagram menunjukkan aktivitas sistem dalam bentuk kumpulan aksi-aksi, bagaimana masing-masing aksi tersebut dimulai, keputusan yang mungkin terjadi hingga berakhirnya aksi. *Activitydiagram* dapat menggambarkan proses lebih dari satu aksi selama waktu bersamaan. *Activity Diagram* adalah aktivitas-aktivitas, objek, state, transisi state, dan event(Suendri, 2018).

Tabel 2.2*Activity diagram*(Hendini, 2016)

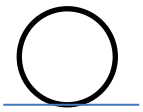
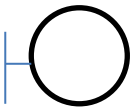
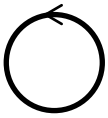
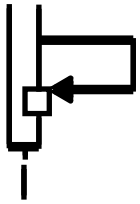
Gambar	Keterangan
	*Start Point*, diletakkan pada pojok kiri atas dan merupakan awal aktivitas.
	*End Point*, akhir aktivitas.
	*Activities,*menggambarkansuatu proses/kegiatan bisnis.
	*Fork*/percabangan, digunakan untuk menunjukkan kegiatan yang dilakukan secara paralel atau untuk menggabung kan dua kegiatan paralel menjadi satu.
	*Join* (penggabungan) atau *rake*, digunakan untuk menunjukkan adanya dekomposisi .
	*Decision Points*, menggambarkan pilihan untuk pengambilan keputusan, *true*atau *false*

	*Swimlane*, pembagian *activity diagram* untuk menunjukkan siapa melakukan apa.

4. *Squence Diagram*

Secara mudahnya *squence* diagram adalah gambaran tahap demi tahap, termasuk kronologi (urutan) perubahan secara logis yang seharusnya dilakukan untuk menghasilkan sesuatu sesuai dengan *Use Case Diagram*(Suendri, 2018)

Tabel 2.3*Sequence diagram*(Hendini, 2016)

Gambar	Keterangan
	*Entity Class*, merupakan bagian dari sistem yang berisi kumpulan kelas berupa entitas-entitas yang membentuk gambaran awal sistem dan menjadi landasan untuk menyusun basis data.
	*Boundary Class*, berisi kumpulan kelas yang menjadi *interfaces* atau interaksi antara satu atau lebih aktor dengan sistem, seperti tampilan form entry dan form cetak.
	*Control class*, suatu objek yang berisi logika aplikasi yang tidak memiliki tanggung jawab kepada entitas, contohnya adalah kalkulasi dan aturan bisnis yang melibatkan berbagai objek.
	*Message*, simbol mengirim pesan antar *class.*
	*Recursive*, menggambarkan pengiriman pesan yang dikirim untuk dirinya sendiri.

	*Activation*, mewakili sebuah eksekusi operasi dari objek, panjang kotak ini berbanding lurus dengan durasi aktivasi.
	Lifeline, garis titik-titik yang terhubung dengan objek, sepanjang *lifeline* terdapat *activation.*

2.4 *One Time Password* (OTP)

OTP merupakan pengembangan dari S/*KeyOne-Time Password System* yang dikembangkan oleh *Bellcore*. OTP dikembangkan untuk mengurangi resiko *password* dikirimkan kepada pihak lain melalui media yang tidak aman serta mencegah terjadinya *replay attack*, yaitu sebuah serangan yang mencoba untuk menggunakan sebuah informasi yang pernah disimpan dari sesi sebelumnya untuk digunakan di periode waktu yang berbeda. Karena OTPhanya bisa digunakan satu kali dan memiliki periode waktu yang terbatas, maka OTPsangat cocok untuk diimplementasikan pada sistem *login* berbasis *web*, terutama pada komputer publik dimana seringkali pengguna lupa untuk menghapus *cookies* atau *session*nya pada *browser*. Hal ini bisa mengurangi resiko terjadinya serangan *session hijacking*. Terdapat dua entitas yang bermain dalam skema OTP, yaitu *generator* yang bertugas untuk menghasilkan OTPdari kombinasi *passphrase* pengguna dan informasi yang disediakan pada sebuah *challenge* dari *server*, serta *server* yang bertugas untuk mengirimkan *challenge* serta melakukan verifikasi

terhadap nilai OTP yang diterima. Panjang dari keluaran yang dihasilkan adalah sebesar 64 *bit* yang kemudian diproses lagi sehingga menjadi 6-8 digit angka. Teknik yang digunakan dalam menghasilkan nilai OTPdicetuskan oleh *Leslie Lamport*. OTPsendiri dibagi lagi menjadi dua kategori besar, yaitu HOTP (*HMAC-based* OTP) yang diatur pada RFC 4226 dan TOTP (*Time-based* OTP) yang diatur pada RFC 6238(Sudiarto Raharjo et al., 2017).

One Time Password (OTP) adalah sebuah algoritma yang menghasilkan *password* yang hanya dapat digunakan satu kali. Dibandingkan dengan *password* biasa OTP dianggap lebih aman karena *password* terus berubah, yang berarti bahwa itu tidak rentan terhadap serangan ulangan atau *password* yang dicuri. Dalam konteks autentikasi, OTP biasanya digunakan sebagai mekanisme otentikasi tambahan makanya OTP sering disebut sebagai dua faktor otentikasi (*two-factor authentication/second factor authentication*).Metode otentikasi utama tetap menggunakan *username* dan *password*, tetapi untukmembuat dapat bertransaksi anda membutukan otentikasi tambahan, disitulah peran OTP.

Kombinasi *password* OTP hanya dapat digunakan sekali. Ada dua cara utama untuk memperoleh *One-Time Password* ini:

- Token *hardware*: misalnya perangkat token, yang dapat Anda *plug* ke *port USB* Anda dan akan secara otomatis ketik kode OTP untuk Anda.
- Token *software*: seperti *Google Authenticator*, dalam hal ini aplikasi Android sederhana menampilkan anda kode OTP yang dapat Anda masukkan pada *form login* Anda.

Password OTP dibuat secara acak atau semi-acak. Hal tersebut penyerang sulit untuk menebak nilai yang dihasilkan. Selain itu OTP juga menggunakan

fungsi *hash* yang dapat digunakan untuk menghasilkan nilai tetapi sulit untuk ditebak dan dibalikkan. (Id & Mahdiyah, 2016)

OTP merupakan metode otentikasi yang menggunakan *password* yang selalu berubah setelah setiap kali *login*, atau berubah setiap interval waktu tertentu. OTP dapat dibedakan atas dua kategori yaitu:

1. OTPBerbasisAlgoritmeMatematika :

OTP jenis ini menggunakan algoritme matematika kompleks seperti fungsi *hash* kriptografi untuk membangkitkan *password* baru berdasarkan *password* sebelumnya dan dimulai dari kunci *shared* rahasia. Contoh algoritme matematika yang digunakan dalam OTP ini adalah algoritma *open source* OATH yang telah distandarkan dan algoritma-algoritma lainnya yang telah dipatenkan. Beberapa produk aplikasi yang menggunakan otentikasi ini adalah:

a. *CRYPTOCard*

CRYPTOCard menghasilkan OTP baru setiap kali tombolnya ditekan. Sistem komputer akan menerima beberapa nilai balasan jika tombolnya ditekan lebih dari sekali secara tidak sengaja atau jika *client*-nya gagal mengotentikasi.

b. *Verisign*

Verisign unified authentication menggunakan standar dari OATH.

c. *E-Token Aladdin Knowledge System* NG-OTP

E-token Aladdin knowledge system NG-OTP merupakan *hybrid* antara USB dan token OTP *E-token Aladdin knowledge system* NG-OTP mengkombinasikan fungsionalitas dari token otentikasi yang berbasis

smart card dan teknologi otentikasi *user One-Time Password* dalam mode terpisah.

2. OTP berbasis sinkronisasi waktu

OTP jenis ini berbasis sinkronisasi waktu yang berubah secara konstan pada setiap satuan interval waktu tertentu. Proses ini memerlukan sinkronisasi antara token milik *client* dengan *server* otentikasi. Pada jenis token yang terpisah (*disconnected token*), sinkronisasi waktu dilakukan sebelum token diberikan kepada *client*. Tipe token lainnya melakukan sinkronisasi saat token dimasukkan dalam suatu alat input. Di dalam token terdapat sebuah jam akurat yang telah disinkronisasikan dengan waktu yang terdapat pada *server* otentikasi. Pada sistem OTP ini, waktu merupakan bagian yang penting dari algoritma *password*, karena pembangkitan *password* baru didasarkan pada waktu saat itu dan bukan pada *password* sebelumnya atau sebuah kunci rahasia.

Pada penelitian terkait, OTP jenis ini sudah mulai diimplementasikan terutama pada *remote Virtual Private Network* (VPN), dan keamanan jaringan Wi-Fi dan juga pada berbagai aplikasi *Electronic Commerce* (*E-commerce*). Ukuran standar penggunaan waktu pada algoritma ini adalah 30 detik. Nilai ini dipilih sebagai keseimbangan antara keamanan dan kegunaan.

Pada penelitian ini, OTP yang digunakan berbasis sinkronisasi waktu dengan kombinasi *salt*. OTP ini diterapkan pada pengecekan *sesi_id user* SSO UUI untuk menghasilkan *sesi_id user* yang selalu berubah berdasarkan nilai waktu. Kombinasi nilai *salt* digunakan untuk memperkuat pola OTP. Selain itu, nilai *salt* juga akan dicampur dengan nilai waktu untuk menghasilkan *sesi_id* auntentikasi yang dinamis sehingga setiap aplikasi yang terhubung dengan SSO

akan mendapatkan nilai *sesi_ id* auntentikasi yang berbeda-beda. Tidak hanya itu, *sesi_ id* yang dibangkitkan juga memiliki masa aktif tertentu. Setelah *sesi_id* berhasil diverifikasi pada sisi *client* SSO, *sesi_id* tersebut tidak dapat digunakan kembali untuk yang kedua kali. Secara lebih jelas, algoritma OTP dengan kombinasi nilai *salt* dapat dilihat pada gambar 2.1(Musliyana et al., 2016).

Algoritma One-Time Password SSO UUI dengan Kombinasi Salt

```
Input: Salt, WM (waktu_mulai), WP(waktu_proses), BW(batas_waktu), TW (toleransi_waktu), SIK(Sesi_id Kirim), SIP(Sesi_id Proses), Use_id
WM = ambil waktu saat user login
Salt = nilai salt (statik/dinamis)
TW = 30 (detik)  / optional
Use_id = 0
Output: SI (Sesi_id) (Akses Diterima / Ditolak)
SIK= Salt + WM
WP = ambil nilai waktu saat proses autentikasi
BW = WM+TW
while (WM  ≤ BW) do
    if WM = WP
    SIP = Salt + WP
        if Use_id ≤ 0 and SIP = SI
            Use_id++
            out: Sesi_id valid akses diterima
        end if
    end if
    WM = WM+1
end while
```

Gambar 2.1 Algoritma OTP UUI dengan kombinasi *salt*(Musliyana et al., 2016)

2.5 *Flowchart*

Flowchart merupakan diagram simbol yang menunjukkan arus data dan tahapan operasi dalam sebuah sistem yang digunakan baik oleh editor maupun oleh personal sistem. Ada berbagai jenis *flowchart* secara teori, namun *flowchart* yang akan digunakan dalam memecahkan permasalahan distribusi dokumen sistem informasi keuangan penerimaan dan pengeluaran kas pada penulisan ini, adalah gabungan antara *flowchart* analitik, *flowchart* dokumen dan diagram distribusi formulir.Mengingat pemisahan dan pembagian tugas merupakan elemen pengendalian internal, membutuhkan teknik untuk membagi tugaspengolahan data antar personel dan atau departemen/bagian.

Jenis-Jenis Flowchart

Adapun jenis-jenis *flowchart* yang digunakan dalampenelitian ini adalah sebagai berikut.

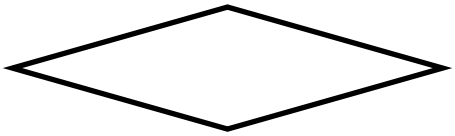
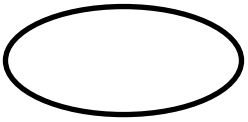
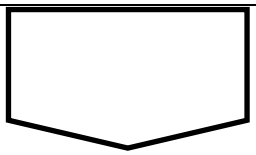
a. *Flowchart* Analitik, adalah bagan alir yang ditandai dengan penggunaan simbol yang dihubungkan dengan garis. *Flowchart* analitik mengidentifikasi semua proses signifikan pada sebuah aplikasi, dengan penekanan pada pemprosesan tugas.

b. *Flowchart* Dokumen, adalah bagan alir yang hanya terdiri dari simbol-simbol dokumen yang digunakan dalam *flowchart* tersebut. Tetapi, simbol lain pada dasarnya boleh saja digunakan untuk memperjelas suatu *flowchart*. Tujuan dari *flowchart*semacam ini adalah untuk mengetahui setiap dokumen yang digunakan dalam setiap sistemaplikasi dan mengidentifikasi titik awal dokumen, distribusi dokumen serta titik akhir setiap dokumen. *Diagram* distribusi formulir, adalah diagram alir yang menggambarkan distribusi setiap salinan formulir dalam sebuah organisasi. Dalam diagram ini, penekanannya terletak pada siapa yang akan mendapatkan formulir tertentu, bukan pada bagaimana setiap formulir akan diproses(Ratumurun, 2015).

Flowchart adalah representasi secara simbolik dari suatu algoritma atau prosedur untuk menyelesaikan suatu masalah, dengan menggunakan *flowchart* akan memudahkan pengguna melakukan pengecekan bagian-bagian yang terlupakan dalam analisis masalah, disamping itu *flowchart* juga berguna sebagai fasilitas untuk berkomunikasi antara pemrogram yang bekerja dalam tim suatu proyek.

Flowchart membantu memahami urutan-urutan logika yang rumit dan panjang. *Flowchart* membantu mengkomunikasikan jalannya program ke orang lain (bukan pemprogram) akan lebih mudah(Santoso & Nurmalina, 2017).

