



**PENGAMANAN WEB PAGE LOGIN MENGGUNAKAN
KOMBINASI ALGORITMA MD5 DAN BASE64
BERBASIS WEB SERVER LOKAL**

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

SKRIPSI

OLEH

**NAMA : TARCISIUS P. SIHOMBING
NPM : 1614370285
PROGRAM STUDI : SISTEM KOMPUTER**

**FAKULTAS SAINS DAN TEKNOLOGI
UNIVERSITAS PEMBANGUNAN PANCA BUDI
MEDAN
2020**

ABSTRAK

Web Page Login adalah suatu proses untuk masuk kedalam halaman *website* yang dapat menampilkan gambar, teks dan bahkan suara. *Login* dimaksud untuk mengatur proses identifikasi yang terdiri dari *username* dan *password* harus dengan tepat untuk mendapat hak akses ketika masuk ke dalam *website*.

Pengamanan *Web Page Login* sangat penting untuk menjaga validitas dan integritas data serta menjamin ketersediaan layanan bagi penggunanya. Kombinasi antara Algoritma *Message Digest* (MD5) dan *Base 64* sangat mendukung dalam penggunaan keamanan *username* dan *password* pada sebuah *web page login* yang berbasis *web server* lokal. Keamanan *web page login* antara *username* dan *password* yang telah dienkripsi akan lebih terjaga karena dengan menggunakan md5 dan base 64 membutuhkan proses waktu yang cukup lama jika ada pihak yang ingin meretas *web server* tersebut. *Web server* adalah perangkat lunak (*software*) dalam server yang memberikan layanan berbasis data dan berfungsi untuk menerima permintaan (*request*) berupa halaman.

Dengan menggunakan Kombinasi *Message digest* (MD5) dan *Base 64* diharapkan dapat meningkatkan pengamanan pada sebuah *web server* lokal.

Kata Kunci : *Web Page Login*. Algoritma *Md5* dan *base65*, *web server*.

DAFTAR ISI

LEMBAR JUDUL

LEMBAR PENGESAHAN

KATA PENGANTAR iii

DAFTAR ISI v

DAFTAR TABEL ix

DAFTAR GAMBAR x

BAB 1 PENDAHULUAN 1

1. Latar Belakang 1

2. Rumusan Masalah 2

3. Batasan Masalah 2

4. Tujuan Penelitian 3

5. Manfaat Penelitian 3

BAB 2 LANDASAN TEORI 4

1. Keamanan Sistem 4

2. Kriptografi 4

3. Pengertian Web Page 5

4. Pengertian Login 6

5. Pengertian Algoritma 6

6. Defenisi Algoritma 7

7. Tugas Algoritma 7

8. Rekayasa Algoritma 8

9. Message Digest 5 (MD5)	8
a. Cara Kerja message Digest 5 (MD5)	9
b. Pengertian Fungsi Hash	11
10. Pengertian Algoritma Base64	12
11. Konsep Enkripsi dan Deskripsi.....	14
12. Web Server.....	14
13. Pengertian IP Address.....	18
14. Sistem Operasi Ubuntu	19
15. Flowchart	20
16. Unified Modeling Language	21
BAB 3 METODE PENELITIAN	24
1. Tahapan Penelitian.....	24
2. Metode Pengumpulan Data.....	27
3. Analisis Yang Sedang Berjalan.....	27
4. Rancangan Penelitian.....	28
5. UML (Unified Modelling Language)	28
a. Use Case Diagram.....	29
b. Activity Diagram.....	30
c. Sequence Diagram.....	31
d. Class Diagram	32
6. Rancangan Desain Database	33

7. Rancangan Relasi Database	37
8. Rancangan Flowchart.....	38
a. Perancangan konfigurasi MD5 dan Base64	39
9. Rancangan Topologi Jaringan.....	40
10. Rancangan Security.....	41
BAB 4 HASIL dan PEMBAHASAN	43
1. Kebutuhan Spesifikasi Minimum Kebutuhan	43
2. Implementasi Sistem	44
a. Setting Dns Server.....	44
b. Setting Web Server	53
3. Pengujian Aplikasi	57
4. Hasil Pengujian Aplikasi.....	60
a. Home	60
b. Halaman Data Form buku	61
c. Halaman Data Form Anggota	62
d. Halaman Data Form Transaksi.....	62
e. Halaman Data Form Laporan.....	63
f. Halaman Form User	63
5. Perhitungan Manual Enkripsi dan Deskripsi Md5 dan Base64	64
BAB 5 KESIMPULAN DAN SARAN	69
1. Kesimpulan	69

2. Saran.....	69
DAFTAR PUSTAKA	71
LAMPIRAN.....	73

DAFTAR TABEL

1. Daftar Simbol Flowchart.....	21
2. Daftar Simbol Unified Modeling Language	23
3. Rancangan Form Anggota	34
4. Rancangan Form Buku	35
5. Rancangan Form Transaksi.....	35
6. Rancangan Form Laporan	36
7. Rancangan Form User.....	36
8. Rancangan Relasi Antar Tabel.....	37
9. Tabel Pengujian Aplikasi.....	57

DAFTAR GAMBAR

11. Proses HMD5	10
12. Tahapan Penelitian.....	24
13. Use Case Diagram Berbasis Web Server Lokal.....	29
14. Activity Diagram	31
15. Squence Diagram	32
16. Class Diagram	32
17. Rancangan Form Login Pada Web Server	33
18. Rancangan Halaman Menu Utama	34
19. Flowchart Sistem Login Yang Dibangun	38
20. Diagram Alir Perancangan Konfigurasi Login	39
21. Rancangan Topologi Jaringan.....	41
22. Pengujian Client.....	53
23. Rancangan Web Login.....	59
24. Halaman Login Admin	60
25. Halaman Home	60
26. Halaman Data Buku	61
27. Halaman Data Anggota.....	62
28. Halaman Data Transaksi	62
29. Halaman Data Laporan	63
30. Halaman Data User	64

KATA PENGANTAR

Puji dan syukur Tuhan yang Maha Esa atas berkat dan kasih anugrahnya Penulis masih diberi kesehatan dan keselamatan sehingga penulis dapat menyelesaikan skripsi ini dengan baik dan lancar.

Selesainya penulisan skripsi ini telah banyak dibantu oleh pihak-pihak tertentu. Pada kesempatan ini, penulis ingin mengucapkan banyak terimakasih kepada pihak-pihak yang telah banyak membantu dan mendoakan penulis dalam menyelesaikan skripsi ini.

Dalam kesempatan ini, penulis mengucapkan terimakasih yang sebesar besarnya kepada banyak pihak yang telah membantu dalam penyelesaian penyusunan skripsi ini. Penulis ingin mengucapkan terimakasih kepada :

1. Kepada orang tua tercinta yaitu Ayahanda Pentar Sihombing dan Ibunda Milianur Sitanggung yang selama ini memberi dorongan baik berupa materi, motivasi, saran, serta doa sehingga penulis dapat menyelesaikan skripsi ini.
2. Bapak Dr. H. Muhammad Isa Indrawan, S.E., M.M, selaku Rektor Universitas Pembangunan Panca Budi Medan.
3. Bapak Hamdani S.T., MT selaku Dekan Fakultas Sains dan Teknologi Universitas Pembangunan Panca Budi Medan.

4. Bapak Eko Hariyanto, S.Kom., M.Kom selaku Ketua Program Studi Komputer yang telah banyak member dukungan dalam menyelesaikan skripsi ini.
5. Bapak Dian Kurnia, S.Kom., M.Kom selaku Dosen Pembimbing I penulis, yang telah banyak memberi bimbingan dan arahan kepada penulis dalam menyelesaikan skripsi ini.
6. Ibu Sry Wahyuni, S.Kom., M.Kom selaku Dosen Pembimbing II penulis yang telah banyak member bimbingan dan arahan kepada penulis dalam menyelesaikan skripsi ini.
7. Seluruh Dosen Universitas Pembangunan Panca Budi Medan yang telah memberikan ilmunya kepada penulis.
8. Kepada seluruh teman seperjuangan yang ikut serta dalam mendoakan dan membantu penulisan skripsi ini, yang tidak bisa penulis sebutkan satu persatu.

Penulis menyadari bahwa penyusunan skripsi ini belum sempurna baik dalam penulisan maupun isi. Oleh karena itu penulis berharap kritik dan saran yang bersifat membangun dari berbagai pihak sehingga dapat memperbaiki dan menyempurnakan skripsi ini agar dapat bermanfaat bagi diri sendiri dan bagi setiap siapapun yang membacanya.

Medan, Juni 2020
Penulis,

TARCISIUS P. SIHOMBING
1614370285

BAB 1

PENDAHULUAN

1.1 Latar Belakang

Pengamanan sangat perlu dilakukan terhadap *web page* baik itu untuk pribadi atau untuk perusahaan. Untuk mengamankan *web page login* dibutuhkan suatu cara yang dapat menghindari dari penyalahgunaan *web page* tersebut. Teknik algoritma adalah salah satu yang dapat digunakan untuk menghindari *web page* dari penyalahgunaan tersebut. *Web Page* ini dibuat dengan menggunakan suatu format standar HTML (*Hipertext Mark-up Language*) dimana dokumen HTML tersebut tersimpan dalam sebuah server.

Kombinasi Algoritma Md5 dan Base64 adalah proses yang terlibat dalam pengamanan *web page login*. Proses algoritma md5 adalah salah satu penggunaan fungsi hash satu arah yang paling banyak digunakan dalam menjaga integritas data. Algoritma Base64 merupakan salah satu algoritma untuk *Encoding* dan *Decoding* suatu data ke dalam format ASCII, yang didasarkan pada bilangan dasar 64 atau bisa dikatakan sebagai salah satu metode yang digunakan untuk melakukan *encoding* (penyandian) terhadap data binary. (Aulia et al., 2018)

Kriptografi adalah salah satu aspek yang sangat penting dalam menjaga kerahasiaan, integritas data dan autentikasi. Kerahasiaan merupakan layanan yang digunakan untuk menjaga isi dari informasi dari siapapun kecuali memiliki otoritas atau kunci rahasia untuk membuka informasi yang sudah di sandi. Integritas data merupakan kemampuan untuk mendeteksi manipulasi data dari pihak-pihak yang tidak berhak antara lain penyisipan, penghapusan dan

pengsubstitusian data lain kedalam data yang sebenarnya. Autentikasi adalah berhubungan dengan identifikasi atau pengenalan baik secara kesatuan sistem maupun informasi itu sendiri. Dua pihak yang saling berkomunikasi harus memperkenalkan diri dan harus diautentikasi keasliannya, isi data dan waktu pengirimannya. (Rifki, 2016)

Salah satu mekanisme untuk meningkatkan keamanan adalah dengan menggunakan teknologi enkripsi. Data-data yang dikirimkan diubah sedemikian rupa sehingga tidak mudah disadap. Berdasarkan latar belakang yang sudah dikemukakan, maka penulis mengambil penelitian dengan judul **“Pengamanan Web Page Login Menggunakan Kombinasi Algoritma MD5 dan Base64 Berbasis Web Server Lokal”**

1.2 Rumusan Masalah

Berdasarkan latar belakang di atas, maka dapat dirumuskan masalah sebagai berikut:

1. Bagaimana membangun sebuah pengamanan *web page login* berbasis *web server* lokal ?
2. Bagaimana cara base64 cara menyandikan sebuah web tersebut?
3. Bagaimana cara mengkombinasikan algoritma md5 dan base64 ?