Tabel 2.4 Simbol *Flowchart*(Santoso & Nurmalina, 2017)

Simbol	Fungsi
	Permulaan sub program
	Perbandingan, pernyataan, penyeleksian data yang memberikan pilihan untuk langkah selanjutnya
	Penghubung bagian-bagian flowchart yang berada pada satu halaman.
	Penghubung bagian-bagian flowchart yang berada pada halaman berbeda
	Permulaan/akhir program
	Arah aliran program
	Proses inisialisasi/pemberian harga awal
	Proses penghitung/ proses pengolahan data
	Proses input/output data

Bagan alir (*flowchart*) adalah bagan (*chart*) yang menunjukkan alir (*flow*) di dalam program atau prosedur sistem secara logika. Bagan alir digunakan terutama untuk alat bantu komunikasi dan untuk dokumentasi. Ada lima macam bagan alir, di antaranya:

a. Bagan Alir Sistem (*system flowchart*) merupakan bagan yang menunjukkan arus pekerjaan secara keseluruhan dari sistem.
b. Bagan Alir Dokumen (*document flowchart*) disebut juga bagan alir formulir (*form flowchart*) merupakan bagan alir yang menunjukkan arus dari laporan dan formulir termasuk tembusan-tembusannya.
c. Bagan Alir Skematik (*schematic flowchart*) merupakan bagan alir yang menggambarkan prosedur di dalam sistem dengan menggunakan simbol-simbol bagan alir sistem dan gambar-gambar komputer serta peralatan lainnya yang digunakan oleh sistem.
d. Bagan Alir Program (program *flowchart*) merupakan bagan yang menjelaskan secara rinci langkah-langkah dari proses program.
e. Bagan Alir Proses (*process flowchart*) merupakan bagan alir yang banyak digunakan di teknik industri untuk menggambarkan proses dalam suatu prosedur(Verawati & Liksha, 2018)

2.6 *Email*

Email atau surat elektronik merupakan layanan pengiriman surat digital yang disediakan oleh *Internet Service Provider* (ISP). ISP menyediakan *server email* atau *mail server* yang berfungsi untuk melakukan pendeteksian pesan dan mengirimkannya pada *email* tujuan. Layanan surat elektronik sendiri terbagi kedalam dua bagian layanan surat elektronik bebas (*free*) dan layanan surat

elektronik terbatas. Layanan surat elektronik ini sendiri dapat diakses melaui berbagai cara :

1. *Web Mail*

Merupakan aplikasi berbasis *website* yang disediakan oleh penyedia layanan *email* agar para pengguna dapat dengan mudah mengakses layanan yang diberikan. Pengguna surat elektronik hanya membutuhkan *web browser* serta koneksi *internet* untuk melakukan pengaksesan layanan tersebut.

2. Aplikasi *email Client*

Merupakan aplikasi yang dibuat khusus untuk melakukan pengaksesan layanan surat elektronik. Dengan menggunakan aplikasi *mail client* ini pengguna dapat dengan mudah melakukan manajemen surat elektronik yang dimiliki, bahkan dapat melakukan penulisan surat elektronikmeskipun tidak terdapat koneksi *internet.*

Fungsi yang dilakukan oleh *email client* adalah sebagai berikut:

a. Mengambil *email* dari kotak surat.

b. Menampilkan *header* dari pesan-pesan yang ada di kotak surat. Pada beberapa kasus, sebagian isi *email* juga ditampilkan.

c. Menulis *email* baru.

Beberapa *email client* yang sering digunakan antara lain : *Mozilla Thunderbird, Microsoft Outlook, Eudora Mail* dan beberapa aplikasi *email client* yang terintegrasi dengan sistem operasi perangkat bergerak.

3. *Email Server*

Email server atau yang biasa disebut dengan *mail server* adalah komputer yang terhubung ke jaringan yang berfungsi sebagai kantor pos virtual, dalam hal

komputer yang berfungsi sebagai penyimpan dan penyampai surat elektronik (EC Council, 2010). Proses komunikasi jaringan antara *email client* dan *email server* dapat dilihat pada gambar 2. Ketika *email client* meminta *email* baru ke *email server*, *email server* meminta *username* dan *password* akun *email.* Setelah *email server* mencocokkan keduanya, *email server* akan mengirimkan *header email* baru ke *email client.*

Proses pengiriman *email* sendiri melalui beberapa protokol, yaitu:

1. SMTP

SMTP (*Simple Mail Transfer Protocol*) mekanisme yang digunakan untuk melakukan pengiriman surat elektronik antar *host* dalam jaringan komputer dengan menggunakan TCP / IP. SMTP merupakan protokol yang handal dan efisien yang menggunakan *port* 25 untuk operasinya. SMTP melakukan koneksi dengan melakukan pembukaan koneksi melalui SMTP *client* untuk melakukan koneksi ke *server* SMTP, setelah *server* mendapatkan koneksi dari klien SMTP *server* akan mencari keberadaan SMTP *server* tujuan dan mengirimkan surat elektronik tersebut.

2. POP3

POP (*Post Office Protocol*) versi 3 merupakan protokol yang dibuat pada tahun1984 yang berfungsi untuk melakukan penerimaan surat elektronik. POP sendiri merupakan mekanisme penarikan surat elektronik dari *mailserver* ke aplikasi *email* milik pengguna. POP pada dasarnya bekerja mirip dengan kotak surat konvensional. Dengan memanfaatkan protokol POP ini surat elektronik yang berada pada *mail server* akan terhapus. Seperti halnya protokol *email* yang lain

POP juga menggunakan perintah dalam operasinya. Perintah yang digunakan dapat dilihat pada gambar 2.2

Gambar 2.2 Proses komunikasi *email client* dan *email server*(Hamid, 2017)

3. IMAP

IMAP (*Internet Message Access Protocol*) merupakan pengembangan dari protokol POP versi 2. IMAP memiliki fungsi yang sama dengan POP yaitu digunakan untuk melakukan pembacaan surat elektronik. Perbedaan mendasar antara POP versi 3 dan IMAP terletak pada surat yang disimpan, jika POP3 akan menyalin seluruh surat dari *server* dan menyimpannya pada sisi *client*, IMAP tidak melakukan penyalinan dan penghapusan surat elektronik dari *mail server.*

2.6.1 Keamanan *Email*

Aspek yang penting dalam keamanan *email* adalah, kerahasiaan (*Confidentiality*), keaslian (*Authentication*), integritas (*Integrity*), anti penyangkalan (*Nonrepudiation*). Surat elektronik atau *email* itu sendiri bagaikan surat konvensional, jalur yang dilalui dari pengirim ke penerima sangat panjang melalui beberapa kantor pos cabang, pusat dan dibawa oleh beberapa petugas pengirim surat. *Email* juga demikian, jalur yang dilalui dari pengirim ke penerima melalui beberapa *router*, *mail servers*, dan beberapa jaringan komputer. *Email* sangat rentan dengan serangan baik pasif maupun aktif. Contoh ancaman pasif yang mungkin adalah :

1. Pembukaan isi *email*

Kebanyakan *email* ditransmisikan dalam bentuk jelas (tanpa enkripsi), artinya beberapa orang dengan aplikasi tertentu bisa melihat isi *email.*

2. Analisa lalu lintas data

Beberapa negara secara rutin memantau isi *email*.

Sedangkan ancaman serangan aktif antara lain sebagai berikut :

1. Modifikasi isi *email*

Isi *email* dapat dimodifikasi pada saat *transport*asi atau penyimpanan. Selama penyerang ada dalam satu jaringan, penyerang bisa menggunakan *ARP spoofing* untuk mencegat lalu memodifikasi isi *email* ke *mail server* maupun dari *mail server*. Teknik ini yang nantinya akan digunakan untuk pengujian.

2. *Masquerade* (Penyamaran)

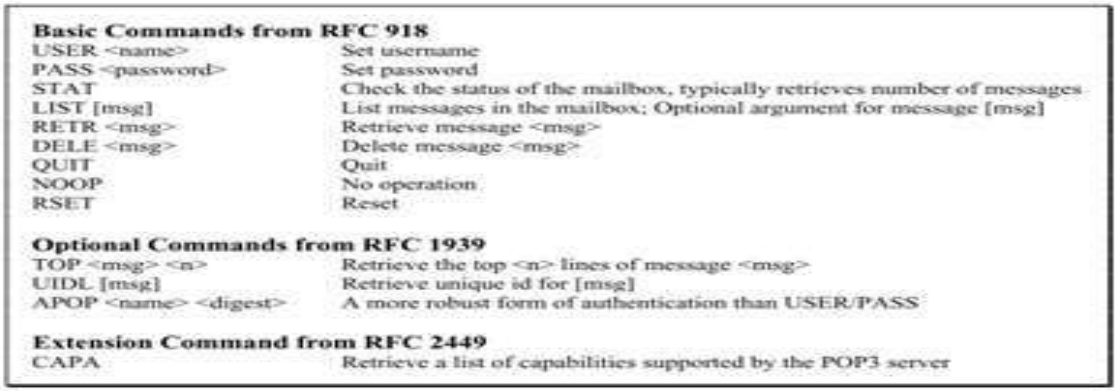
Dimungkinkan untuk mengirim pesan sebagai orang atau organisasi lain.

3. *Spoofing*

Pesan palsu dapat dimasukkan ke dalam sistem *mail* pengguna lain.

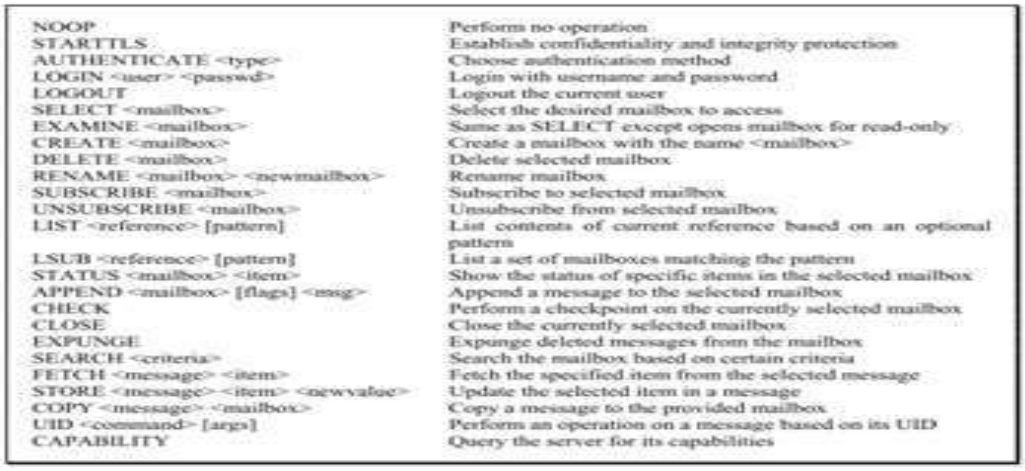
4. *Denial of Service*

Dimungkinkan untuk membuat *mail server* sibuk dan *overload* sehingga membuat *mail server* tersebut tidak bisa melayani pengguna lain.



Basic Commands from RFC 918	
USER <name>	Set username
PASS <password>	Set password
STAT	Check the status of the mailbox, typically retrieves number of messages
LIST [msg]	List messages in the mailbox; Optional argument for message [msg]
RETR <msg>	Retrieve message <msg>
DELE <msg>	Delete message <msg>
QUIT	Quit
NOOP	No operation
RSET	Reset
Optional Commands from RFC 1939	
TOP <msg> <n>	Retrieve the top <n> lines of message <msg>
UIDL [msg]	Retrieve unique id for [msg]
APOP <name> <digest>	A more robust form of authentication than USER/PASS
Extension Command from RFC 2449	
CAPA	Retrieve a list of capabilities supported by the POP3 server

Gambar 2.3 Perintah pada protokol POP(Hamid, 2017)



NOOP	Perform no operation
STARTTLS	Establish confidentiality and integrity protection
AUTHENTICATE <type>	Choose authentication method
LOGIN <user> <passwd>	Login with username and password
LOGOUT	Logout the current user
SELECT <mailbox>	Select the desired mailbox to access
EXAMINE <mailbox>	Same as SELECT except opens mailbox for read-only
CREATE <mailbox>	Create a mailbox with the name <mailbox>
DELETE <mailbox>	Delete selected mailbox
RENAME <mailbox> <newmailbox>	Rename mailbox
SUBSCRIBE <mailbox>	Subscribe to selected mailbox
UNSUBSCRIBE <mailbox>	Unsubscribe from selected mailbox
LIST <reference> [pattern]	List contents of current reference based on an optional pattern
LSUB <reference> [pattern]	List a set of mailboxes matching the pattern
STATUS <mailbox> <item>	Show the status of specific items in the selected mailbox
APPEND <mailbox> [flags] <msg>	Append a message to the selected mailbox
CHECK	Perform a checkpoint on the currently selected mailbox
CLOSE	Close the currently selected mailbox
EXPUNGE	Expunge deleted messages from the mailbox
SEARCH <criteria>	Search the mailbox based on certain criteria
FETCH <message> <item>	Fetch the specified item from the selected message
STORE <message> <item> <newvalue>	Update the selected item in a message
COPY <message> <mailbox>	Copy a message to the provided mailbox
UID <command> [args]	Perform an operation on a message based on its UID
CAPABILITY	Query the server for its capabilities

Gambar 2.4 Perintah pada protokol IMAP(Hamid, 2017)**.**

Guna mengatasi ancaman – ancaman tersebut diatas, maka dikembangkan metode pengamanan *email* yang terenkripsi. Pada dasarnya ada 2 metode dalam enkripsi *email*, yaitu:

1. *Pretty Good Privacy* (PGP)

   Metode ini merupakan metode yang sangat sering digunakan. PGP dirilis pertama kali pada tahun 1991. PGP tersedia baik gratis maupun yang berbayar. PGP mendukung enkripsi dari 5 layanan, yaitu *authentication, confidentiality, compression, e-mail compatibility* dan *segmentation*. Selain 5 layanan itu, PGP juga mendukung *digital signature.*

2. S/MIME (*Secure / Multipurpose)*

   (*Internet Mail Extensions*) S/MIME dicetuskan oleh RSA Data *Security* pada tahun 1995. Dalam hal fungsionalitas umum, S/MIME sangat menyerupai PGP. Keduanya menawarkan kemampuan untuk menandatangani dan atau mengenkripsi pesan. Layanan-layanan yang dienkripsi juga sama dengan PGP. Pada sisi penyedia layanan, enkripsi bisa dilakukan dalam komunikasi *client* ke *server* ataupun komunikasi antar *mail server*. Enkripsi ini biasanya menggunakan standar enkripsi TLS (*Transport Layer Security*). Protokol TLS

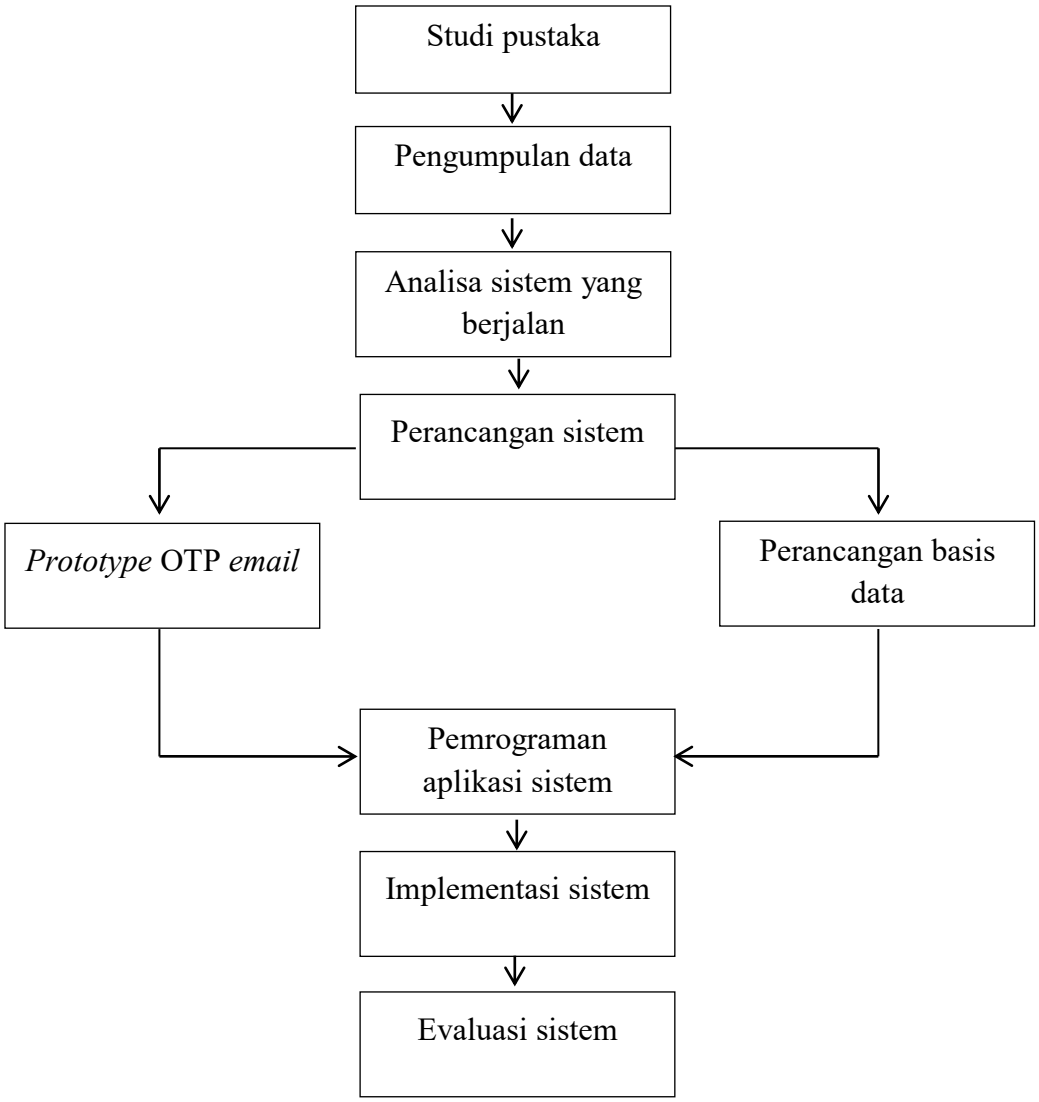
sendiri mirip dengan protokol *Secure Sockets Layer* (SSL) yang dikombinasikan dengan protokol POP (995), IMAP (993), dan SMTP (465) yang berfungsi untuk enkripsi komunikasi antara aplikasi *email client* dan *email server*(Hamid, 2017).

BAB III

METODE PENELITIAN

3.1 Tahapan Penelitian

Tahapan-tahapan penelitian yang dapat dilakukan dalam penelitian ini yaitu sebagai berikut :



Gambar 3.1 Tahapan penelitian

3.2 Teknik Pengumpulan Data

Adapun teknik pengumpulan data yang dilakukan peneliti dalam penelitian tugas akhir ini yaitu :

1. Studi Pustaka

Pada tahapan ini bertujuan untuk mendapatkan buku, literaturataureferensi-referensi yang mendukung dari berbagaisumber yang terkaitdenganpermasalahan yang adauntukmembantudalammemcahkanmasalah.

2. PengumpulanData

Pada tahapan ini penulis mengumpulkan data-data dengan melakukan observasipadasistem-sistem*website* yang telah mengimplementasikan desain sistemkeamanan*page login*menggunakan OTP *email*.

3. AnalisaSistem

Pada tahapan ini merupakansuatu proses mengidentifikasimasalah, memecahkan masalah pada sistem, dan menerapkan rancangan sesuaidengan yang di butuhkan oleh*user*.

4. Perancangan Sistem

Padatahapaninipenulismembuatgambaranataurancangansistemsesuaidenganpe mecahanmasalah yang ada, data-data yang di dapatdansesuaidengankebutuhan user.

5. Prototype OTP *Email*

Padatahapaninipenulismelakukanperancangansistempada*page loginwebsite* admin denganmenggunakan OTP (*One Time Password*) dimana password login akanditerimamelalui*email*dari*user* yang valid danmempunyaiakses admin pada*database website* yang dirancang.

6. Perancangan Basis Data

Melakukanperancangan basis data untukpenyimpanan data datapendukung page *login website*, data admin dan*user*akses.

7. PemrogramanAplikasiSistem

Melakukanpemrogramanaplikasisistem *page login website*denganpemrograman PHP danpada basis data menggunakan*software apache*dan MySQL MAMP.

8. ImplementasiSistem

Padatahapaniniakandilakukanimplementasisistemuntukmengamankan*page login website*terutamapada*login*akses administrator *website*. Implementasisisteminiakanmengujisecaratidaklangsungberjalannyaalgoritmapadar ancangansistemdenganaplikasi yang telahselesaidiprogram.

9. Evaluasi Sistem

Padatahapaniniakandilakukanpengujiansistemuntukmemeriksasuatusistem yang dihasilkanapakahsudahdapatdijalankansesuaidengankebutuhannyadanmelihatapak ahmasihadakesalahan-kesalahanataukekurangan-kekurangan yang adapadasisteminformasi yang di uji

3.3AnalisaSistem Yang Berjalan

Analisis sistem merupakan penguraian dari suatu sistem yang utuh ke dalam bagian-bagian komponennya dengan maksud untuk kesempatan-kesempatan, hambatan-hambatan yang terjadi dan kebutuhan-kebutuhan yang diharapkan sehingga dapat diusulkan perbaikan-perbaikannya. Perangkat Lunak yang akan di bangun oleh penulis adalah *Prototype* Keamanan *Login Page* Admin

Menggunakan Teknik OTP Berbasis *Email*.Dari hasil analisa awal, kebutuhan aplikasi yang akan di buat dapat disimpulkan sebagai berikut:

1. Mampu memberikan kode verifikasi token yang aman bagi adminstrator.
2. Mampu menampilkan halaman dari *web protype* yang di rancang sebagai akses admin dengan keamanan tingkat tinggi menggunakan algoritma MD5*Hash*.

Saat ini, sistem keamanan pada *website* secara umum masih menggunakan sistem yang lama yaitu manual. *User* masuk ke halaman *website* tanpa ada pengamanan yang ketat di sisi keamanan *website*. Banyak dari *user* mengeluhkan tidak adanya fasilitas keamanan yang mudah dan efektif. Maka dari itu diperlukan sebuah Sistem Verifikasi Token pada *page login website* sehingga menjadi lebih aman.

1. Komunikasidenganpengguna

Dalam pembuatan sistem verifikasi token, terlebih dahulu penulis melakukan komunikasi pada *website* yang masih melakukan secara manual seperti SMK TMI. Komunikasi dengan pihak tersebut diketahui apa saja yang diinginkan agar aplikasi verifikasi token yang dihasilkan dapat efektif dan tepat sasaran.

User memerlukan suatu aplikasi verifikasi token yang mencakup:

a. Sistem Verifikasi token yang dapat diakses dimana saja berbasis *website* dan di ketika diakses di android maka tampilan *website* bisa menyesuaikan.
b. Sistem Verifikasi yang dapat memberikan keamanan data pada *website* sehingga *user* dapat merasa aman dan nyaman dalam menggunakan *website* tersebut.

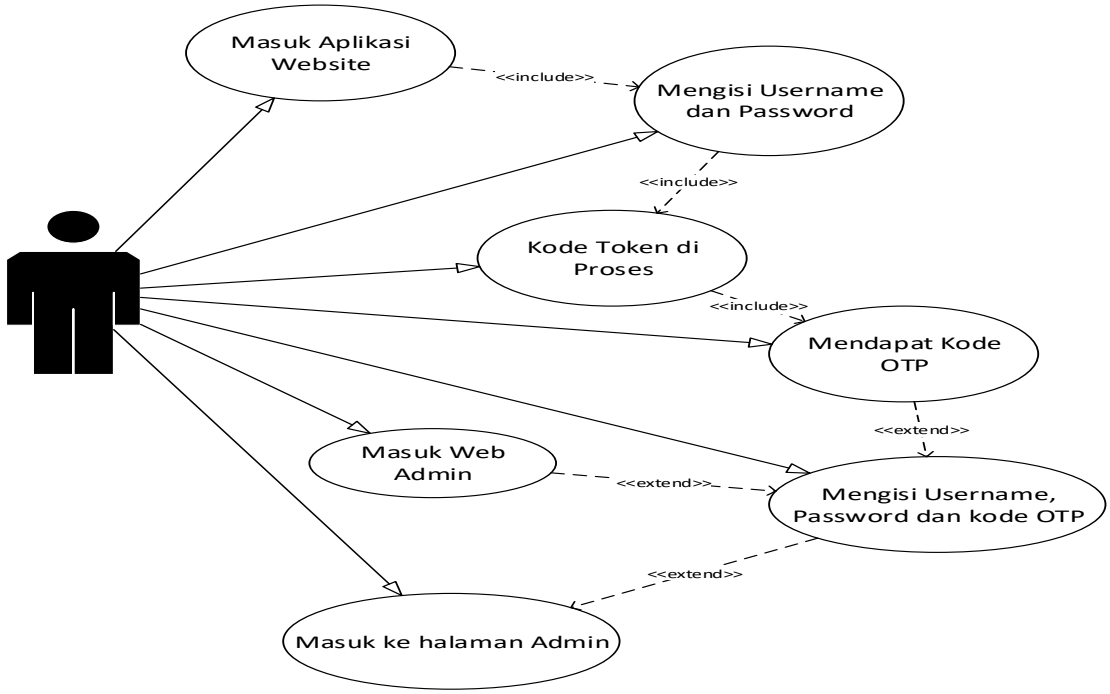
Melihat kebutuhan *user* tersebut, maka saya berusaha membuat *Prototype* Keamanan *Login Page* Admin Menggunakan Teknik OTP Berbasis *Email*.

3.3 Rancangan Penelitian

3.3.1 Perancangan UML

1. *Use Case Diagram*

Merupakan permodelan dari perilaku sistem informasi yang akan dibuat. Sebuah *use case* mempresentasikan sebuah interaksi antara aktor dengan sistem .



Gambar 3.2 *Use Case* diagram sistem OTP oleh admin

Pada gambar 3.2 diatas terdapat satu aktor yaitu *user* (Admin). Untuk membuka halaman admin pada *prototype website* yang di bangun, *user* harus memasukkan kode OTP yang dikirim ke *email* admin yang didapat dari *website prototype*. Setelah *user* memasukkan *username* dan *password*, maka kode OTP akan dikirim ke *email admin*, lalu kode tersebut dimasukkan ke halaman *login web prototype* untuk masuk ke halaman admin *prototype website*. Kemudian akan diproses oleh sistem untuk menentukan informasi apa yang diperlukan admin.

2. *UseCase* Narrative

Adapun *UseCase*Narrative dapat dipresentasikan pada tabel berikut ini :

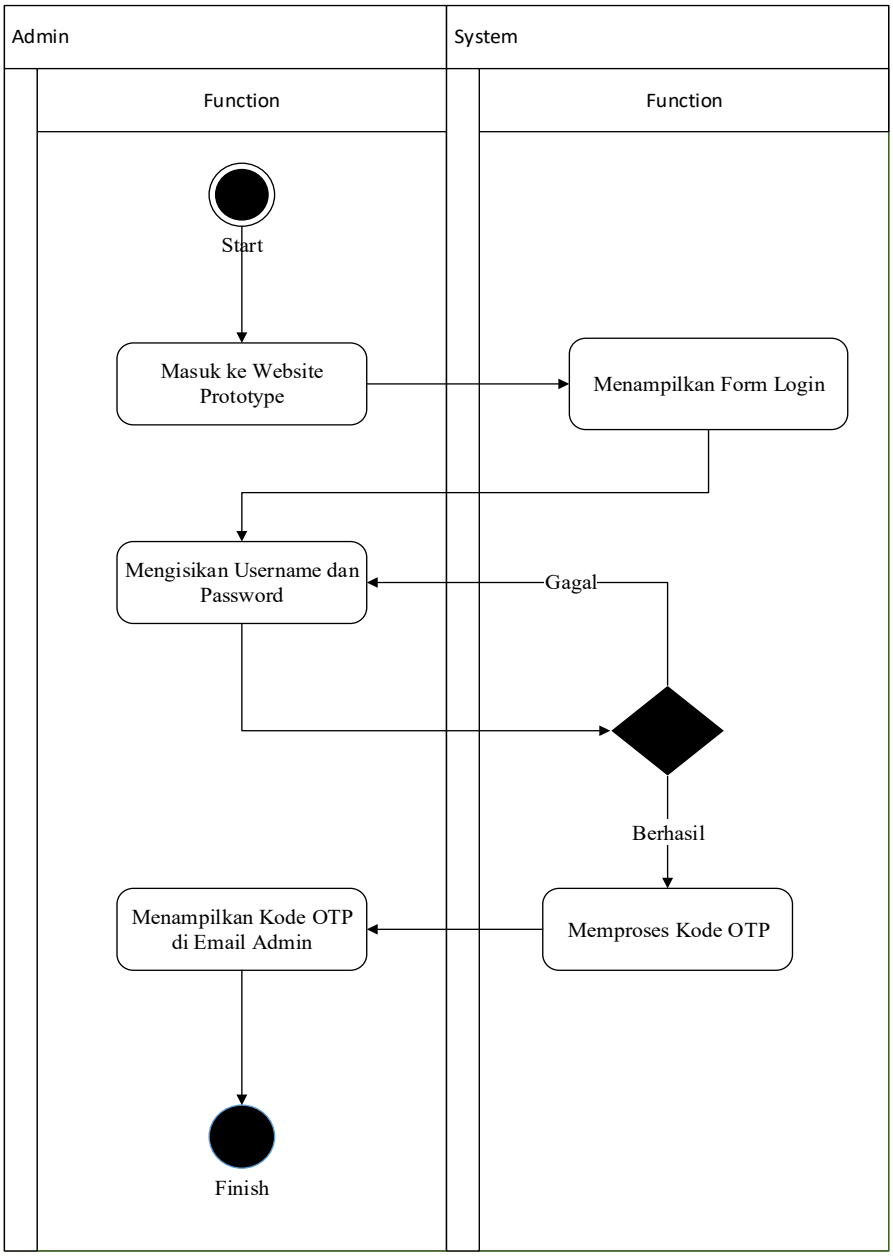
Tabel 3. 1 *UseCase* Narrative *Prototype Website*