1.3 Batasan Masalah

Adapun batasan masalah yang digunakan dalam penulisan tugas akhir ini adalah sebagai berikut:

1. Pengamanan web page login menggunakan kombinasi algoritma MD5 dan Base64
2. Pengamanan web page login tersebut berbasis lokal.
3. Program aplikasi yang digunakan adalah menggunakan virtual Box dan ubuntu.

1.4 Tujuan Penelitian

Adapun tujuan penelitian yang digunakan dalam penelitian tugas akhir adalah sebagai berikut:

- a. Membuat pengamanan *web page login* sebagai salah satu keamanan bagi pengguna *web server*
- b. Membantu pengguna *web page* agar lebih mudah mengamankan *web page* dari pihak yang tidak bertanggung jawab.
- c. Untuk melakukan pengamanan mengkombinasikan algoritma md5 dan base64.

1.5 Manfaat Penelitian

Adapun manfaat penelitian yang digunakan dalam penulisan tugas akhir ini adalah sebagai berikut:

- a. Penelitian ini bermanfaat untuk memberikan informasi tentang kombinasi algoritma md5 dan base64.
- b. Meningkatkan keamanan *web page login* yang berbasis *web server lokal*.
- c. Memberi kenyamanan bagi pemilik *web page* tersebut.

BAB II

LANDASAN TEORI

2.1 Keamanan Sistem

Masalah keamanan merupakan salah satu aspek penting dari sebuah sistem informasi, sayang sekali masalah keamanan ini seringkali kurang mendapat perhatian dari pemilik dan pengolah sistem informasi. Jatuhnya informasi ke pihak lain, misalnya pihak lawan bisnis yang dapat menimbulkan kerugian bagi pemilik informasi. Untuk itu keamanan dari sistem informasi yang digunakan harus terjamin dalam batas yang diterima. *Web server* dan *database server* bagaikan jantung dan otak dari organism internet. Dua komponen ini menjadi komponen pokok dari sebuah aplikasi internet yang tangguh dan tepatlah keduanya menjadi target *hacker*. Dalam beberapa kasus kita dapat menentukan titik-titik lemah dalam aplikasi yang bisa menjadi sasaran penyerang. (Ertie Nur Hartiwati, 2014)

2.2 Kriptografi

Kriptografi adalah ilmu yang mempelajari mengenai cara mengamankan suatu informasi. Pengamanan ini dilakukan dengan mengenkrip informasi tersebut dengan suatu kunci khusus. Informasi ini sebelum dienkrip dinamakan *plaintext* dan setelah dienkrip dengan suatu kunci dinamakan *ciphertext*. Ada empat tujuan mendasar dari ilmu kriptografi ini yang juga merupakan aspek keamanan informasi yaitu: (Inayatullah, 2007)

1. Kerahasiaan, adalah layanan yang digunakan untuk menjaga isi dari informasi dari siapapun kecuali yang memiliki otoritas atau kunci rahasia untuk membuka atau mengupas informasi yang telah disandi.
2. Integritas data, adalah berhubungan dengan penjagaan dari perubahan data secara tidak sah, istem harus memiliki kemampuan untuk mendeteksi manipulasi data oleh pihak-pihak yang tidak berhak, antara lain penyisipan, penghapusan, dan pensubtitusian data lain kedalam data yang sebenarnya.
3. Autentikasi, adalah berhubungan dengan identifikasi atau pengenalan, baik secara kesatuan sistem maupun informasi itu sendiri. Dua pihak yang saling berkomunikasi harus saling memperkenalkan diri. Informasi yang dikirimkan melalui kanal harus diautentikasi keaslian, isi datanya, waktu pengiriman dan lain-lain.
4. Non-repudiasi, adalah usaha untuk mencegah terjadinya penyangkalan terhadap pengiriman atau terciptanya suatu informasi oleh yang mengirimkan atau membuat.

2.3 Pengertian *Web Page*

Web page adalah suatu halaman yang ditampilkan pada suatu website di internet yang dapat menampilkan tulisan, teks, gambar video dan suara. Halaman web page ini juga di ibaratkan seperti halaman yang ada dalam buk. *Web page* digunakan untuk menunjukkan suatu halaman *web site*. Atau defenisi *web page* adalah sekelompok data yang dapat tampil pada *word wide web* dengan

menyebutkan alamatnya yang biasa dikenal dengan istilah URL (*uniform resource locator*). *Web page* ini dibuat dengan menggunakan suatu format standar HTML (*hypertext mark-up language*), dimana dokumen HTML tersebut tersimpan dalam sebuah server. Fungsi *web page* adalah untuk menunjukkan suatu halaman pada website yang dapat menampilkan tulisan atau teks gambar, dan video.

2.4 Pengertian Login

Login disebut juga dengan "*logon*" adalah istilah dalam hal keamanan komputer yakni berupa proses pintu masuk bagi pengguna untuk mengakses sebuah sistem komputer. *Login* dimaksudkan untuk mengatur proses identifikasi. Berbeda dengan *logout*, proses *login* membutuhkan hal spesifik tertentu. Dengan teknologi terkini, proses *login* semakin diperketat dengan enkripsi secara hardware. Dengan memasukkan identitas akun minimal terdiri dari *username* pengguna dan *password* untuk mendapatkan hak akses antara *username* dengan *password* untuk *login* harus tepat dan tidak dapat dipisahkan karena keduanya saling terkait.

2.5 Pengertian Algoritma

Algoritma adalah urutan langkah-langkah penyelesaian masalah secara sistematis dan logis, langkah-langkah penyelesaian masalah untuk kasus yang dapat diproses secara terkomputerisasi. Algoritma digunakan untuk perhitungan, pemrosesan data, dan penalaran otomatis. Algoritma sangat berperan dalam

pembangunan suatu *software*. Dalam dunia sehari-hari mungkin tanpa kita sadari algoritma telah masuk dalam kehidupan kita. (Nugroho1, 2015)

2.6 Defenisi Algoritma

Algoritma adalah urutan langkah-langkah logis penyelesaian masalah yang disusun secara sistematis dan logis. Kata logis merupakan kata kunci dalam algoritma. Langkah-langkah dalam algoritma harus logis dan harus dapat ditentukan bernilai salah atau benar. Dalam beberapa konteks, algoritma adalah spesifikasi urutan langkah untuk melakukan pekerjaan tertentu (Donald Ervin Knuth).

2.7 Tugas Algoritma

Tugas sederhana dapat diselesaikan dengan algoritma yang dihasilkan dengan beberapa menit, tingkat kompleksitas menjalankan tantangan yang panjang, namun sampai pada masalah yang sangat rumit sehingga mereka telah menghalangi matematikawan yang tak terhitung jumlahnya selama bertahun-tahun bahkan berabad-abad. Komputer modern menghadapi masalah pada tingkat keamanan dunia maya serta penanganan data besar, penyortiran set data yang efisien dan menyeluruh sedemikian besar sehingga komputer standar tidak dapat memprosesnya secara tepat waktu.

2.8 Rekayasa Algoritma

Ketika desain algoritma baru diterapkan dalam istilah praktis, disiplin terkait dikenal sebagai rekayasa algoritma. Meskipun organisasi yang lebih besar seperti *amazon* dan *google* mempekerjakan desainer dan insinyur khusus, mengingat tingkat kebutuhan mereka akan algoritma baru dan khusus. Seperti proses desain, rekayasa algoritma sering kali melibatkan akreditasi sains komputer, dengan latar belakang yang kuat dalam matematika dimana mereka ada sebagai profesi yang terpisah dan terspesialisasi, insinyur algoritma mengambil ide-ide konseptual dari desainer dan proses kreatif dari mereka yang akan dipahami oleh komputer. Dengan kemajuan teknologi digital yang mantap, para insinyur yang berdedikasi akan terus menjadi semakin umum.

2.9 Message Digest 5 (MD5)

Md5 adalah fungsi hash yang banyak digunakan dalam kriptografik secara luas dengan *hash value* 128 bit. Md5 menerima masukan berupa pesan dengan ukuran sembarang dan menghasilkan message yang panjangnya 128 bit. Pada standard internet (RFC 1321), md5 telah dimanfaatkan secara bermacam-macam pada aplikasi keamanan dan md5 juga umum digunakan untuk melakukan pengujian integritas sebuah file. Md5 adalah salah satu dari serangkaian algoritma *message digest* yang didesain oleh professor Ronald Rivest dari MIT. (Ridha,2014.)

2.9.1 Cara kerja *message digest* (md5)

Langkah-langkah yang dibutuhkan untuk pembuatan *message digest* secara garis besar : (Kurniawan, 2004)

1. Penambahan bit pengganjal (padding bits)

Pesan akan ditambahkan bit-bit tambahan sehingga panjang bit akan kongruen dengan $448, \text{ mod } 512$. Hal ini berarti pesan akan mempunyai panjang yang walaupun panjang dari pesan sudah kongruen dengan $488, \text{ mod } 512$ bit. Penambahan bit dilakukan dengan menambahkan 1 diawal dan diikuti 0 sebanyak yang diperlukan sehingga sepanjang pesan akan kongruen dengan $488, \text{ mod } 512$.

2. Penambahan nilai panjang pesan semula

Setelah penambahan bit, pesan masih membutuhkan 64 bit agar kongruen dengan kelipatan 512 bit. 64 bit tersebut merupakan perwakilan dari b (panjang pesan sebelum penambahan bit dilakukan). Bit-bit ini ditambahkan kedalam dua *word* (32 bit) dan ditambahkan dengan *low-order* terlebih dahulu. Penambahan pesan biasa disebut juga *MD Strengthening* atau Penguatan MD.

3. Inisialisasi penyangga (buffer) MD.

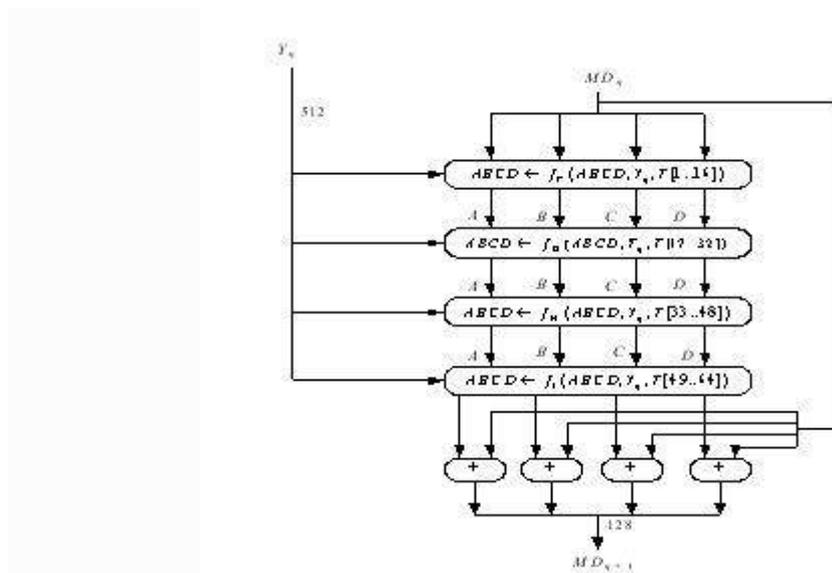
Pada md5 terdapat empat buah penyanggah(*buffer*) yang masing-masing panjangnya 32 bit. Total panjang penyangga adalah $4 \cdot 32 = 128$ bit. Keempat penyangga ini menampung hasil antara dan hasil akhir. Keempat penyangga ini diberi nama A, B, C, dan D. setiap penyangga diinisialisasi dengan nilai-nilai (dalam notasi HEX) sebagai berikut:

A = 01234567
 B = 89ABCBEF
 C = FEDCBA98
 D = 76543210

Register-register ini biasa disebut dengan nama *Chain variable* atau variable rantai

4. Pengolahan pesan dalam blok berukuran 512 bit.

Setiap blok 512 bit diproses bersama dengan penyangga MD menjadi keluaran 128 bit dan ini disebut proses HMD5 diperlihatkan pada gambar berikut ini.