USE CASE NAME:	*Use-Case Narrative Prototype Website*
PRIMARY ACTOR:	Admin *Protype Web*
GOAL	Menampilkan Kode Token
DESCRIPTION:	*Use case* ini berjalan pada saat admin akan membuka *Back-End-System*
PRE-CONDITION:	1. Memasukkan *Username* Admin 2. Memasukkan *Password* Admin 3. Menekan Tombol *Generate*
TRIGGER:	Admin ingin menampilkan kode token
SCENARIO	1. Admin Login ke halaman login *administration* 2. Admin memasukkan *username* 3. Admin memasukkan *password* 4. Admin menekan tombol "*GENERATE*" untuk mendapat kode token
ALTERNATE FLOW:	Admin keluar dari *website*
CONCLUTION:	*Use case* ini selesai saat admin mendapat kode token melalui *email* yang terdaftar di *database*
POST-CONDITION:	Admin masuk ke menu *login* pada *website*
IMPLEMENTATION CONTRAINTS AND SPECIFICATIONS:	*Username* dan *password* sudah ditentukan oleh Super Admin

USE CASE NAME:	*UseCase* Narrative *Login Prototype Website*
PRIMARY ACTOR:	Admin *Website Protype Website*
GOAL:	Masuk ke halaman admin pada *website Protype*
DESCRIPTION:	*Use case* ini berjalan ketika admin membuka menu *login* di *website Prototype Website*
PRE-CONDITION:	1. Memasukkan *Username* Admin 2. Memasukkan *Password* Admin 3. Memasukkan Kode OTP yang diperoleh dari *Website Prototype* melalui *email*
TRIGGER:	Admin ingin masuk ke halaman *Website Prototype*
SCENARIO:	1. Admin membuka *website Prototype* dan masuk ke menu *login* 2. Admin mengisi *Username* 3. Admin mengisi *Password* 4. Admin mengisi Kode OTP
ALTERNATE COURSE:	Keluar dari *website Prototype*
CONCLUTION	*Use case* ini selesai saat admin dapat masuk ke halaman admin pada *website Prototype*
POST-CONDITION:	Admin dapat masuk ke halaman admin *website prototype*
IMPLEMENTATION CONTRAINTS AND SPECIFICATIONS:	Kode OTP berlaku jika halaman *login* belum di klik *login* atau proses validasi halaman selanjutnya.

3. Activity diagram

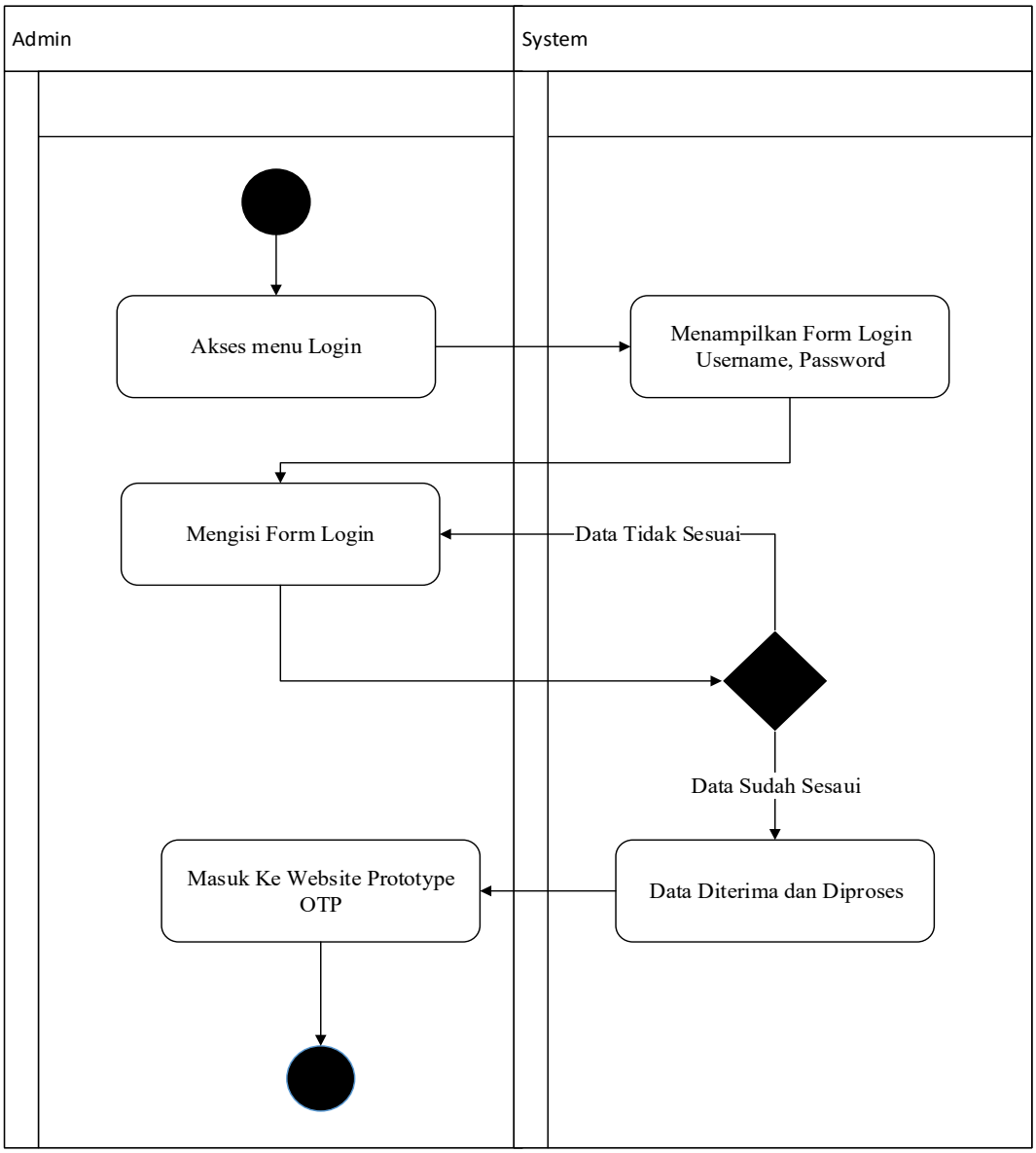
a. *Request* Token *Web Page login* ke *Email*



Gambar 3.3*Request* token *web page login* ke *email*

Pada *activity request* kode OTP pada *Website*, *Software* "*Prototype* OTP" akan menampilkan *form login* untuk diisi oleh admin. Jika pengisian data *username* dan *password* tidak sesuai, maka *login* gagal dan kembali ke menu *form*. Jika pengisian data *username* dan *password* sudah sesuai maka *website* akan

menampilkan kode OTP yang diperlukan untuk masuk ke *website PrototypeWebsite* dan kode OTP dikirim ke *email* admin.



Gambar 3.4 Proses autentikasi *request token web page login* ke *email*.

Pada *Activity Login Website* OTP, *user* mengisi *form login Prototype Website* OTP yang telah disediakan. Kemudian kesesuaian data informasi akan diperiksa. Jika data tidak sesuai, maka akan kembali ke *form login user*. Jika *username* dan *password* serta token sudah sesuai, maka aplikasi akan memproses data informasi dan menampilkan halaman *web Prototype Website* OTP.

3. Class Diagram

Pada *class diagram*, digunakan 2 macam kelas, yaitu siswa dan *users*. Kelas yang satu dengan yang lain memiliki hubungan dan mempunyai keterkaitan. Berikut adalah *class diagram* dari *database* "otp" yang digunakan pada *website prototype* OTP.

Gambar 3.5*Class diagram prototype* OTP

3.4.2 Rancangan *Database*

Pada penelitian ini digunakan nama *database* yaitu "otp". Di dalam *database* ini terdiri dari tabel siswa dan *user*. Adapun rancangan tabel dalam *database* yang digunakan dalam penelitian yaitu sebagai berikut:

Tabel 3.2 "siswa" pada *database* "otp"

No	Nama Variabel	Type Data	Panjang karakter
1	Id	Int	11
2	Nis	varchar	255
3	Nama	Text	
4	Alamat	Text	

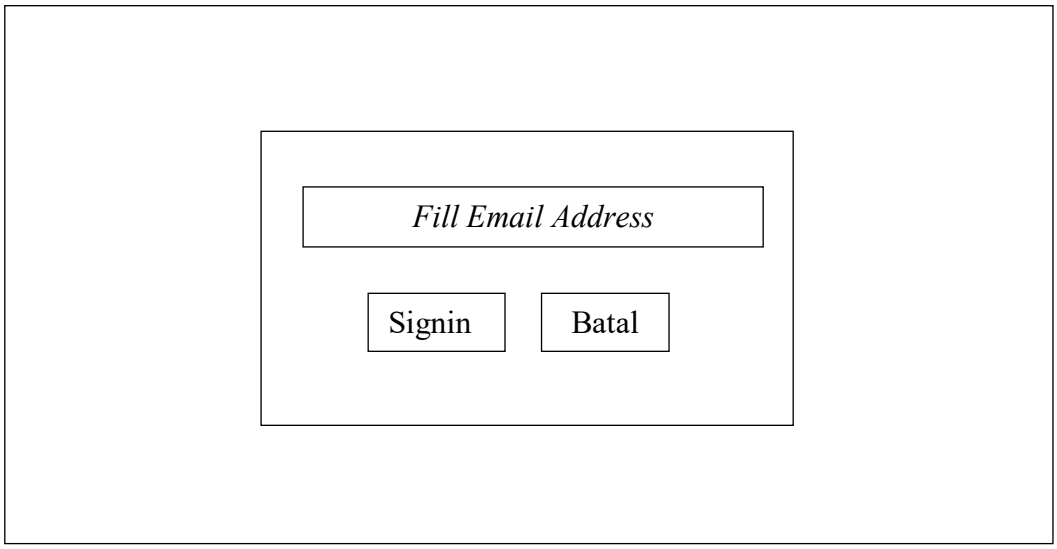
Tabel 3.3 "*user*" pada *database* "otp"

No	Nama Variabel	Type Data	Panjang karakter
1	Id	Int	5
2	name	varchar	50
3	email	varchar	255
4	password	varchar	255
5	created_at	timestamp	

3.4.3 Rancangan antar muka

1. Antar muka Tampilan awal *website*

Adapun tampilan dari antar muka awal *website* yang akan dibangun yaitu sebagai berikut :



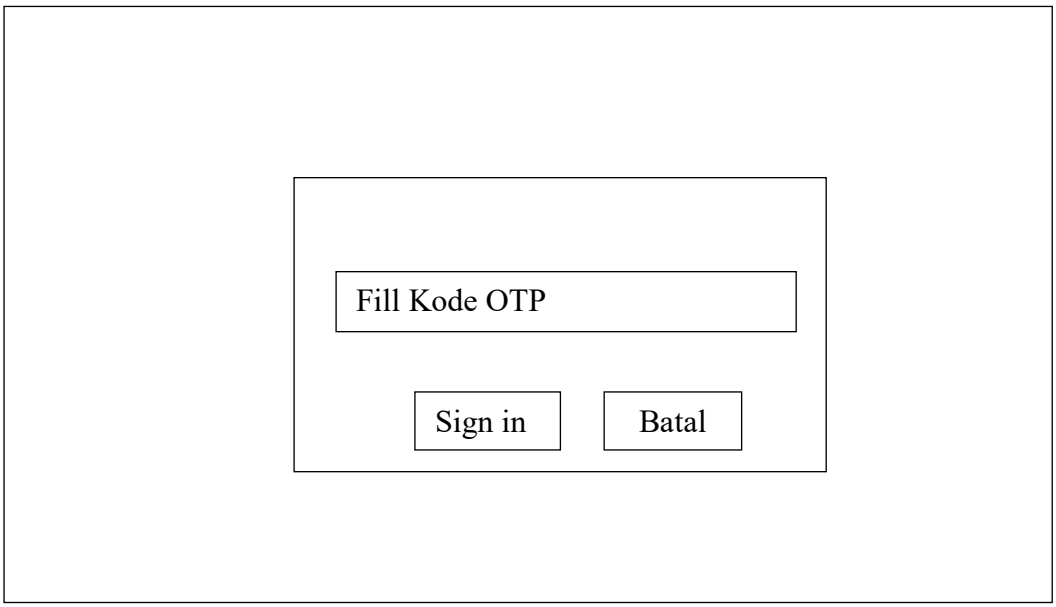
Gambar 3.6 Rancangan antarmuka *login website*

1. *Fill Email Address* untuk inputan isian *email* yang terdaftar pada *database* "otp".
2. Tombol *Sign In* untuk login kedalam *system*, dan meminta kode *token email.*

3. Tombol Batal untuk membatalkan inputan yang di isi pada *Fill Email Address*

2.Tampilan Antarmuka *Fill* Kode OTP

Adapun tampilan antarmuka *fill kode OTP* adalah sebagai berikut :

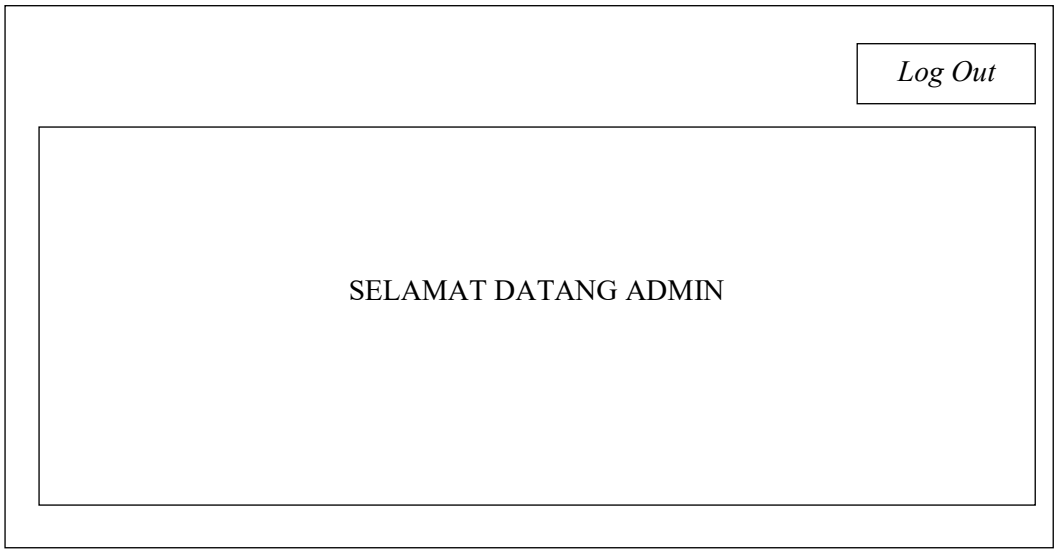


Gambar 3.7 Rancangan Antarmuka *Fill* Kode OTP

1. *Fill* kode OTP untuk inputan isian kode OTP yang di *replay* ke *email* admin.
2. Tombol *Sign In* untuk *login* kedalam sistem, dan melakukan verifikasi apakah kode OTP yang diinputkan adalah sesuaikan dan kode yang di *replay* kedalam *email*.
3. Tombol Batal untuk membatalkan inputan yang di isi pada *Fill* kode OTP.