Gambar 1. proses HMD5

(sumber. yusuf, 2004)

5. Proses pesan didalam blok 16 word
6. keluaran md5

Keluaran md5 adalah 128 bit dari word terendah A dan tertinggi word D masing-masing 32 bit.

Algoritma md5 yang utama beroperasi pada kondisi 128 bit, dibagi menjadi empat *word* 32 bit, menunjukkan A, B, C, D. Operasi tersebut diinisialisasi dijaga untuk tetap konstan. Algoritma utama kemudian beroperasi pada masing-masing blok pesan 512 bit masing-masing blok melakukan perubahan terhadap kondisi. Pemrosesan blok pesan terdiri atas empat tahap, batasan putaran, setiap putaran membuat 16 operasi serupa berdasarkan pada fungsi non-linier F, penambahan modular, dan rotasi ke kiri.

2.9.2 Pengertian Fungsi Hash

Hash adalah suatu teknik klasik dalam ilmu komputer yang banyak digunakan dalam praktek secara mendalam. Hash merupakan metode yang secara langsung mengakses record-record dalam suatu table dengan melakukan transformasi aritmatik pada key yang menjadi alamat dalam sebuah table tersebut. Key merupakan suatu input dari pemakaian dimana pada umumnya berupa nilai atau string karakter. Pelacakan dengan menggunakan Hash terdiri dari dua langkah utama, yaitu : (Prasetyo & Suryana, 2016)

1. menghitung Fungsi Hash.

Fungsi Hash adalah suatu fungsi yang mengubah key menjadi alamat dalam table. Fungsi hash memetakan sebuah key ke suatu alamat dalam table. Idealnya, key yang berbeda seharusnya dipetakan ke dalam alamat-alamat yang berbeda juga. Pada kenyataannya, tidak ada fungsi hash yang sempurna kemungkinan besar yang terjadi adalah dua atau lebih key yang berbeda dipetakan ke alamat yang sama dalam table. Peristiwa ini disebut dengan *collision resolution* (tabrakan).

Karena itulah diperlukan langkah-langkah berikutnya, yaitu *collision resolution* (pemecahan tabrakan).

2. *Collision Resolution*

Collision resolution merupakan proses untuk menangani kejadian dua atau lebih key di hash ke alamat yang sama. Cara yang dilakukan jika terjadi *collision* adalah mencari lokasi yang kosong dalam table hash secara terurut. Cara lainnya adalah dengan menggunakan fungsi hash yang lain untuk mencari lokasi kosong tersebut.

2.10 Pengertian Algoritma Base64

Algoritma Base64 merupakan salah satu algoritma untuk *Encoding* dan *Decoding* suatu data ke dalam format ASCII, yang didasarkan pada bilangan dasar 64 atau bisa dikatakan sebagai salah satu metode yang digunakan untuk melakukan *encoding* (penyandian) terhadap data binary.

Algoritma ini banyak digunakan di dunia Internet sebagai media data format untuk mengirimkan data, penggunaan tersebut dikarenakan hasil dan *encode base64* berupa *plaintext*, maka data ini akan jauh lebih mudah dikirim, dibandingkan dengan format data yang berupa binary. Skema Base64 biasanya digunakan ketika ada kebutuhan untuk menyandikan data biner yang perlu disimpan dan ditransfer melalui media yang dirancang untuk menangani data tekstual.

Algoritma Base64 menggunakan kode ASCII dan kode index base64 dalam melakukan proses enkripsi ataupun dekripsinya. Dalam melakukan enkripsi pada

URL website, kode index base64 perlu dimodifikasi. Simbol (+) dimodifikasi menjadi (-) dan simbol (/) menjadi (_). Algoritma kriptografi Base64 ini sebenarnya menggunakan algoritma kunci simetris atau disebut juga algoritma kriptografi konvensional, yaitu algoritma yang menggunakan kunci untuk proses enkripsi sama dengan kunci untuk proses dekripsi. (et al., 2017)

Adapun tahapan - tahapan enkripsi menggunakan Algoritma Base64 adalah sebagai berikut :

1. Mengkonversi karakter ke biner.
2. Perhatikan dan pastikan bahwa ada 24 bit.
3. Mengkonversi 24 bit dari tiga kelompok 8 bit ke empat kelompok 6 bit.
4. Convert masing-masing empat kelompok 6 bit ke desimal.
5. Gunakan masing-masing desimal untuk mencari kode karakter pada index Base64.

Adapun tahapan - tahapan dekripsi menggunakan Algoritma Base64 adalah sebagai berikut :

1. Mengkonversi karakter Base64 ke biner dengan menggunakan 6 bit.
2. Konversi 24 bit dari empat kelompok 6 bit ke tiga kelompok 8 bit.
3. Konversi masing-masing tiga kelompok 8 bit ke desimal.
4. Gunakan masing-masing tiga desimal untuk mencari karakter ASCII untuk nilai yang ada.

2.11 Konsep Enkripsi dan Deskripsi

Salah satu mekanisme untuk meningkatkan keamanan adalah dengan menggunakan teknologi enkripsi. Data-data yang dikirimkan diubah sedemikian rupa sehingga tidak mudah disadap. Jadi enkripsi adalah proses yang dilakukan untuk mengamankan sebuah pesan (yang disebut plaintext) menjadi pesan yang tersembunyi (disebut ciphertext) adalah enkripsi (*encryption*). *Ciphertext* adalah pesan yang sudah tidak dapat dibaca dengan mudah. Terminologi yang lebih tepat digunakan adalah “*encipher*”. Proses sebaliknya, untuk mengubah *ciphertext* menjadi plaintext, disebut dekripsi (*decryption*). Terminologi yang lebih tepat untuk proses ini adalah “*decipher*”.

Berdasarkan cara memproses teks (plaintext), cipher dapat dikategorikan menjadi dua jenis: block cipher and stream cipher. Block cipher bekerja dengan memproses data secara blok, dimana beberapa karakter/data digabungkan menjadi satu blok. Setiap proses satu blok menghasilkan keluaran satu blok juga. Sementara itu stream cipher bekerja memproses masukan (karakter atau data) secara terus menerus dan menghasilkan data pada saat yang bersamaan. (Aulia, 2012)

2.11 Web Server

Web server adalah perangkat lunak (*software*) dalam server yang memberikan layanan berbasis data dan berfungsi untuk menerima permintaan (*request*) berupa halaman web melalui protokol HTTP dan atau HTTPS dari klien yang lebih dikenal dengan nama *browser*, kemudian mengirimkan kembali

(*respon*) hasil permintaan tersebut kedalam bentuk halaman web yang pada umumnya berbentuk dokumen HTML. (Ramadhani, 2017)

1. Fungsi Web Server

Fungsi utama dari web server adalah untuk melakukan atau mentransfer berkas permintaan pengguna melalui protokol, komunikasi yang telah ditentukan sedemikian rupa. Halaman web yang diminta terdiri dari berkas teks, video, gambar, file dan banyak lagi. salah satu contoh dari web server adalah *Apache*. *Apache (Apache Web Server- the http web server)* merupakan web server yang paling banyak dipergunakan di internet. Program ini pertama kali didesain untuk sistem operasi lingkungan UNIX. *Apache* mempunyai program pendukung yang cukup banyak hal ini memberikan layanan yang cukup lengkap bagi penggunanya.

Beberapa dukungan *Apache*:

a. PHP (*personal home page/PHP hypertext processor*)

Program dengan metode semacam CGI, yang memproses teks dan bekerja di server. *Apache* mendukung PHP dengan menempatkannya sebagai salah satu modulnya (*mod php*).

b. Kontrol akses

Control ini dapat dijalankan berdasarkan nama host atau IP CGI (*Common gateway interface*). Yang paling terkenal untuk digunakan adalah *PERL (practical extraction and report language)* didukung oleh *Apache* dengan menempatkannya sebagai modul (*mod perl*).

2. Cara kerja web Server

Kontribusi analisis web server untuk pengembangan hosting server institusi, khusus fokus pada bagian implementasi web server yang bertemu pada masalah bagaimana kinerja web server, berujung pada perbandingan kinerja web server:

1. *Client* melalui *browser* membagi url menjadi beberapa bagian, pembagiannya termasuk alamat, *path name* dan protocol.
2. DNS menerjemahkan nama domain ke alamat IP yang sesuai karena memang alamat sesungguhnya dari suatu *website* adalah alamat IP yang biasa kita tulis di *browser* seperti *facebook.com* itu hanyalah domain yang mewakili IP dari *web facebook*.
3. Kemudian *browser* memutuskan protokol apa yang dapat digunakan. FTP, HTTP adalah beberapa contoh dari protokol namun protokol umum digunakan dalam web adalah protokol HTTP.
4. Server website mengirimkan permintaan GET ke web server untuk mengambil alamat yang telah diberikan. Server website memverifikasi alamat yang telah diberikan, menemukan file yang diperlukan, berjalan sesuai *script* pertukaran *cookies* jika diperlukan dan mengembalikan permintaan ke *browser*.
5. Browser sekarang mengkonversi data ke dalam basis data HTML dan menampilkan hasil ke pengguna. Jika tidak menemukan data yang diminta server akan mengirimkan pesan kesalahan ke browser dan browser akan menampilkan kepada client.

3. Contoh Web Server

Setelah mengetahui pengertian web server dan fungsinya, kini Kita beralih ke produk web server. Ada banyak sekali produk web server yang diproduksi untuk hosting website. Berikut ini beberapa contoh web server yang paling populer dan sering digunakan antara lain :

1. *Apache*

merupakan web server yang paling populer dan paling banyak digunakan. Web server ini memiliki beberapa dukungan seperti PHP, control akses, dan SSL. *Apache* meletakkan kontrol akses sebagai modul dimana paling banyak digunakan adalah modul perl. sementara fitur PHP merupakan program yang mirip CGI (*common gateway interface*) untuk memproses teks.