3. Antarmuka Halaman Admin

Adapun antarmuka halaman Admin dapat di lihat pada gambar berikut ini:



Gambar 3.8 Rancangan antarmuka halaman admin

1. Tombol *Log Out* digunakan untuk keluar dari halaman admin

BAB IV

HASIL DAN PEMBAHASAN

4.1 Kebutuhan Spesifikasi Minimum *Hardware* dan *Software*

Kebutuhan spesifikasi minimum *hardware* dibutuhkan untuk mengetahui sistem yang dibangun dapat berjalan pada *hardware* yang spesifikasi minimum sehingga *user* lain yang menggunakan *system* ini mendapatkan pengetahuan jika ingin mengimplementasikan ke *hardware* miliknya. Adapun kebutuhan spesifikasi Minimum *hardware* yang digunakan dalam penelitian yaitu:

4.1.1 Kebutuhan spesifikasi minimum *hardware*

Analisis kebutuhan sistem merupakan analisis yang dibutuhkan untuk menentukan spesifikasi kebutuhan sistem. Spesifikasi ini juga meliputi elemen atau komponen–komponen apa saja yang dibutuhkan untuk sistem yang akan dibangun sampai dengan sistem tersebut diimplementasikan. Analisis kebutuhan ini juga menentukan spesifikasi masukkan yan diperlukan sistem, keluaran yang akan dihasilkan sistem dan proses yang dibutuhkan untuk mengolah masukkan sehingga menghasilkan suatu keluaran yang diinginkan.

1. Analisis Perangkat Keras (*Hardware*)

Perangkat keras minimum yang digunakan untuk membangun sistem informasi penjualan ini adalah

a. Processor berkecepatan 2.0 Ghz
b. RAM 2 Gb
c. Hardisk minimal 10 Gb untuk menyimpan data
d. LAN Card

e. Keyboard dan Mouse

f. Monitor

4.1.2 Kebutuhan spesifikasi minimum *software*

Untuk mendukung dalam penyimpanan informasi, dibutuhkan suatu fasilitas yang memadai. Yaitu berupa perangkat lunak (*software*) yang dirancang untuk memudahkan dalam pembangunan dan menjalankan sistem nantinya. Adapun perangkat lunak yang digunakan adalah sebagai berikut :

a. Minimum Sistem Operasi Microsoft Windows 7 32 Bit

b. MAMP

c. Browser Internet seperti Mozilla Firefox & Chrome

4.2 Pengujian Aplikasi dan Pembahasan

Tahapan pengujian aplikasi berupa tampilan-tampilan dari implementasi yang dilakukan *prototype website* secara lokal. Adapun pengujian dapat di lihat pada pembahasan berikut :

4.2.1 Pengujian aplikasi

Tahap pengujian aplikasi merupakan lanjutan dari tahap perancangan sistem. Pada tahap ini dilakukan implementasi sistem ke dalam bahasa pemrograman berdasarkan hasil analisa dan perancangan sistem. Pada tahap pengujian ini digunakan perangkat lunak dan perangkat keras, sehingga sistem yang dibangun dapat diselesaikan dengan baik.

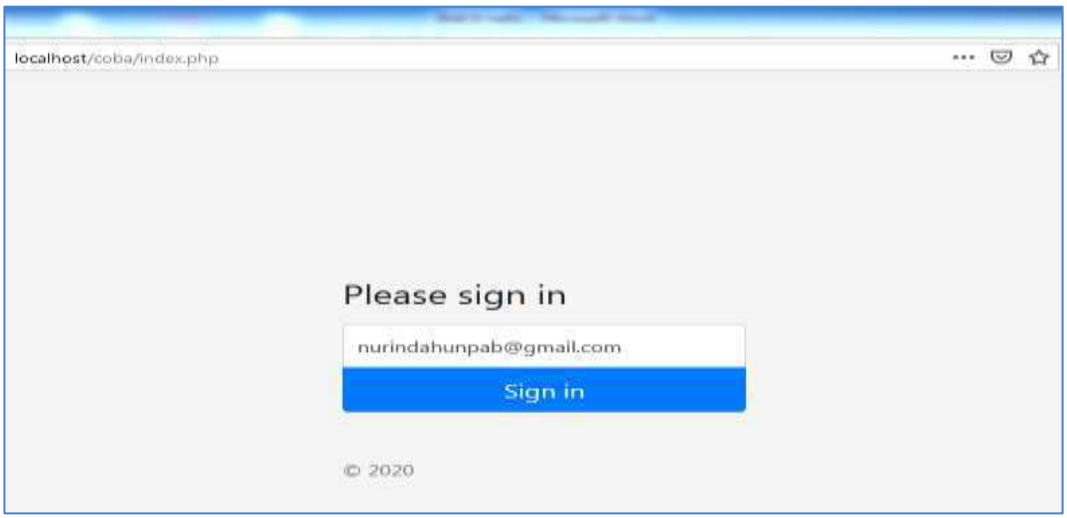
1. Tampilan Antarmuka *Login Prototype*

Dalam percobaan ini untuk mengakses tampilan *login page website prototype* OTP. Maka perlu di*running*kan *service* dari Apache dan MYSQL yang terdapat pada fitur *software* MAMP. Software ini mendukung bahasa pemrogram PHP 5, dan PHP 7. Dalam pembuatan *website* ini menggunakan bahasa pemrograman tersebut. untuk mengakses tampilan *login* antarmuka perlu di klik *browser* seperti Mozilla dan google chrome. Ketiksa sudah tampil maka diketika perintah http://localhost/coba/ pada kotak dialog url browser internet tersebut. adapun tampilan dapat di lihat pada gambar 4.1 berikut :

Gambar 4.1 Antarmuka awal *login prototype*

Pada gambar 4.1 di atas diketahui isian *email address*, yang berjudul *Please Signin*. Kemudian tombol *Sign in* untuk melanjutkan tahapan berikutnya dari proses *login*, yaitu pengiriman kode OTP. Tahapan selanjutnya yaitu di isi nama *email* yang terdaftar pada *database* dengan di isi yaitu : nurindahunpab@gmail.com kemudian klik tombol *Signin* untuk melanjutkan tahapan selanjutnya. Maka *system* akan mengirimkan kode OTP yang sudah

dideskripsikan dan di kirim ke *email*nurindahunpab@gmail.com. Adapun tampilan dapat di lihat pada gambar 4.2 berikut :



Gambar 4.2 Isian *email* pada kotak isian *email address*

Tahapan selanjutnya*system website* melakukan navigasi link ke link = http://localhost/coba/index-step2.php?id=2 . Maka tampilan dilanjutkan dengan judul *Please Sign In*dan notifikasi dibawahnya yaitu: "*Password* telah dikirimkan melalui alamat *email*nurindahunpab@gmail.com. silahkan memeriksakan kotak masuk *email* tersebut. adapun tampilan *page login* tahapan ini dapat di lihat pada tampilan gambar 4.3 berikut :

Gambar 4.3 Notifikasi kode OTP di kirim pada *email* terkait

Pada gambar 4.3 akan muncul apabila *email* yang diinputkan pada tahap pertama *login website* tervalidasi dan sesuai pada *database system* MAMP. Jika data *email* tidak sesuai maka akan muncul *email not found*. Percobaan dilakukan menggunakan *email* yang belun terdaftar pada *system database* MAMP. Kemudian diisikan *email* : medanjaya@gmail.com pada kotak dialog *Email Addres* pada tahapan awal. *Email* ini tidak terdaftar pada *database*. Adapun tampilan percobaan dapat di lihat pada gambar 4.4 sebagai berikut :

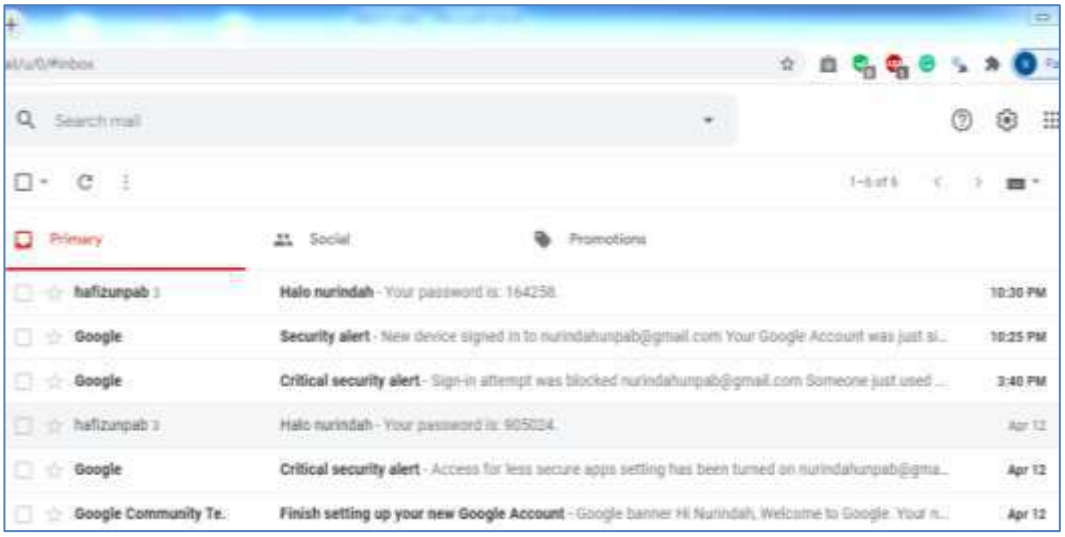
Gambar 4.4 Isian *email* tidak terdaftar pada *system database*

Percobaan selanjutnya diklik tombol *Sign in*, maka muncul notifikasi "*email not found*" adapun tampilan dapat dilihat pada gambar 4.5 berikut :

Gambar 4.5 Notifikasi *Email Not Found* dikarenakan *email* tidak valid

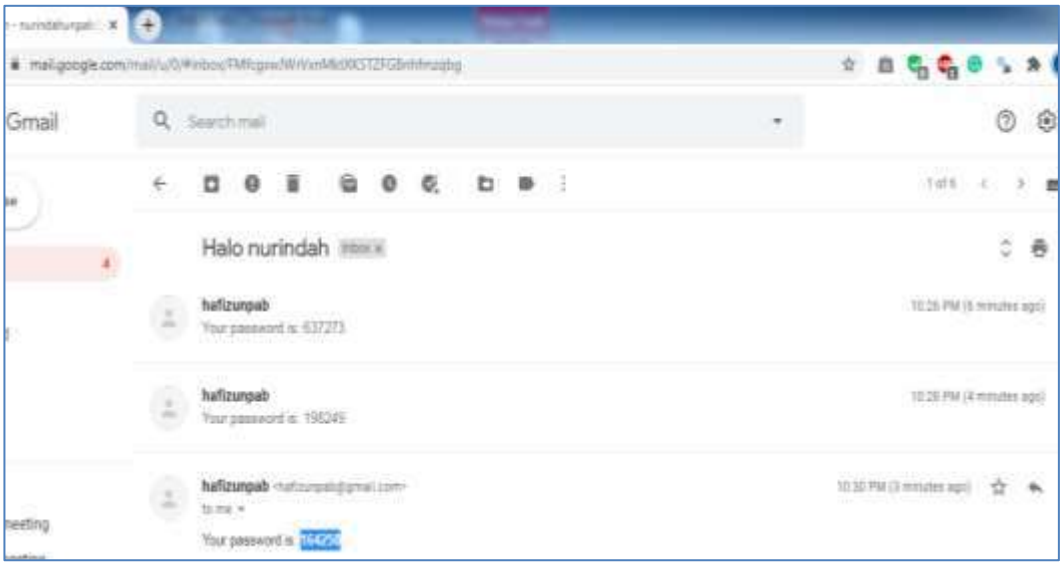
2. Pengecekan Kode OTP pada *Email*

Tahapan ini dilakukan untuk pengecekan pesan *email* masuk yang berasal dari kiriman pesan *system website prototype* OTP. Pada *website* terdapat *email* yang disetting pada PHP miller, menggunakan *email* yaitu : hafizunpab@gmail.com dengan *password* Unpab###2020. Pesan OTP ditujukan ke *email*nurindahunpab@gmail.com . Adapun kode OTP yang diterima oleh *email* : nurindahunpab@gmail.com dapat di lihat pada tampilan 4.6 berikut ini :



Gambar 4.6 Kode OTP yang masuk pada nurindahunpab@gmail.com

Tahapan selanjutnya diklik pesan dari akun *gmail* hafizunpab, kemudian diketahui terdapat 2 pesan yang dikirim sebelumnya dan 1 pesan yang dikirim baru. Pesan yang dikirim baru ini yang digunakan untuk dimasukan sebagai kode *password* verifikasi pada tahapan *login* di link http://localhost/coba/index-step2.php?id=2. Adapun tampilan dapat di lihat pada gambar 4.6 berikut :



Gambar 4.7 Isi pesan berupa kode OTP *email* dari akun hafizunpab

Tahapan selanjutnya ditemukan kode OTP = 164258, diinputkan ke isian kotak dialog *password* pada isian *login* step2. Kode OTP ini hanya berlaku jika *systemwebsite* tidak te*refresh* pada tampilan *login* step-1, atau index.php. Jika kode OTP yang dikirim terverifikasi valid dan sesuai dengan *database* MAMP *system*. Maka akan muncul halaman selanjutnya yaitu halaman admin.