2. IIS (*internet information services*)

Web server IIS ini digunakan dalam OS Windows (windows 2000 dan windows 2003) yang didukung dengan komponen seperti protokol jaringan DNS, TCIP/IP dan software yang digunakan untuk membuat situs web. IIS juga kompatibel untuk mendukung beberapa protokol seperti FTP, HTTP, NNTP, SMTP, dan SSL. Kelebihan dari server ini bisa diakses penuh pada *windows* dan mendukung *platform*. Kekurangannya adalah web server ini termasuk jenis yang berbayar.

3. Nginx

Web server *Nginx* atau dibaca *engine x* ini merupakan web server yang *open source* dan bisa digunakan oleh siapapun secara gratis selain *apache*.

Keunggulan Nginx dibanding *apache* yaitu pada *apache* tidak dapat menangani web server yang memiliki *traffic* tinggi.

4. Lighttpd

Lighttp atau yang dibaca *lightly* ini merupakan web server yang juga *open source* dan dikembangkan oleh *programmer* kebangsaan Jerman. Web server ini lebih diutamakan digunakan pada Os linux atau dari kelompok inix lainnya. Kelebihan dari web server ini yaitu memiliki kemampuan untuk mengatur CPU *Load* efektif dengan beberapa fitur lainnya seperti *Fast CGI, SCGI, URL Writing* dan *output-compresson*.

2.12 Pengertian IP Address

Ip Address adalah sebuah alamat yang digunakan untuk mengidentifikasi sebuah perangkat secara unik pada sebuah jaringan IP. Alamat IP terdiri dari 32 bit binary yang terdiri dari porsi *network* dan porsi *host* dengan bantuan sebuah *subnet maks*. 32 bit binary terdiri dari 4 octet (1octet = 8 bit). Masing-masing octec dikonversi menjadi desimal dan dipisahkan dengan tanda titik (dot). Dengan demikian sebuah alamat ip dinyatakan dalam format dotted decimal (contoh 192.168.1.200). Nilai dari setiap masing-masing octed berkisar antara 0 sampai 255 dalam decimal atau 0000000-11111111 dalam binary. (Mubarak & Wahid, 2006)

Ip Address adalah identitas satu komputer dalam jaringan komputer atau internet seperti halnya rumah kita mempunyai nomor rumah yang tertempel pada dinding. penulisan Ip Address terbagi atas 4 kelompok 8 bit yang dituliskan dalam

bilangan biner. Dimana setiap kelompok *Ip Address* dipisahkan oleh titik. Nilai terbesar dari bilangan biner 8 bit adalah 255. Oleh karena itu jumlah *Ip Address* yang tersedia ialah 255.255.255.255 *Ip Address* yang sebanyak ini harus dibagi bagikan keseluruh pengguna jaringan komputer atau internet diseluruh dunia. sedangkan *Ip Address* sendiri memiliki 2 fungsi yakni :

1. Sebagai alat identifikasi host atau antarmuka pada jaringan komputer. fungsi ini diilustrikan seperti nama orang sebagai suatu metode untuk mengenali siapa orang tersebut dalam jaringan komputer berlaku hal yang sama.
2. Sebagai alamat lokasi jaringan komputer. Fungsinya diibaratkan seperti alamat rumah kita berada. Untuk memudahkan pengiriman paket data maka *Ip Address* memuat informasi keberadaannya. Ada rute yang harus dilalui agar dapat sampai ke komputer yang dituju.

2.13 Sistem Operasi Ubuntu

Ubuntu adalah berkumpulnya dari individu-individu yang umum dalam menciptakan sebuah sistem operasi yang bebas. Sistem operasi open source itu dapat disebut juga dengan Ubuntu. Sebuah sistem operasi dengan beberapa program dasar dan utilitas yang membuat komputer dapat berjalan. Inti dari sebuah sistem operasi tersebut dapat di sebut juga dengan kernel. Pengertian dari kernel adalah program yang palingdasar yang ada pada komputer dan memungkinkan kita untuk memulai program lain.

Kernel yang di gunakan Ubuntu saat ini menggunakan kernel Linux atau kernel FreeBSD. Linux yang dimulai dari Linus Torvalds dan didukung ribuan programmer di seluruh dunia. FreeBSD adalah sebuah sistem operasi termasuk kernel dan perangkat lunak lainnya.

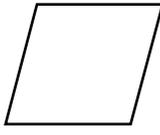
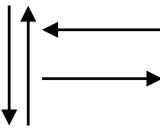
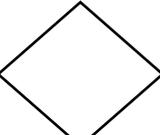
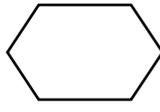
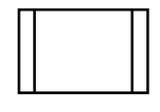
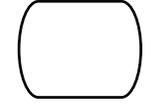
Program perangkat lunak tersebut dapat membantu brainware dalam mendapatkan apa yang ingin mereka lakukan dan diperbuat, dari memodifikasi dokumen untuk menjalankan bisnis, bermain game dan menulis perangkat lunak yang lebih banyak lagi. Ubuntu datang dengan lebih dari 45.000 paket (software precompiled yang terbungkus dalam format yang bagus untuk memudahkan dalam installasi dan konfigurasi), manajer paket (APT) dan beberapa utilitas yang mungkin dapat untuk mengelola ribuan paket yang ada pada ribuan komputer dengan mudah untuk menginstal sebuah aplikasi. Ubuntu sangat mengatur segala sesuatu pekerjaan di sistem operasinya sehingga semua bekerja dengan sangat baik. (Muslim, 2006)

2.14 *Flowchart*

Flowchart adalah bagian-bagian yang memiliki arus dan menggambarkan langkah-langkah penyelesaian suatu masalah. Flowchart merupakan suatu cara penyajian dari suatu Algoritma.

Flowchart disusun dengan simbol. Simbol ini dipakai sebagai alat bantu menggambarkan proses didalam program. Simbol-simbol yang digunakan dapat dibagi, yakni sebagai berikut:

Table 2.1 Daftar Simbol *Flowchart*

Simbol	Nama	Keterangan
	Input/Output	Digunakan untuk mewakili data input/output
	Arus/Flow	Digunkana untuk menunjukkan arah/alir dari suatu proses.
	Proses	Digunakan untuk mewakili suatu proses.
	Keputusan/ <i>Decision</i>	Digunakan untuk suatu penyelesaian kondisi dalam program.
	<i>Pendefined</i> Proses	Digunakan untuk memberikan nilai awal dari proses.
	<i>Predefined</i> proses	Digunakan untuk proses yang detilnya terpisah.
	Awal/akhir (Terminal)	Digunakan untuk menunjukkan awal dan akhir dari proses.

2.15 *Unified Modeling Language*

UML (*Unified Modeling Language*) adalah adalah sebuah bahasa yang berdasarkan grafik atau gambar untuk memvisualisasi, menspesifikasikan, membangun, dan pendokumentasian dari sebuah sistem pengembangan software berbasis OO (Object-Oriented). UML sendiri juga memberikan standar 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.(Suendri, 2018)

Diagram *Unified Modeling Language* (UML) antara lain sebagai berikut :

1. *Use Case* Diagram

Use case menggambarkan *external view* dari sistem yang akan kita buat 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.

2. *Class* Diagram

Diagram ini memperlihatkan himpunan kelas-kelas antarmuka, kolaborasi dan relasi-relasi antar objek.

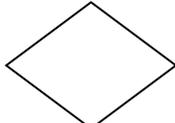
3. *Sequence* Diagram

Diagram ini memperlihatkan interaksi yang menekankan pada pengiriman pesan dalam suatu waktu tertentu.

4. *Activity* Diagram

Diagram ini memperlihatkan aliran aktivitas ke aktivitas lainnya dalam suatu sistem. Diagram ini terutama penting dalam pemodelan fungsi-fungsi dalam suatu sistem dan memberikan tekanan pada tekanan pada aliran kendali objek.

Tabel 2.2 Daftar Simbol *Unified Modeling Language*

No	Gambar	Nama	Keterangan
1		Activity	Memperlihatkan dimana masing-masing kelas antar muka saling berinteraksi satu sama lain.
2		Activity Final Note	Bagaimana objek dibentuk dan diakhiri
3		Decision	Digunakan untuk menggambarkan suatu keputusan atau tindakan yang harus diambil pada kondisi tertentu.
4		Line Connector	Digunakan untuk menghubungkan satu simbol dengan simbol lainnya.

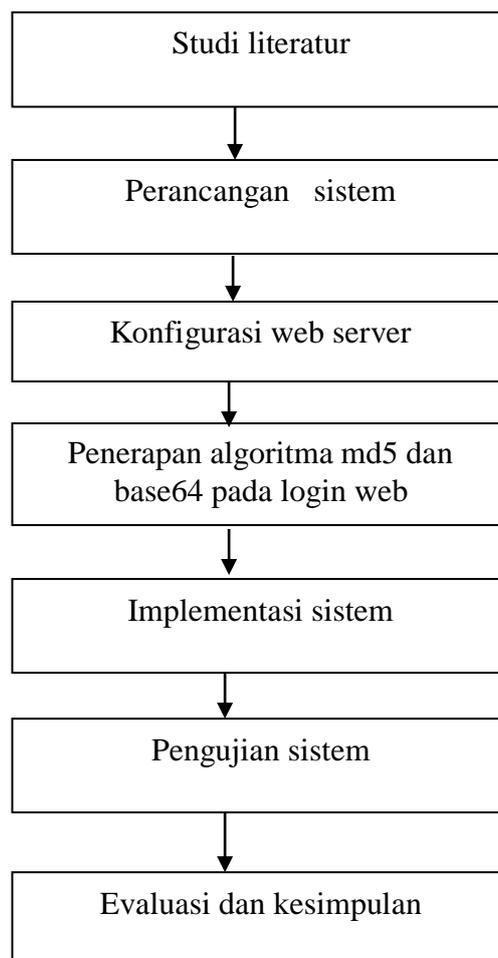
BAB III

METODE PENELITIAN

3.1 Tahapan Penelitian

Metode yang digunakan dalam membangun sistem ini adalah model *waterfall*. Model ini terdiri dari beberapa tahapan, yaitu: Studi Literatur, perancangan sistem, konfigurasi web server, penerapan algoritma md5 dan base64 pada login web, implementasi sistem pengujian sistem, evaluasi dan kesimpulan.

Adapun metode perancangan adalah sebagai berikut :



Gambar 3.1 Tahapan penelitian

Dalam menyelesaikan penelitian ini ada beberapa tahapan-tahapan yang dilakukan seperti dalam gambar yaitu:

1. Studi Literatur

Pada tahapan ini dilakukan untuk mencari sumber-sumber informasi, konsep-konsep yang mendasar terkait dengan sistem *web page login*. Materi ini diperoleh dari orang-orang yang berkompeten didalamnya baik dengan dosen pembimbing, teman-teman, buku-buku, serta artikel-artikel di *internet* yang mendukung dalam pembuatan *web page login* ini.

2. Perancangan Sistem

Meliputi beberapa tahap yang terstruktur sebagai berikut :

- a. Sistem dirancang menggunakan sistem operasi dan konfigurasi linux, paket pendukung linux ubuntu dan kombinasi algoritma md5 dan base64 , menggunakan sistem operasi windows sebagai pengujian.
- b. Hasil dan pembahasan dengan cara Implementasi perangkat dan pengujian sistem.