3. Halaman Antarmuka Admin Area

Pada tahapan selanjutnya, di halaman admin akan tampil beberapa menu yang terdiri dari *Home*, *Akun*, *Logout*. Dan Notifikasi yang menginfokan “Selamat datang di Admin Area, Anda *login* sebagai Administrator”. Adapun tampilan dapat di lihat pada gambar 4.8 sebagai berikut :

Gambar 4.8 Halaman antarmuka admin area

Tahap selanjutnya di klik Menu Akun untuk melihat antarmuka halaman *page* akun *email* yang terdaftar pada *database* MAMP *System*.

4. Menu Halaman Antar Muka Akun

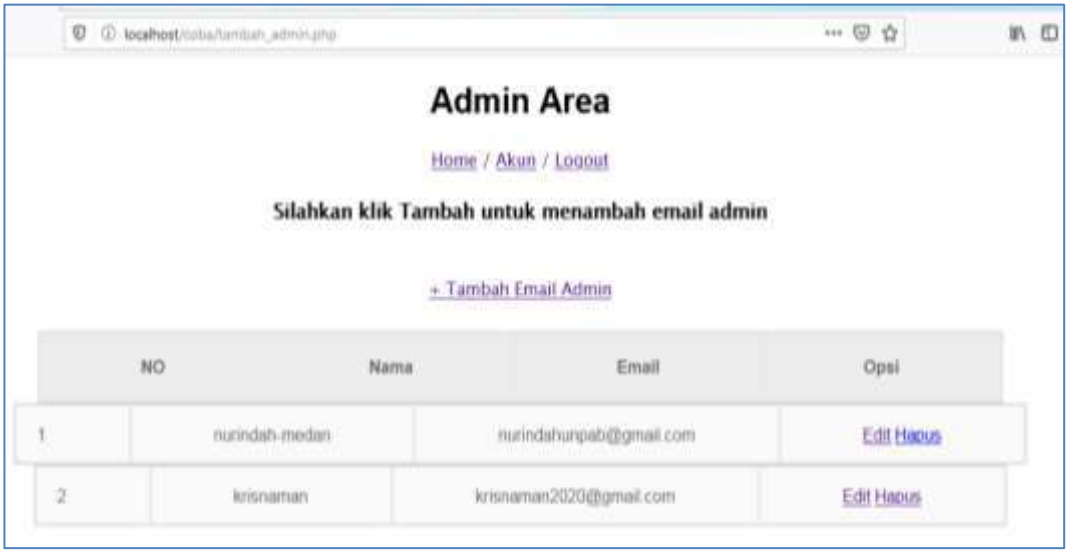
Pada halaman ini, difokuskan untuk menambah akun *email*, dan pilihan aksi untuk mengedit *email* yang terdaftar pada *database* MAMP *system*, dan juga menghapus akun *email* yang terdaftar pada *database*. Adapun tampilan dapat di lihat pada gambar 4.9 sebagai berikut :

Gambar 4.9 Halaman antarmuka akun *website*

Pada gambar 4.9 tersebut kemudian di klik Menu Tambah *Email* Admin, kemudian akan diarahkan ke link http://localhost/coba/tambah.php, dilanjutkan dengan mengisi *form* isian Nama=Krisnaman dan Alamat *Email*=krisnaman2020@gmail.com , dilanjutkan dengan di klik tombol Simpan. Sehingga data yang di isi akan di *entry* kedalam *database system* MAMP.

Gambar 4.10 Tambah data *email* admin pada admin area

Kemudian link tampilan *website* Admin Area kembali ke halaman http://localhost/coba/tambah_admin.php Adapun tampilan dapat di lihat pada gambar sebagai berikut :

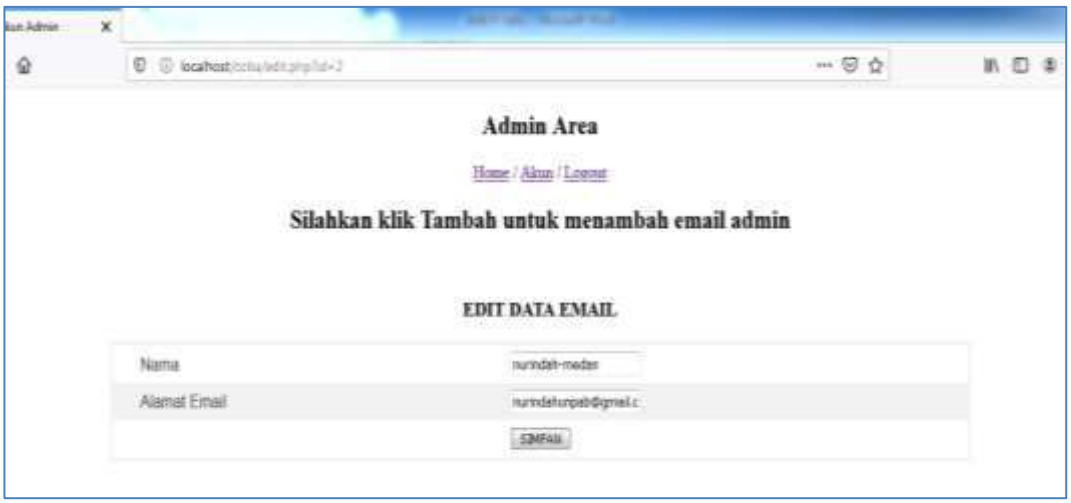


Gambar 4.11 Akun *email* baru berhasil ditambahkan

Akun email yang ke-2 adalah akun *email* baru yang ditambahkan yaitu nama Krisnaman dan *Email* = Krisnaman2020@gmail.com . Langkah selanjutnya yaitu melakukan pengeditan pada Akun *Email*, pada pembahasan ini di klik pada no 1 yaitu *email* = nurindahunpab@gmail.com dengan di klik opsi *Edit* kemudian ubah nama pengguna *email* dan *email* lama. Adapun tampilan *edit* akun admin awal dapat di lihat pada gambar berikut :

Gambar 4.12 Halaman edit data *email*

Tahapan selanjutnya diubah nama akun nurindah dengan nurindah-medan, kemudian Alamat *Email* tidak terjadi di buat perubahan. Adapun tampilan dapat di lihat pada gambar 4.13 berikut :



Gambar 4.13 Isian edit data *email*

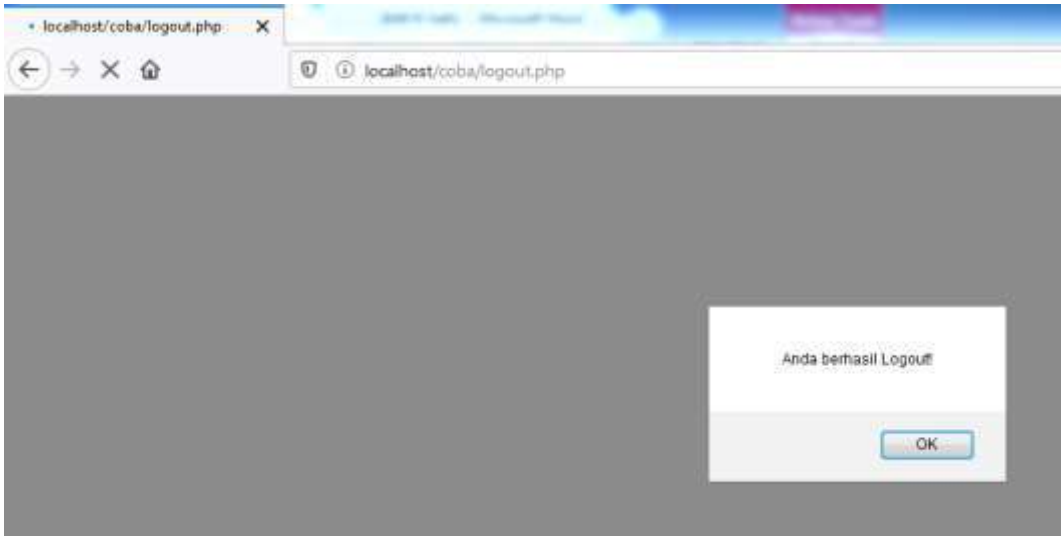
Tahap berikutnya yaitu menghapus akun *email* yang ditambahkan sebelumnya yaitu krisnaman2020@gmail.com. Pilih daftar akun *email* no.2 kemudan di klik Hapus pada pilihan menu opsi. Kemudian tampilan *refresh* dari Admin Area dapat di lihat pada gambar 4.14 berikut :

Gambar 4.14 Tampilan admin area setelah di*remove* 1 akun *email*

Tahapan selanjutnya yaitu melakukan pengujian menu *logout system website* OTP.

5. Tampilan pengujian *LogOut System*

   Adapun tampilan *logout system* dapat dilihat pada gambar 4.15 berikut :



Gambar 4.15 Tampilan *logout system prototype website* OTP

Pada gambar 4.15 diketahui tampilan *logout system*, untuk melakukan pengujian ini, di klik menu *logout* pada halaman admin *web*. Kemudian akan muncul notifikasi "Admin berhasil *logout*", kemudian klik OK. Untuk melanjutkan keluar dari *system*. Jika berhasil keluar dari *system* maka akan muncul kembali ke tampilan awal *system*. Adapun tampilan dapat di lihat pada gambar 4.16 berikut :

Gambar 4.16 Tampilan halaman antarmuka muncul setelah *logout Web*

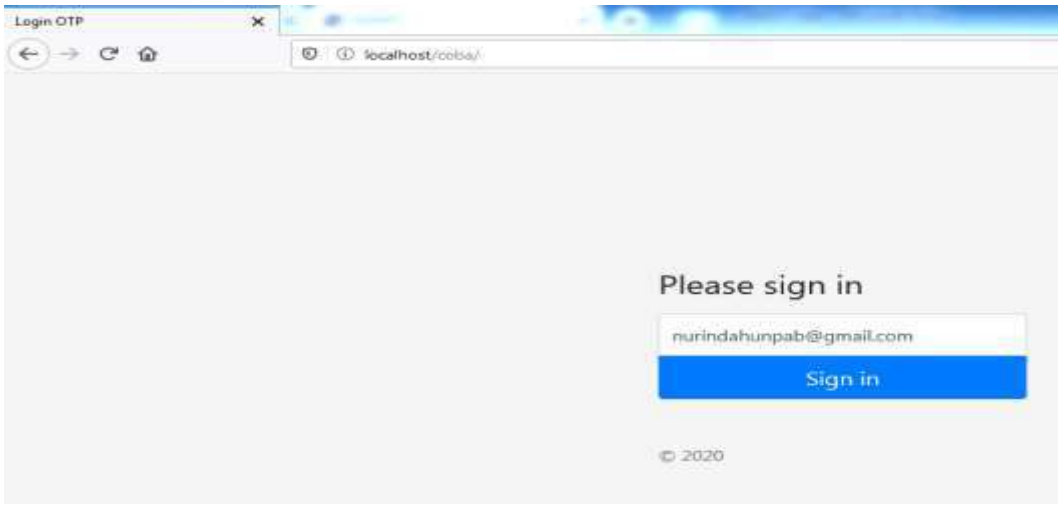
Pada gambar 4.16 diketahui *logout* berhasil jika dilakukan *back* pada *browser system Mozilla firefox*, tidak dapat mengakses tampilan halaman Administrasi kembali tanpa akses *login* OTP.

4.2.2 Pengamanan kode OTP dengan MD5 *Hash* pada *database*

Dalam penelitian ini, saya melakukan pengujian 5 data *login* dengan akun *email*= nurindahunpab@gmail.com. Dalam hal ini akan dicocokan kode OTP yang dikirim random (acak) dari *database* dengnan yang diterima oleh akun *email*nurindahunpab@gmail.com dalam mendekripsikan kode MD5 hash yang ada di *database* ini saya menggunakan *website online* MD5. Adapun tampilan percobaan dapat di lihat pada gambar berikut ini :

1. *Login ke Prototype Website* OTP dengan Percobaan ke-1

Adapun dalam percobaan ke-1 tahap awal diinputkan *email* kedalam *form login* pada tampilan awal *protoype website* OTP. Adapun tampilan dapat di lihat pada gambar 4.17 berikut:



Gambar 4.17 *Sign in* pada percobaan ke-1

Setelah diinputkan data ke-1 pada gambar 4.17 di atas maka akan dikirimkan perintah untuk melakukan random kode OTP berupa MD5 *Hash* tersimpan ke dalam *database* dan juga mengirim data kode OTP ke *email*. Adapun hasil kode OTP yang tersimpan dalam bentuk *hashing* pada waktu percobaan dapat dilihat pada tampilan gambar berikut :

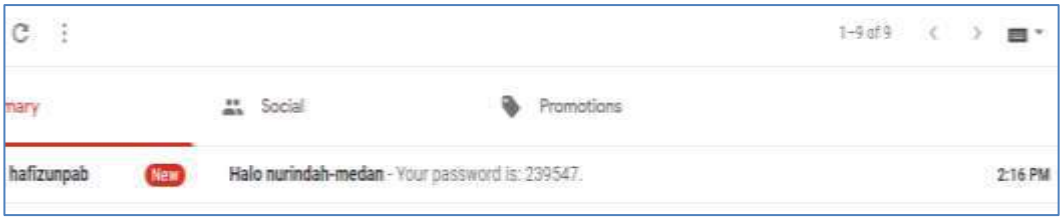
Gambar 4.18*TableUsers* yang pada *database* "otp" yang berisi kode OTP pada percobaan ke-1

Kode OTP yang tersimpan pada *database* pada gambar 4.18 diatas diketahui = 7e14fe6383100b17e0f49898489922a. kode OTP ini akan dibuktikan deskripsinya

menggunakan *website* MD *Decryption*, dalam hal ini saya menggunakan url link http://www.md5online.org . Adapun tampilan deskripsi pada percobaan ke-1 dapat dilihat pada gamabar berikut :