3. Konfigurasi *Web Server*

Dalam penelitian ini konfigurasi menggunakan linux ubuntu dan tools tambahan pendukung dalam menjalankan sistem tersebut kemudian memasukkan *script* kombinasi algoritma md5 dan base64 untuk membentuk pengamanan sebuah *web page login* yang berbasis *web server* lokal.

4. Penerapan algoritma Md5 dan Base64 pada *Web Login*

Penerapan algoritma Md5 dan Base64 adalah sebagai salah satu cara agar dapat mengamankan suatu web login dimana md5 digunakan untuk pengujian keintegritas suatu file dan base64 digunakan untuk penyandian (*encoding*) terhadap suatu data.

5. Implementasi Sistem

Implementasi sistem pengamanan *web page login* berbasis *web server* lokal menggunakan kombinasi md5 dan base64. Bahasa pemrograman *ubuntu server* 10.4 dengan basis data yang digunakan adalah MYSQL. Aplikasi *ubuntu server* tersebut dapat dijalankan pada perangkat keras PC (*Personal computer*) dengan sistem operasi *Microsoft Windows XP*.

6. Pengujian Sistem

Melakukan pengujian dan penaksiran ulang sistem yang telah melakukan implementasi.

7. Evaluasi

Apakah sistem yang telah di miliki mendapatkan kinerja yang baik dan keamanan dengan tingkat yang baik.

8. Kesimpulan

Setelah melakukan pengujian sistem dan evaluasi maka dapat disimpulkan bahwa sistem pengamanan *web login* yang dibangun dapat bekerja dengan baik dengan memasukkan *username* dan *password* bagi pengguna *web page login* tersebut.

3.2 Metode Pengumpulan Data

Untuk mendukung penelitian yang akan dibangun dibutuhkannya metode pengumpulan data yang diambil dari buku panduan, dosen pembimbing dan teman-teman yang lain. Dalam tahap ini juga melakukan analisa sistem yang berjalan dan kebutuhan sistem yang nantinya akan dikonfigurasi.

3.3 Analisis Sistem Yang Sedang Berjalan

Analisis merupakan gambaran tentang *system* jaringan yang saat ini sedang berjalan. Pada analisis ini yang akan dijelaskan adalah pengamanan *web page login*, dimana pengamanan *web page login* ini menggunakan kombinasi algoritma md5 dan base64. Algoritma adalah urutan langkah-langkah penyelesaian masalah secara sistematis dan logis yang digunakan untuk perhitungan, pemrosesan data dan penalaran otomatis. Kombinasi algoritma md5 dan base64 adalah proses yang terlibat dalam pengamanan *web page login*, dimana algoritma md5 sebagai pengujian keintegritas sebuah file dan base64 digunakan sebagai salah satu metode yang digunakan untuk melakukan *encoding* (penyandian) terhadap data. Pengamanan *web page login* ini hanya berbasis *web server* lokal. Md5 dan base 64 akan mengenkripsi pada pengguna yang memiliki level, contohnya seperti pada pengguna admin level = 1 maka md5 dan base64 akan mengenkripsi *username* dan *password* yang terdapat pada admin level = 1.

3.4 Rancangan Penelitian

Dalam penelitian ini akan mengkombinasikan sebuah algoritma md5 dan base64 yang sangat berperan dalam pengamanan *web page login* yang mana kombinasi algoritma md5 dan base 64 dimasukkan dalam *data base mysql* agar dapat menampilkan keamanan dalam *web page login*. Salah satu mekanisme untuk meningkatkan keamanan adalah dengan menggunakan teknologi enkripsi. Data-data diubah sedekimian rupa agar tidak mudah di sadap. Terminologi yang tepat digunakan adalah *enchiper*. Proses sebaliknya, untuk mengubah *chipertext* menjadi *plaintext*, disebut deskripsi (*decryption*). Terminologi yang lebih tepat untuk proses ini adalah *decipher*.

3.4.1 UML (*Unified Modelling Language*)

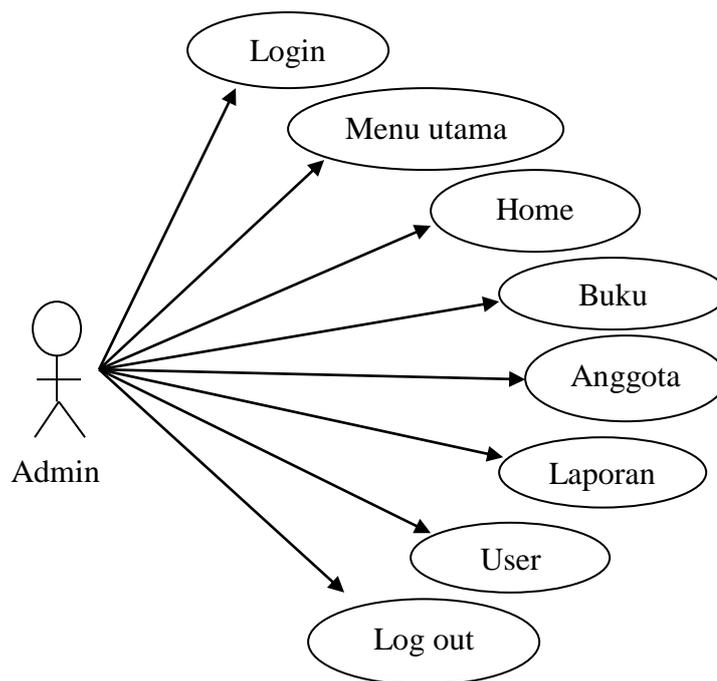
Unified modeling language (UML) adalah sebuah bahasa yang berdasarkan grafik atau gambar untuk memvisualisasi, menspesifikasikan, membangun, dan pendokumentasian dari sebuah sistem pengembangan software berbasis OO (Object-Oriented). UML sendiri juga memberikan standar penulisan sebuah sistem blue print, yang meliputi konsep bisnis proses, penulisan kelas-kelas dalam bahasa program yang spesifik, skema database, dan komponenkomponen yang diperlukan dalam sistem software.(Suendri, 2018)

Dalam perancangan sistem web page login yang berbasis web server lokal ini topologi jaringan menggunakan pemodelan sistem *use case* diagram, *activity* diagram, *sequence* diagram dan *class* diagram sesuai dengan analisis kebutuhan dan rancangan sistem.

Tahapan yang dilakukan dalam mendesain dan membuat sistem informasi *web page login* adalah sebagai berikut :

1. Use Case Diagram

Pada gambar *use case* diagram web login berbasis web server lokal ini maka dijelaskan proses-proses yang terjadi dari sistem yang dibuat.



Gambar 3.4 *use case* diagram berbasis web server lokal

Dari gambar *use case* diagram diatas terdapat actor yang terlibat di dalam sistem. Actor ini berperan sebagai admin yang sebagai orang yang dapat melakukan aktifitas seperti melihat informasi dari *web server* mulai dari melihat, *login*, halaman utama,*home*, buku, anggota, laporan, *user*, dan *log out*. Pada gambar diatas terdapat 8 *use case* yaitu :

1. Login

Menampilkan halaman utama setelah masuk ke dalam db.perpus

2. Halaman utama

Merupakan tampilan halaman utama dari db.perpus yang berisi informasi dan logo dari db.perpus tersebut.

3. Home

Menampilkan halaman awal saat admin *login*.

4. Buku

Menampilkan halaman informasi tentang jenis buku-buku yang terdapat pada db.perpus

5. Anggota

Menampilkan halaman yang berisi informasi tentang jumlah anggota yang terdapat pada db.perpus

6. Laporan

Menampilkan halaman yang berisi seluruh laporan tentang db.perpus

7. *User*

Menampilkan halaman yang berisi tentang admin dari db.perpus

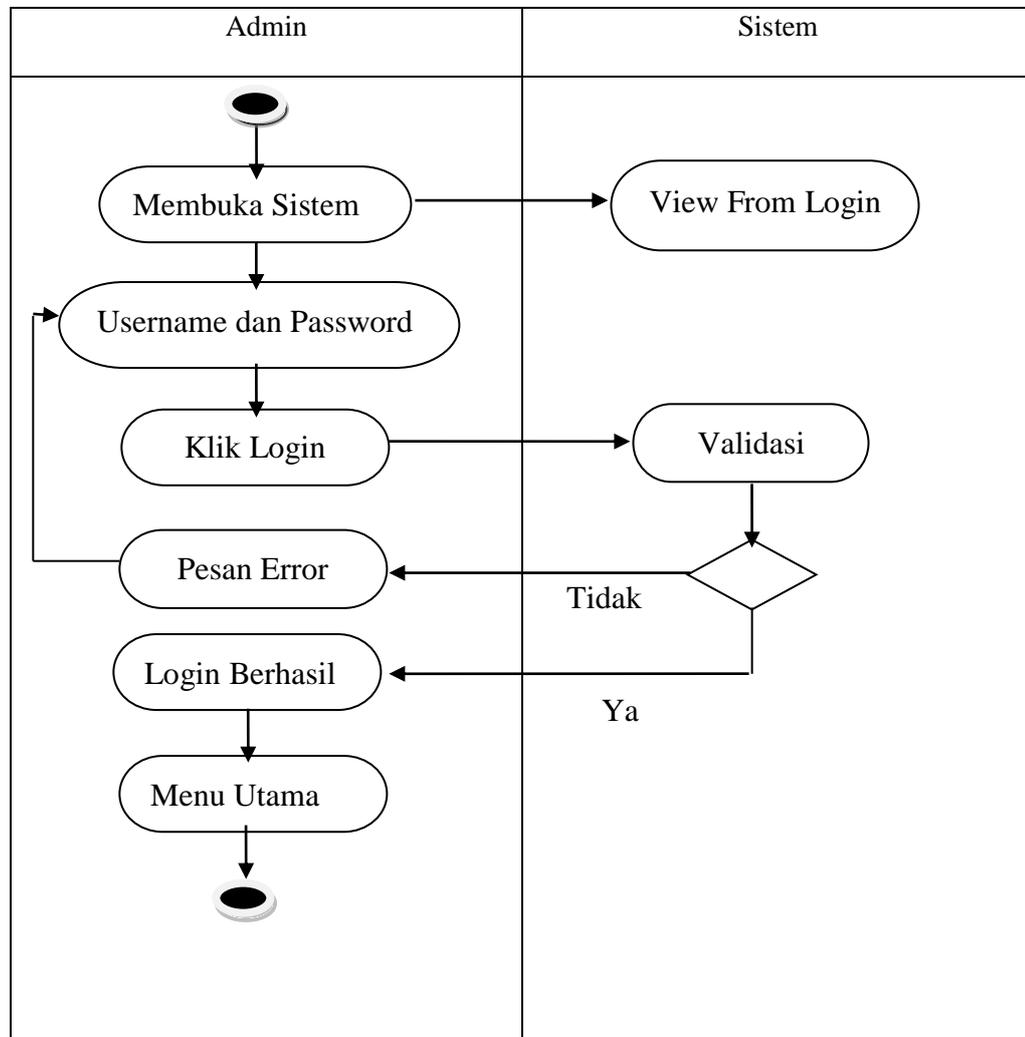
8. *Log out*

Halaman ini merupakan langkah terakhir keluar dari db.perpus oleh admin.