Gambar 4.19 Deskripsi MD5 dengan data percobaan ke-1

Data hasil percobaan dari gambar 4.19 kemudian ditemukan deskripsi dari kode OTP MD5 = 7e14fe6383100b17e0f49898489922a, nilai plainteks yang dihasilkan yaitu 239547. Nilai Kode OTP ini akan dicocokan dengan nilai kode OTP yang dikirim ke alamat email nurindahunpab@gmail.com . Adapun tampilan nilai kode OTP adalah sebagai berikut :

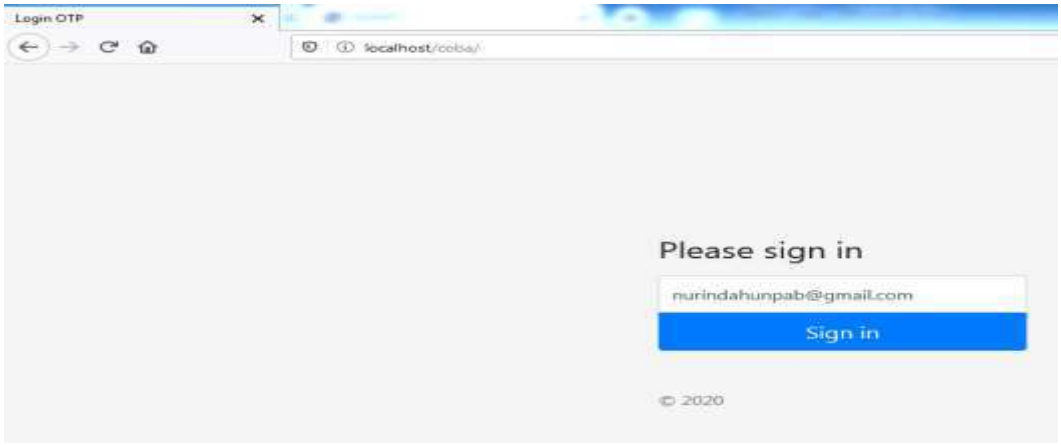


Gambar 4.20 Kode OTP yang diterima akun nurinda-medan pada percobaan ke-1

Dari hasil percobaan deksipris kode OTP MD5 dengan hasil kode OTP yang diterima oleh akun nurindahunpab@gmail.com diketahui nilai kode OTP adalah sama nilai (*balance)* yaitu 239547.

2. *Login ke Prototype Website* OTP dengan Percobaan ke-2

Adapun dalam percobaan ke-2 tahap awal diinputkan *email* kedalam *formlogin* pada tampilan awal *protoype website* OTP. Adapun tampilan dapat di lihat pada gambar 4.21 berikut:



Gambar 4.21 *Sign in* pada percobaan ke-2

Setelah diinputkan data ke-2 pada gambar 4.21 di atas maka akan dikirimkan perintah untuk melakukan random kode OTP berupa MD5 *Hash* tersimpan ke dalam *database* dan juga mengirim data kode OTP ke *email*. Adapun hasil kode OTP yang tersimpan dalam bentuk *hashing* pada waktu percobaan dapat dilihat pada tampilan gambar berikut :

Gambar 4.22*Table users* yang pada *database* "otp" yang berisi kode OTP pada percobaan ke-2

Kode OTP yang tersimpan pada *database* pada gambar 4.22 diatas diketahui = 58f759527fc21b9b8b7815503ed0de19. kode OTP ini akan dibuktikan deskripsinya menggunakan *website* MD *Decryption*, dalam hal ini saya

menggunakan url link http://www.md5online.org . Adapun tampilan deskripsi pada percobaan ke-2 dapat dilihat pada gambar berikut :

Gambar 4.23 Deskripsi MD5 dengan data percobaan ke-2

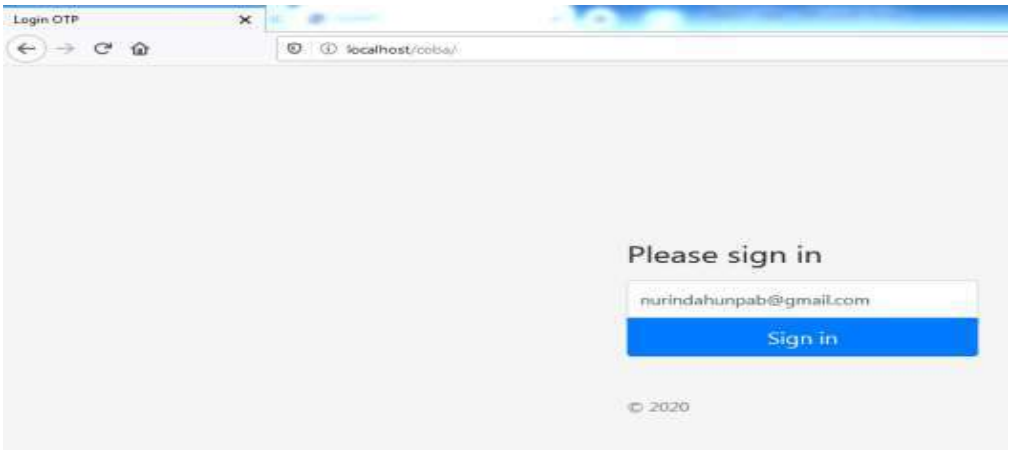
Data hasil percobaan dari gambar 4.23 kemudian ditemukan deskripsi dari kode OTP MD5 = 58f759527fc21b9b8b7815503ed0de19, nilai plainteks yang dihasilkan yaitu 874817. Nilai Kode OTP ini akan dicocokan dengan nilai kode OTP yang dikirim ke alamat *email*nurindahunpab@gmail.com . Adapun tampilan nilai kode OTP adalah sebagai berikut :

Gambar 4.24 Kode OTP yang diterima akun nurinda-medan pada percobaan ke-2

Dari hasil percobaan deksipri kode OTP MD5 dengan hasil kode OTP yang diterima oleh akun nurindahunpab@gmail.com diketahui nilai kode OTP adalah sama nilai (*balance)* yaitu 874817.

3. *Login* ke *Prototype Website* OTP dengan Percobaan ke-3

Adapun dalam percobaan ke-3 tahap awal diinputkan *email* kedalam *formlogin* pada tampilan awal *protoype website* OTP. Adapun tampilan dapat di lihat pada gambar 4.25 berikut:



Gambar 4.25 *Sign in* pada percobaan ke-3

Setelah diinputkan data ke-3 pada gambar 4.25 di atas maka akan dikirimkan perintah untuk melakukan random kode OTP berupa MD5 *Hash* tersimpan ke dalam *database* dan juga mengirim data kode OTP ke *email*. Adapun hasil kode OTP yang tersimpan dalam bentuk *hashing* pada waktu percobaan dapat dilihat pada tampilan gambar berikut :

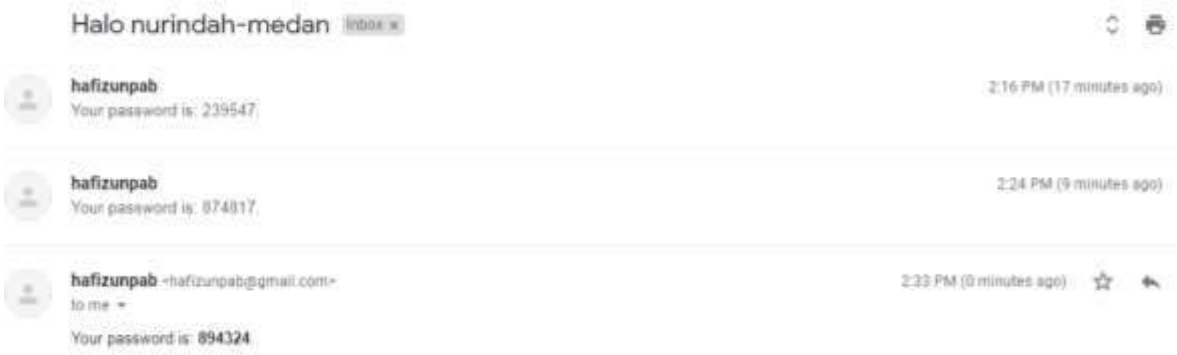
Gambar 4.26*Table users* yang pada *database* "otp" yang berisi kode OTP pada percobaan ke-3

Kode OTP yang tersimpan pada *database* pada gambar 4.26 diatas diketahui = 9e18dd21255242080c18d1d61d4733f3. kode OTP ini akan dibuktikan deskripsinya menggunakan *website* MD *Decryption*, dalam hal ini

sayamenggunakan url link http://www.md5online.org . Adapun tampilan deskripsi pada percobaan ke-3 dapat dilihat pada gamabar berikut :

Gambar 4.27 Deskripsi MD5 dengan data percobaan ke-3

Data hasil percobaan dari gambar 4.27 kemudian ditemukan deskripsi dari kode OTP MD5 = 9e18dd21255242080c18d1d61d4733f3, nilai plainteks yang dihasilkan yaitu 894324. Nilai Kode OTP ini akan dicocokan dengan nilai kode OTP yang dikirim ke alamat *email*nurindahunpab@gmail.com . Adapun tampilan nilai kode OTP adalah sebagai berikut :

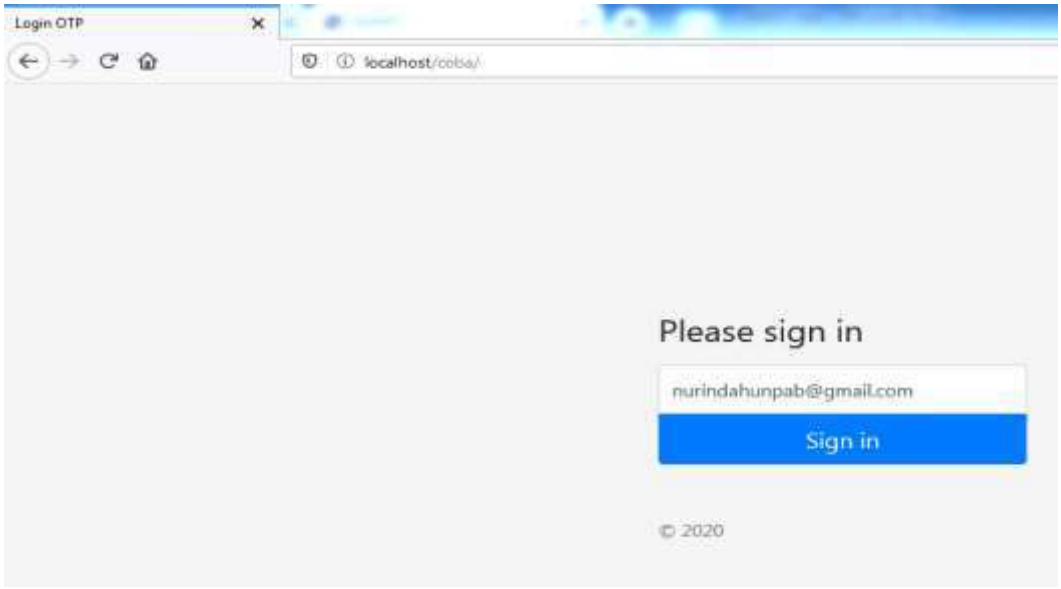


Gambar 4.28 Kode OTP yang diterima akun nurinda-medan pada percobaan ke-3

Dari hasil percobaan deksipri kode OTP MD5 dengan hasil kode OTP yang diterima oleh akun nurindahunpab@gmail.com diketahui nilai kode OTP adalah sama nilai (*balance)* yaitu 894324.

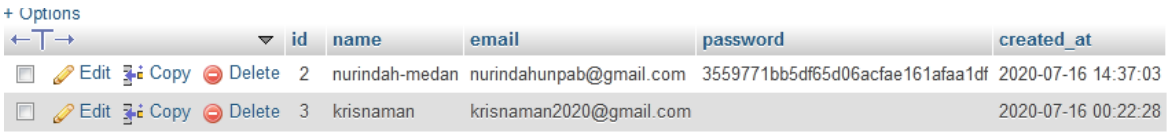
4. *Login* ke *Prototype Website* OTP dengan Percobaan ke-4

Adapun dalam percobaan ke-4 tahap awal diinputkan *email* kedalam *formlogin* pada tampilan awal *protoype website* OTP. Adapun tampilan dapat di lihat pada gambar 4.29 berikut:



Gambar 4.29 *Signin* pada percobaan ke-4

Setelah diinputkan data ke-4 pada gambar 4.29 di atas maka akan dikirimkan perintah untuk melakukan random kode OTP berupa MD5 *Hash* tersimpan ke dalam *database* dan juga mengirim data kode OTP ke *email*. Adapun hasil kode OTP yang tersimpan dalam bentuk *hashing* pada waktu percobaan dapat dilihat pada tampilan gambar berikut :

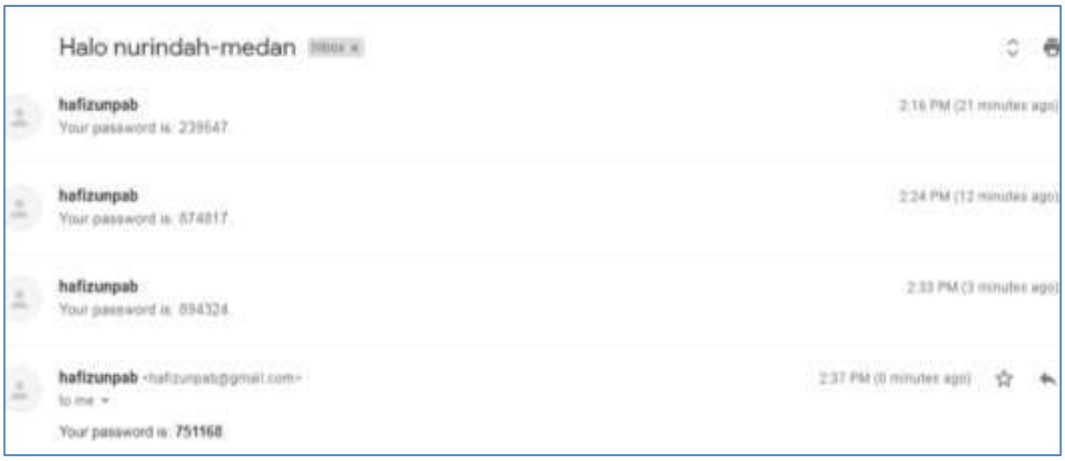


Gambar 4.30*Table users* yang pada database "otp" yang berisi kode OTP pada percobaan ke-4

Kode OTP yang tersimpan pada *database* pada gambar 4.30 diatas diketahui yaitu =3559771bb5df65d06acfae161afaa1df. kode OTP ini akan dibuktikan deskripsinya menggunakan *website* MD *Decryption*, dalam hal ini saya menggunakan url link http://www.md5online.org . Adapun tampilan deskripsi pada percobaan ke-4 dapat dilihat pada gambar berikut :

Gambar 4.31 Deskripsi MD5 dengan data percobaan ke-4

Data hasil percobaan dari gambar 4.31 kemudian ditemukan deskripsi dari kode OTP MD5 = 3559771bb5df65d06acfae161afaa1df, nilai plainteks yang dihasilkan yaitu 751168. Nilai Kode OTP ini akan dicocokan dengan nilai kode OTP yang dikirim ke alamat *email*nurindahunpab@gmail.com . Adapun tampilan nilai kode OTP adalah sebagai berikut :

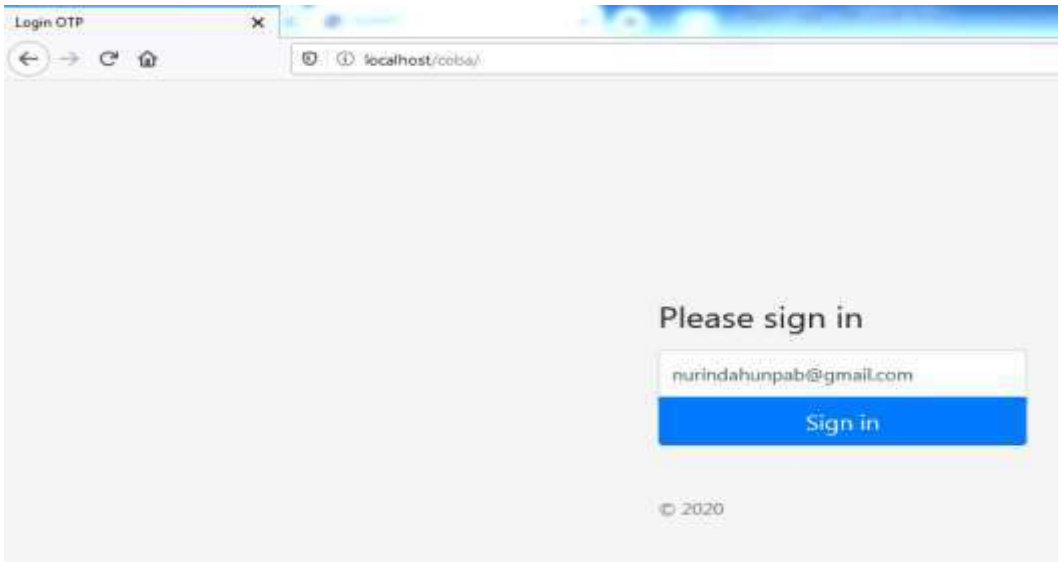


Gambar 4.32 Kode OTP yang diterima akun nurinda-medan pada percobaan ke-4

Dari hasil percobaan deksipri kode OTP MD5 dengan hasil kode OTP yang diterima oleh akun nurindahunpab@gmail.com diketahui nilai kode OTP adalah sama nilai (*balance)* yaitu 751168.

5. *Login* ke *Prototype Website* OTP dengan Percobaan ke-5

Adapun dalam percobaan ke-5 tahap awal diinputkan *email* kedalam *form login* pada tampilan awal *protoype website* OTP. Adapun tampilan dapat di lihat pada gambar 4.33 berikut:



Gambar 4.33 *Sign in* pada percobaan ke-5

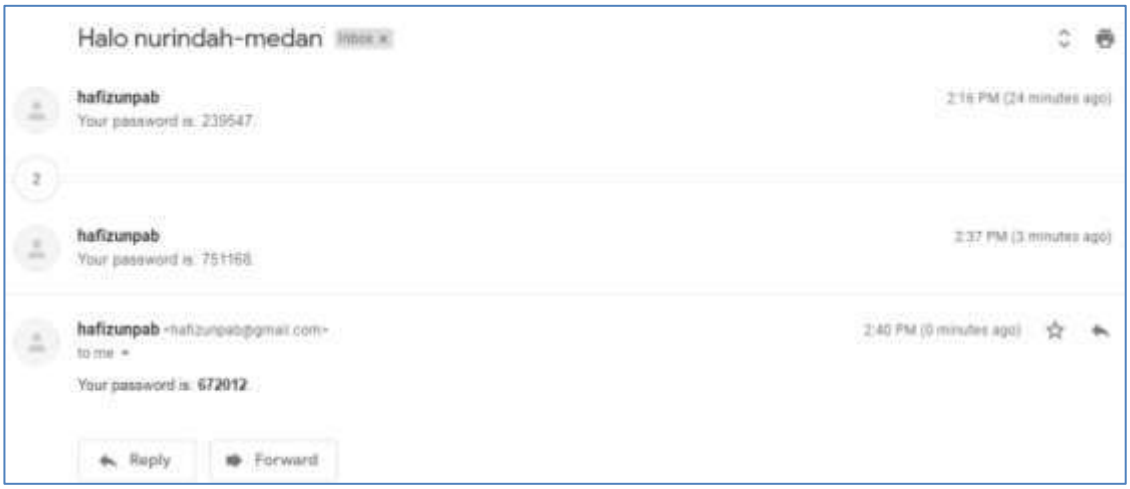
Setelah diinputkan data ke-5 pada gambar 4.33 di atas maka akan dikirimkan perintah untuk melakukan random kode OTP berupa MD5 *Hash* tersimpan ke dalam *database* dan juga mengirim data kode OTP ke *email*. Adapun hasil kode OTP yang tersimpan dalam bentuk *hashing* pada waktu percobaan dapat dilihat pada tampilan gambar berikut :

Gambar 4.34*Tableusers* yang pada *database* "otp" yang berisi kode OTP pada percobaan ke-5

Kode OTP yang tersimpan pada *database* pada gambar 4.34 diatas diketahui = 01b9a18da0741c8c1c890fc71952c297 . kode OTP ini akan dibuktikan deskripsinya menggunakan *website* MD *Decryption*, dalam hal ini saya menggunakan url link http://www.md5online.org . Adapun tampilan deskripsi pada percobaan ke-5 dapat dilihat pada gamabar berikut :

Gambar 4.35 Deskripsi MD5 dengan data percobaan ke-5

Data hasil percobaan dari gambar 4.35 kemudian ditemukan deskripsi dari kode OTP MD5 = 01b9a18da0741c8c1c890fc71952c297, nilai plainteks yang dihasilkan yaitu 672012. Nilai Kode OTP ini akan dicocokan dengan nilai kode OTP yang dikirim ke alamat *email*nurindahunpab@gmail.com . Adapun tampilan nilai kode OTP adalah sebagai berikut :



Gambar 4.36 Kode OTP yang diterima akun nurinda-medan pada percobaan ke-5

Dari hasil percobaan deksipri kode OTP MD5 dengan hasil kode OTP yang diterima oleh akun nurindahunpab@gmail.com diketahui nilai kode OTP adalah sama nilai (*balance)* yaitu 672012.

6. Tabulasi Tabel Percobaan

Adapun hasil percobaan untuk mendapatkan data ke-1, data ke-2, data ke-3, data ke-4, data ke-5 dapat disajikan dalam tabel 4.1 sebagai berikut :

Tabel 4.1 Tabulasi Hasil Percobaan

No	Percobaan	Kode OTP	
		MD5 Hash	Plainteks
1	Percobaan ke-1	7e14fe6383100b17e0f49898489922a	239547
2	Percobaan ke-2	58f759527fc21b9b8b7815503ed0de19	874817
3	Percobaan ke-3	9e18dd21255242080c18d1d61d4733f3	894324
4	Percobaan ke-4	3559771bb5df65d06acfae161afaa1df	751168
5	Percobaan ke-5	01b9a18da0741c8c1c890fc71952c297	672012

BAB V

KESIMPULAN DAN SARAN

5.1 Kesimpulan

Adapun beberapa hasil kesimpulan yang dapat diambil dari pembahasan penelitian ini yaitu :

1. Sistem *prototype Login* dengan pengamanan OTP berbasis *website* berjalan sesuai dengan algoritma yang dirancang.
2. Pengiriman Kode OTP dilakukan menggunakan *email*hafizunpab@gmail.com ke tujuan *email* admin yang mengakses *login* portal admin, dengan syarat *email* yang diinputkan sesuai dengan *email* yang terdaftar pada *databasesystem*.
3. Kode OTP pada saat pengiriman ke *email* tujuan sudah dienkripsi menggunakan algoritma Md5 *Hash*.

5.2 Saran

Adapun saran dari pembahasan mengenai penelitian ini yaitu :

1. Hendaknya penelitian ini dapat diterapkan ke bahasa pemrograman lainnya seperti android.
2. Notifikasi pengiriman kode OTP pada penelitian ini masih memanfaatkan media *email*dan dapat dikembangkan ke notifikasi kode lainnya menggunakan AP flatform lainnya seperti Whatsapp dan Telegram.

DAFTAR PUSTAKA

Aryza, S., Hermansyah, H., Siahaan, A. P. U., Suherman, S., & Lubis, Z. (2017). Implementasi Energi Surya Sebagai Sumber Suplai Alat Pengering Pupuk Petani Portabel. IT Journal Research and Development, 2(1), 12-18.

Hamid. (2017). *ANALISIS KEAMANAN APLIKASI EMAIL BAWAAN ANDROID DAN GMAIL PADA JARINGAN NIRKABEL*. *23*, 125–136.

Hendini, A. (2016). PEMODELAN UML SISTEM INFORMASI MONITORING PENJUALAN DAN STOK BARANG (STUDI KASUS: DISTRO ZHEZHA PONTIANAK). *Khatulistiwa Informatika*, *IV*(2), 107–116. https://doi.org/10.2135/cropsci1983.0011183x002300020002x

Id, I. D., & Mahdiyah, E. (2016). Implementasi TOTP (Time-Based One-Time Password) Untuk Meningkatkan Keamanan Transaksi E-Commerce. *Konferensi Nasional Sistem & Informasi 2016, August 2016*, 11–13.

Kurnia, D. (2017). Analisis QoS Pada Pembagian Bandwidth Dengan Metode Layer 7 Protocol, PCQ, HTB Dan Hotspot Di SMK Swasta Al-Washliyah Pasar Senen. CESS (Journal of Computer Engineering, System and Science), 2(2), 102-111.

Ismaredah, E. (2015). KEAMANAN E-MAIL MENGGUNAKAN METODE ENKRIPSI GNUPG DENGAN SQUIRELL MAIL DAN THUNDERBIRD. *Jurnal Jupiter*, 13–22.

Ismawan, F. (2018). Implementasi Konsep No Programming Dalam Membangun Perangkat Lunak Email Berbasis Android. *Faktor Exacta*, *11*(3), 214–224. https://doi.org/10.30998/faktorexacta.v11i3.2744

Lalang Erawan, S. (2018). Prototype Aplikasi Web pengaman data pribadi dengan Kriptografi One Time Pad. *Prosiding SNATIF Ke-5 Tahun 2018*, 423–430. https://doi.org/10.2298/PAN0903301G

Meiyanti, R., Subandi, A., Fuqara, N., Budiman, M. A., & Siahaan, A. P. U. (2018, March). The recognition of female voice based on voice registers in singing techniques in real-time using hankel transform method and macdonald function. In Journal of Physics: Conference Series (Vol. 978, No. 1, p. 012051). IOP Publishing.

Musliyana, Z., Arif, T. Y., & Munadi, R. (2016). Peningkatan Sistem Keamanan Autentikasi Single Sign On (SSO) Menggunakan Algoritma AES dan One-Time Password Studi Kasus: SSO Universitas Ubudiyah Indonesia. *Jurnal Rekayasa Elektrika*, *12*(1), 21. https://doi.org/10.17529/jre.v12i1.2896

Radhito, D., Widiyanto, A., & Pujiarto, B. (2019). SISTEM NOTIFIKASI SMS TERHADAP TINDAKAN PENYUSUPAN PADA JARINGAN KOMPUTER DI BIRO TIK UNIVERSITAS MUHAMMADIYAH MAGELANG. *Jurnal Komtika*. https://doi.org/10.31603/komtika.v2i2.2593

Rahmatulloh, A., Rachman, A. N., & Anwar, F. (2019). Implementasi Web Push Notification pada Sistem Informasi Manajemen Arsip Menggunakan PUSHJS. *Jurnal Teknologi Informasi Dan Ilmu Komputer*. https://doi.org/10.25126/jtiik.201963936

Ratumurun, S. (2015). Sistem Informasi Akuntansi Permintaan Barang dari Gudang pada PT. Mauwasa Sejahtera Ambon. *Cita Ekonomika, Jurnal Ekonomi*, *IX*(1), 57–64

Rusdi, M., Sirajudin, H., & Amin, M. (2020). PROTOTYPE APLIKASI PEMESANAN DAN PENGIRIMAN SERBUK KAYU OLEH CV. USAHA BERSAMA SEBAGAI SUPLIER PT. FUMAKILLA. Technologia: Jurnal Ilmiah, 11(3), 152-158.

Santoso, S., & Nurmalina, R. (2017). Perencanaan dan Pengembangan Aplikasi Absensi Mahasiswa Menggunakan Smart Card Guna Pengembangan Kampus Cerdas (Studi Kasus Politeknik Negeri Tanah Laut). *Jurnal Integrasi*, *9*(1), 84–91.

Sudiarto Raharjo, W., E.K. Ratri, I. D., & Susilo, H. (2017). Implementasi Two Factor Authentication Dan Protokol Zero Knowledge Proof Pada Sistem Login. *Jurnal Teknik Informatika Dan Sistem Informasi*, *3*(1), 127–136. https://doi.org/10.28932/jutisi.v3i1.579

Suendri. (2018). Implementasi Diagram UML (Unified Modelling Language) Pada Perancangan Sistem Informasi Remunerasi Dosen Dengan Database Oracle (Studi Kasus: UIN Sumatera Utara Medan). *Jurnal Ilmu Komputer Dan Informatika*, *3*(1), 19. http://jurnal.uinsu.ac.id/index.php/algoritma/article/download/3148/1871

Verawati, & Liksha, P. D. (2018). Aplikasi Akuntansi Pengolahan Data Jasa Service Pada Pt. Budi Berlian Motor Lampung. *Jurnal Sistem Informasi Akuntansi (JUSITA)*, *1*(1), 1–14.