2. **Activity Diagram**

Activity diagram adalah gambar aktivitas *user* terhadap semua menu yang dibuat dalam sistem. Berikut adalah salah satu aktivitas admin

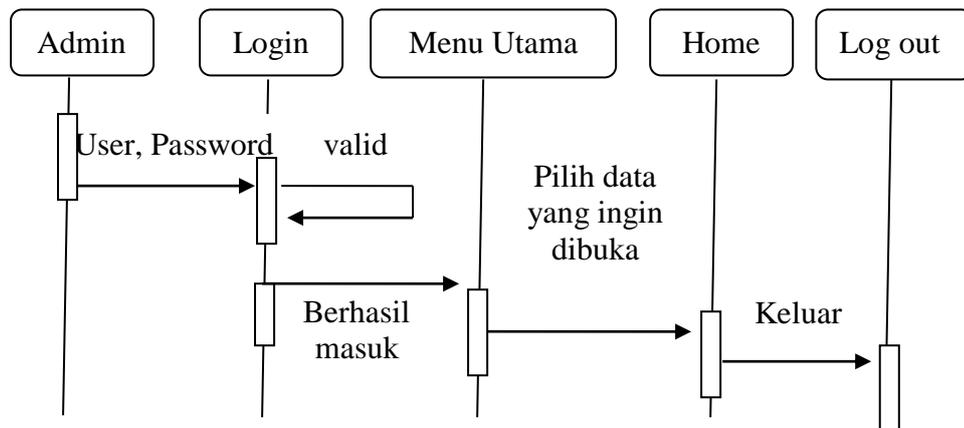
terhadap sistem yang berhubungan dengan menu *login*. Berikut adalah gambar dari *activity* diagram.



Gambar 3.5 Activity Diagram

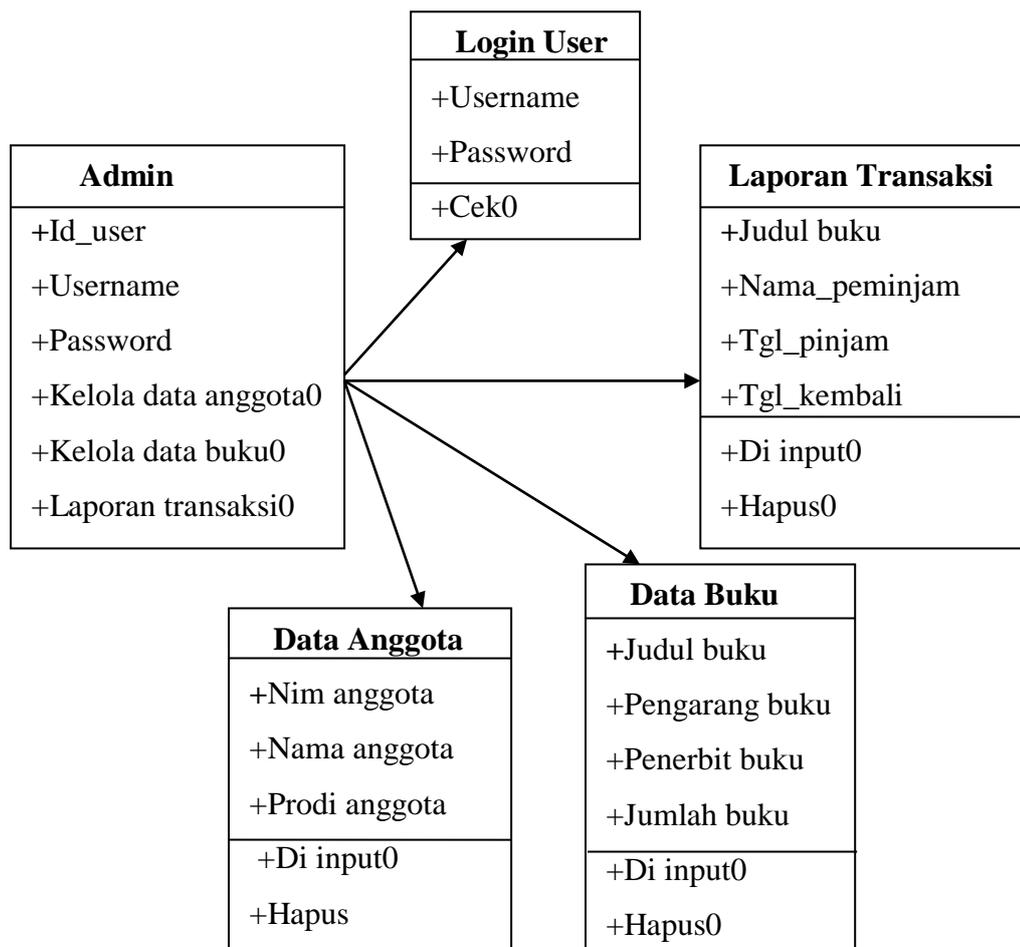
3. Sequence Diagram

Diagram *sequence* merupakan gambar kegiatan *user* berdasarkan rangkaian urutan waktu penggunaan sistem seperti admin, *login*, menu utama, home (data buku, anggota, transaksi, dan laporan) dan *log out*, Diagram *sequence* dapat dilihat pada gambar berikut.



Gambar 3.6 Sequence Diagram

4. Class Diagram



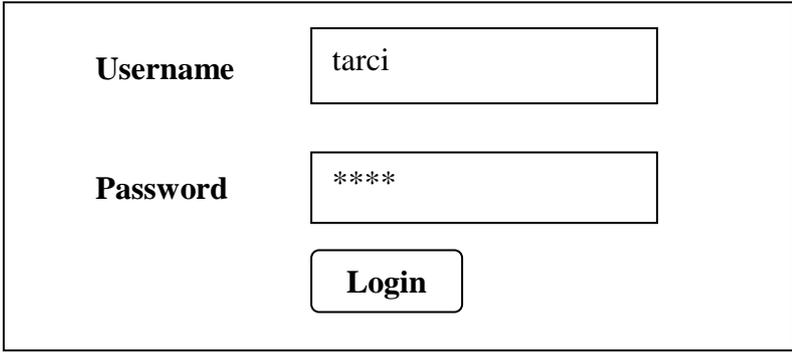
Gambar 3.7 Class Diagram

Class diagram adalah diagram yang menunjukkan class-class yang ada dalam sebuah sistem dan berhubungan secara logika dan grafis mengenai struktur objek statis dari suatu sistem dan hubungan antar objek tersebut. Seperti pada gambar diatas menunjukkan sistem yang saling berhubungan antara : Admin, login, data anggota, data buku dan laporan transaksi yang saling terkait.

3.4.2 Rancangan Desain Database

Rancangan yang akan dibangun dapat digambarkan sebagai berikut:

1. Rancangan Form Login



Username	<input type="text" value="tarci"/>
Password	<input type="password" value="****"/>
	<input type="button" value="Login"/>

Gambar 3.2 Rancangan *form Login* pada *web server*

Form login diatas digunakan untuk dapat masuk kedalam sistem perpus.

Untuk dapat menggunakan *form login* ini kita dapat menginput *username* dan juga *password*. Setelah memasukkan *username* dan *password* yang sesuai, selanjutnya pilih tombol login kemudian akan masuk ke form selanjutnya.

Dari gambar di atas setelah kita berhasil login maka akan tampil seperti dibawah ini.

Menu utama	Welcome To Sistem Informasi Perpustakaan			
>>Home	~Silahkan Pilih Panel Dibawah Ini~			
>>Buku	<div style="display: flex; justify-content: space-around; align-items: center;"> <div style="border: 1px solid black; padding: 10px; width: 15%;">Logo 1</div> <div style="border: 1px solid black; padding: 10px; width: 15%;">Logo 2</div> <div style="border: 1px solid black; padding: 10px; width: 15%;">Logo 3</div> <div style="border: 1px solid black; padding: 10px; width: 15%;">Logo 4</div> </div>			
>>Anggota				
>>Transaksi				
>>Laporan				
>>User				

Gambar 3.3 Rancangan halaman menu utama dalam *web server*.

Adapun penjelasan dari gambar di atas adalah agar dapat masuk kedalam sebuah *web server* tersebut harus memasukkan *username* dan *password* yang diminta dimana jika sudah masuk kedalam *web server* akan terdapat beberapa panel pilihan yaitu: data buku, anggota, transaksi dan laporan yang bias dibuka dan diinput data yang mau ditambahkan.

2. Rancangan Form Anggota

From ini dibuat agar dapat mengetahui data dan jumlah anggota yang ada dalam db.perpus tersebut dimana dalam tabel ini masih dapat menambah jumlah anggota yang diinginkan.

Tabel 3.2 Rancangan form anggota

Data Anggota						
Input Anggota			Nim, Nama Anggota		Cari	
No	Nim	Nama	Prodi	Thn Masuk	Edit	Hapus
1	1614370285	Wewen	Komputer akuntansi	2004	-	X

3. Rancangan Form Buku

Form ini dibuat agar dapat mengetahui data dan jumlah buku yang dipinjam maupun dikembalikan dari perpustakaan dimana dalam tabel ini juga dapat menginput ulang jumlah buku yang dipinjam dan dikembalikan.

Tabel 3.3 Rancangan form Buku

Data Buku						
Input Buku			Judul buku,Pengarang		Cari	
No	Judul Buku	Pengarang	Penerbit	Jumlah	Edit	Hapus
1	Metematika	Kokom	Airlangga	4	-	X
2	PHP Dasar	Irfandi	Lokomedia	3	-	X
3	Samudera PHP	Solihin	Hamzah	2	-	X

4. Rancangan Form Transaksi

Form ini dibuat agar dapat mengetahui data-data nama peminjam buku atau ingin mengembalikan serta form ini juga dapat menginput transaksi kembali.

Tabel 3.4 Rancangan Form Transaksi

Data Transaksi							
Input Transaksi				Nama Peminjam		Cari	
No	Judul Buku	Peminjam	Tgl Pinjam	Tgl Kembali	Terlambat	Kembali	perpanjangan
1	Matematika	Wewen	01-11-2015	08-11-2015	3hari(Rp. 12.000)	kembali	Perpanjangan

5. Rancangan Form Laporan

Form ini dibuat agar dapat mengetahui data-data setiap laporan tentang data anggota, data buku dan data transaksi semua data tersebut disimpan di dalam form ini.

Tabel 3.5 Rancangan Form Laporan

Data Laporan	
All Laporan	
1	Laporan Buku
2	Laporan Anggota
3	Laporan Transaksi

6. Rancangan Form User

Form ini dibuat agar mengetahui admin dalam perpustakaan dan dapat menambahkan *admin* dalam sebuah perpustakaan tersebut.

Tabel 3.6 Rancangan Form User

Data User					
Input User		Cari Nama, Username	Cari		
No	Nama	Email	Level	Edit	Hapus
1	Tarcisius	admin@unpab.net	Admin	-	X
2	Prendi	prendi@gmail.com		-	X

3.4.3 Rancangan Relasi Data Base

Rancangan data base terdiri dari beberapa tabel yang saling berhubungan. Dalam pembuatan data base ini digunakan *mysql* sebagai *data base server* berikut adalah desain data base server.

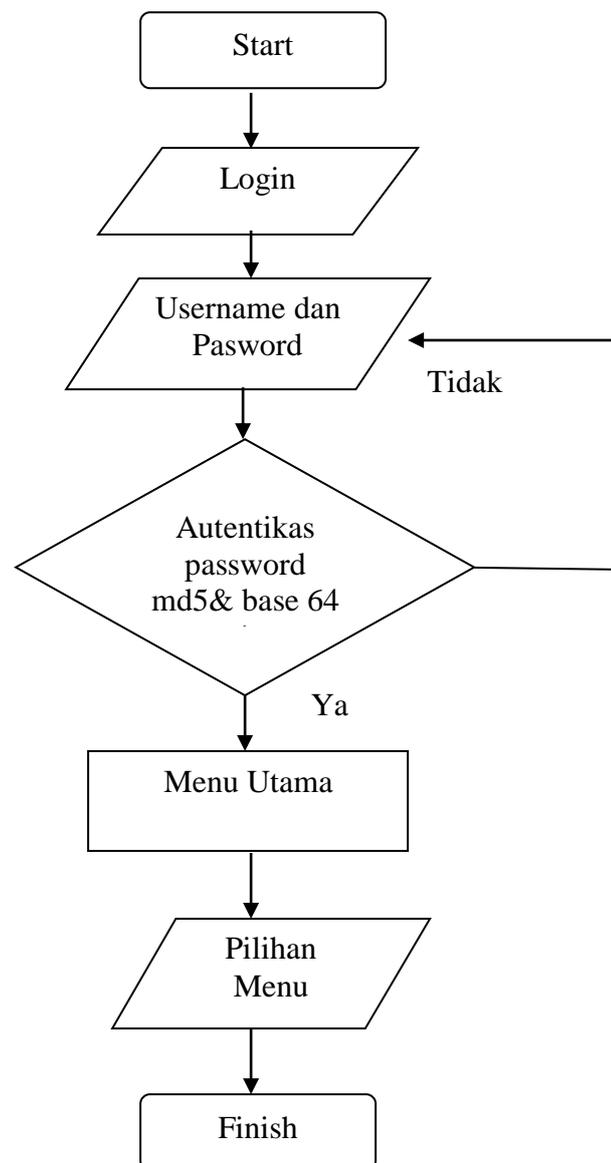
Tabel 3.1 Rancangan relasi antar tabel

db.Perpus tbl_anggota	db.Perpus tbl_Buku
nim : int(11)	Id : int(5)
nama : varchar(250)	Judul : varchar(200)
tempat_lahir : varchar(50)	Penerbit : varchar(150)
tgl_lahir : varchar(15)	Thn_terbit : varchar(4)
jk : enum("L","P")	Isbn : varchar(25)
prodi : varchar (50)	Jumlah_buku : int(25)
thn_masuk : varchar(4)	Lokasi : enum("rak1","rak2","rak3")
	tgl_input : datetime

db.Perpus tbl_transaksi	db.Perpus tbl_user
id : int(5)	id : int(3)
judul : varchar(250)	nama : varchar(200)
nim : int(11)	username : varchar(50)
nama : varchar(100)	password : varchar(200)
tgl_pinjam : varchar(15)	email : varchar(100)
tgl_kembali : varchar (15)	foto : varchar (50)
Satatus : varchar(50)	level : enum("admin:","user")
Ket : varchar(250)	

3.4.4 Rancangan Flow chart

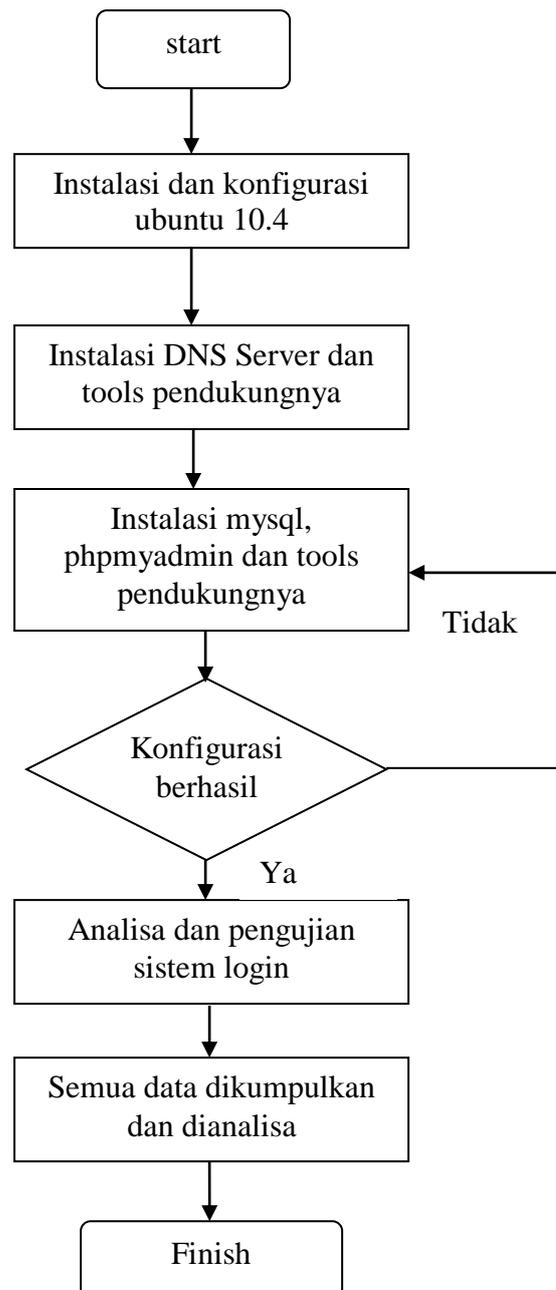
Flowchart adalah bagian-bagian yang memiliki arus dan menggambarkan langkah-langkah penyelesaian suatu masalah dalam membuat suatu program. *Flowchart* merupakan diagram yang menunjukkan bagaimana cara kerja aplikasi. *Flowchart* sistem *web page login* dapat dilihat sebagai berikut.



Gambar 3.3 *Flowchart* sistem *login* yang dibangun

3.4.4.1 Perancangan Konfigurasi Md5 dan Base64

Dalam membangun sebuah *web page login* agar berjalan sesuai dengan apa yang diinginkan dengan baik dibutuhkan proses yang akan dibuat dalam bentuk diagram alir berikut.



Gambar 3.4 Diagram alir perancangan konfigurasi *login web server*

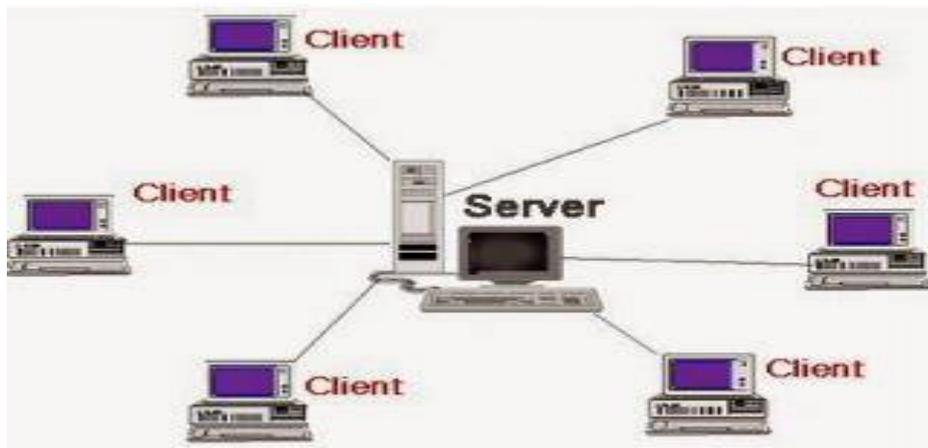
Dari gambar di atas dapat dijelaskan sebagai berikut:

1. Diawali dengan melakukan instalasi Linux Ubuntu 10.4 kemudian mengikuti alur instalasi hingga selesai penginstallan. Saat telah selesai penginstallan lakukan penyesuaian *IP Address* dan konfigurasinya.
2. Setelah selesai melakukan pengaturan *IP Address* dan konfigurasi lainnya kemudian melakukan penginstallan *Dns Server* agar mendukung kinerjanya diperlukan *setting Dns* dimana disana diminta melukan *update Dns Server* setelah di *update* lanjutkan dengan menginstal *Bind9* dan memasukkan *script file* yang diminta agar bias menjalankan paket-paket lain dengan baik. Seperti : *Apache2 link*, *php mysql*, dan *mysql server*
3. Setelah semua paket-paket diinstal kemudian lanjutkan dengan penginstallan *phpmyadmin* dan melakukan pengisian-pengisian konfigurasi yang ditentukan agar dapat menampilkan *web site* yang sudah dimasukkan kedalam *Database* dan melakukan *setting host name*, *password* dan *ussername* dalam *databe* tersebut.
4. Jika semua tahap sudah selesai dilakukan dan berhasil kemudian dilakukan pengujian, pengumpulan data dan menganalisa.

3.4.5 Rancangan Topologi Jaringan

Topologi jaringan adalah struktur topologi jaringan dan dapat digambarkan secara fisik atau logis. Ini adalah aplikasi teori grafik dimana perangkat komunikasi dimodelkan sebagai *node* dan koneksi antar perangkat dimodelkan

sebagai tautan atau garis antar node. Adapun topologi yang dibuat adalah sebagai berikut :



Gambar 3.5 Rancangan Topologi Jaringan

Topologi ini merupakan kontrol terpusat, semua link harus melewati pusat yang menyalurkan data tersebut ke semua simpul atau client yang dipilihnya. Simpul pusat dinamakan stasiun primer atau server dan lainnya dinamakan stasiun sekunder atau client server. Setelah hubungan jaringan oleh server setiap klien server sewaktu-waktu dapat menggunakan hubungan jaringan tersebut tanpa menunggu perintah.

3.4.6 Rancangan Security

Keamanan merupakan salah satu aspek penting dari sebuah sistem yang dibangun agar terhindar dari ancaman yang beresiko merusak sistem. Maka dari itu diperlukan suatu teknik agar dapat menjaga keamanan sistem tersebut dengan menggunakan kombinasi algoritma md5 dan base64. *Message Digest* (md5) digunakan sebagai pengujian integritas sebuah file dan *Algoritma Base64* merupakan salah satu algoritma untuk *Encoding* dan *Decoding* suatu data ke

dalam format ASCII dan bisa dikatakan sebagai salah satu metode yang digunakan untuk melakukan *encoding* (penyandian). Adapun teknik enkripsi menggunakan *algoritma base 64* adalah sebagai berikut:

1. Mengkonversi karakter ke biner.
2. Perhatikan dan pastikan bahwa ada 24 bit.
3. Mengkonversi 24 bit dari tiga kelompok 8 bit ke empat kelompok 6 bit.
4. Convert masing-masing empat kelompok 6 bit ke desimal.
5. Gunakan masing-masing desimal untuk mencari kode karakter pada index Base64.

Dari teknik enkripsi diatas maka diperlukan suatu keamanan berupa *username* dan *password* sebelum masuk ke dalam sistem tersebut.

BAB IV

HASIL DAN PEMBAHASAN

4.1 Kebutuhan Spesifikasi Minimum Hardware dan Software

Spesifikasi perangkat yang digunakan untuk mendukung dalam pembuatan Pengamanan *Web Page Login* agar dapat berjalan dengan baik terdiri dari dua bagian yaitu : kebutuhan perangkat keras (*hardware*) dan kebutuhan perangkat lunak (*software*) dengan penjelasan sebagai berikut :

1. Perangkat keras (*hardware*) dalam pembuatan program ini, penulis menggunakan laptop dan sistem operasi dengan spesifikasi sebagai berikut:
 - a. Tipe Laptop : Hp Notebook
 - b. Processor : Intel (R) Core (TM) i3-5005u CPU @ 2.00GHz @
 - c. Memori : 4.00 GB
 - d. Sistem operasi : windows 10 pro 64 - bit
2. Perangkat lunak (*software*) yang dibutuhkan adalah sebagai berikut:
 - a. Aplikasi Virtual Box
Digunakan sebagai tempat untuk menginstal operasi sistem yang dibutuhkan
 - b. Sistem operasi Linux Ubuntu 10.4
Digunakan sebagai penginstalan *tools* pendukung agar program berjalan dengan baik
 - c. Sistem operasi Win SCP

Sebagai alat mentransfer *file* atau mengedit *file scrip*.

d. Teatering hotspot via smartpone

Sebagai jaringan untuk menghubungkan program yang sedang dijalankan.

4.2 Implementasi Sistem

Proses implementasi sistem dilakukan dengan tujuan agar sistem yang dibangun dapat mengatasi permasalahan dalam penelitian ini. Pada tahap ini sebelum melakukan implementasi, pengguna (admin) harus mempersiapkan kebutuhan-kebutuhan dari program yang diimplementasikan. Kebutuhan-kebutuhan tersebut berupa perangkat lunak dan perangkat keras yang telah dijelaskan sebelumnya. Pada tahap ini dapat dijelaskan bagaimana penggunaan *web page login* berbasis *web server lokal* pada db.perpustakaan yang dibangun.

Hasil implementasi ini dilakukan dengan tujuan menjelaskan penggunaan *web page login* berbasis *web server lokal*. Kepada masing-masing pengguna sesuai dengan fungsi yang dilakukannya. Namun sebelum masuk kedalam penggunaannya maka perlu dilakukan tahapan pembuatan *web login* tersebut dengan langkah-langkah dibawah ini.

4.2.1 Setting DNS Server

Setelah melakukan pengintasilan ubuntu dengan *tools* tambahan pendukung tersebut maka diperlukan juga *setting dns server* agar program

berjalan dengan baik sesuai yang diharapkan.ada beberapa tahap yang perlu dilakukan seperti dibawah ini :

```
root@ubuntu:~# apt-get update
```

Tampilan akhir update

```
Get :1 http://id.archive.ubuntu.com precise/main source [935
KB]
Get :50 http://id.archive.ubuntu.com precise/restriced
sources[5,019KB]
Get :51 http://id.archive.ubuntu.com precise/universe
sources[519KB]
Get :54 http://id.archive.ubuntu.com precise/multiverse
sources[719KB]
Get :55 http://id.archive.ubuntu.com precise/main i386
packages [4,019KB]
Get :57 http://id.archive.ubuntu.com precise/restricted i386
packages [3,019KB]
Get :59 http://id.archive.ubuntu.com precise/universe i386
packages [873KB]
Get :62 http://id.archive.ubuntu.com precise/multiverse i386
packages [4,019KB]
Get :66 http://id.archive.ubuntu.com precise-
backports/universe translation-en [919KB]
Get :68 http://id.archive.ubuntu.com precise/main
translition-en[567KB]
```

```
Get    :69  http://id.archive.ubuntu.com  precise/restricted
translition-en[897KB]
```

```
Get    :70  http://id.archive.ubuntu.com  precise/universe
translition-en[2,897KB]
```

```
Fethed 20.1 MB in 3min 49s (87.8 KB/s)
```

```
Reading package lists... Done
```

Setelah selesai mengupdate *dns server* tersebut kemudian lanjutkan dengan menginstal *bind9* agar dapat menjalankan kelangkah berikutnya seperti dibawah.

```
Get   :1  http://id.archive.ubuntu.com  precise/main source [935
KB]
```

```
Get    :50  http://id.archive.ubuntu.com  precise/restriced
sources[5,019KB]
```

```
Get    :51  http://id.archive.ubuntu.com  precise/universe
sources[519KB]
```

```
Get    :54  http://id.archive.ubuntu.com  precise/multiverse
sources[719KB]
```

```
Get    :55  http://id.archive.ubuntu.com  precise/main  i386
packages [4,019KB]
```

```
Get   :57  http://id.archive.ubuntu.com  precise/restricted i386
packages [3,019KB]
```

```
Get   :59  http://id.archive.ubuntu.com  precise/universe  i386
packages [873KB]
```

```
Get   :62  http://id.archive.ubuntu.com  precise/multiverse i386
packages [4,019KB]
```

```
Get    :66  http://id.archive.ubuntu.com  precise-
backports/universe translation-en [919KB]
```

```
Get      :68      http://id.archive.ubuntu.com      precise/main
transltion-en[567KB]

Get      :69      http://id.archive.ubuntu.com      precise/restricted
transltion-en[897KB]

Get      :70      http://id.archive.ubuntu.com      precise/universe
transltion-en[2,897KB]

Fethed 20.1 MB in 3min 49s (87.8 KB/s)

Reading package lists... Done
```

Tampilan akhir setelah selesai *menginstall DNS Server*

```
root@ubuntu:~# apt-get install bin9
Reading package list... Done
Building dependency tree
Reading state information... Done
The following extra package will be installed:
  bin9-host bin9utils libbin9-80 libcap2  libdns81 libbisc83
  libisccc80 libisccfg82 liblwres80
susggeeted packages:
  bin9-doc rblcheck
The following NEW package will be installed;
  bin9 bin9utils libcap2
The following will be upgraded:
  bin9-host dnsutils libbin9-80 libdns81 libisc83 libisccc80
  libisccfg82 liblwres80
8 upgraded, 3 newly installed,0 to remove and 172 not
upgraded.
Need to get 1.867 KB of archives.
```

After this operation, 1.310 KB of additional disk space will be used.

D you want to continue [y/n]? Y

Processing triggers for ureadahead ...

ureadahead will be reprofiled on next reboot

Setting up libcap2 (1:2.22-lubuntu3) ...

Setting up libisc83 (1:9.8.1 dfsg.P1-lubuntu0.22) ...

Setting up libdns81 (1:9.8.1 dfsg.P1-lubuntu0.22) ...

Setting up libsc80 (1:9.8.1 dfsg.P1-lubuntu0.22) ...

Setting up libsc82 (1:9.8.1 dfsg.P1-lubuntu0.22) ...

Setting up libbin9-80 (1:9.8.1 dfsg.P1-lubuntu0.22) ...

Setting up dnsutils (1:9.8.1 dfsg.P1-lubuntu0.22) ...

Setting up bin9-host (1:9.8.1 dfsg.P1-lubuntu0.22) ...

Setting up dnsutils (1:9.8.1 dfsg.P1-lubuntu0.22) ...

Setting up bin9 (1:9.8.1 dfsg.P1-lubuntu0.22) ...

Adding group 'bind' (GID 106)...

Done

Adding system user 'bind' (UID 106)

Adding new user 'bind' (UID 106) with group 'bind' ...

Not creating home directory 'var/cache/bind'.

wrote key file "/etc/bind/rndc.key"

#

*Starting domain name service... bind9 OK

processing triggers for libc-bin ...

idconfig deferred processing now talking place

Lalu lanjutkan dengan perintah dibawah

```

root@ubuntu:~# cd /etc/bind
root@ubuntu:/etc/bind# ls
bind.keys  db.255      db.root     nemed.conf
           named.conf.options
db,o db.empety  db.perpus  nemd.conf.default-zones
           rndc.key
db.127     db.local   db.perpus.rev  named.conf.local
           Zones.rfc1918
root@ubuntu:/etc/bind# nano named.conf.default-zones

```

Kemudian tambahkan *script* dibawah agar dapat menampilkan db.perpus yang mau dibuat.

```

};
zone "0.in-addr.arpa"{
    type master;
    file "/etc/bind/db.255";
};
zone "200.indrr.arpa" {
    type master;
    file "/etc/bind/db.255";
};
zone "perpus.net"{
    type master;
    file "/etc/bind/db.perpus";
};
zone "200.168.192.in-adrrs.arpa"{
    type master;

```



```

@           IN      NS      seloshop.net.
@           IN      A       192.168.200.1
@           IN      A       192.168.200.1
www         IN      A       192.168.200.1
mail        IN      A       192.168.200.1
ftp         IN      A       192.168.200.1

```

Untuk mengatur *name Dns server* lakukan perintah selanjutnya

```

root@ubuntu:/etc/bind# nano /etc/resolv.conf
# Dynamic resolv.conf(5) file for glibc resolver(3)
generated by resolvconf(8)
# DO NOT EDIT THIS FILE BY HAND -- YOUR CHANGES WILL BE
OVERWRITTEN
search seloshop.net
nameserver 192.168.43.1
nameserver 8.8.8.8

```

Kemudian tekan **ctrl x** dan **y** untuk menyimpan lalu lanjut kelangkah berikut

```

root@ubuntu:/etc/init.d/bind9 restart
* stopping domain name service... bind9
waiting for pid 913 to die [ok]
*starting domain name service... bind9 [ok]
root@ubuntu:/etc/bind#

```

Setelah selesai melakukan *setting dns server* maka perlu dilakukan pengujian agar kita mengetahui apakah *dns server*nya dapat berfungsi dengan baik kana jika tidak berfungsi maka program tidak akan bisa dijalankan atau tidak berjalan dengan baik. Maka diperlukan pengujian sebagai berikut pengujian ini

dilakukan dengan menggunakan *windows xp* yang terhubung dengan *Adapter 2 linux* dengan memasukkan perintah-perintah dibawah ini.

```
* starting domain name service... bind9
```

```
root@ubuntu:/etc/bind# nslookup perpus.net
```

```
Server:          192.168.43.1
```

```
Address:         192.168.43.1#53
```

```
Non-authoritative answer:
```

```
Name:           perpus.net
```

```
Address:194.9.94.86
```

```
Nmae:          perpus.net
```

```
Address: 194.9.94.85
```

```
root@ubuntu:/etc/bind# dig perpus.net
```

```
; <<>> DIG 9.8.1-p1 <<>> perpus.net
```

```
;; global options: +cmd
```

```
:: Got answer:
```

```
::->>HEADER<<- opcode: QUERY: 1, ANSWER:2, AUTHORITY: 0,
```

```
ADDITIONAL: 0
```

```
;; QUESTION SECTION:
```

```
;Perpus.net.      IN      A
```

```
;; ANSWER SECTION:
```

```
perpus.net.      3348 IN      A      194.9.94.85
```

```
perpus.net.      3348 IN      A      194.9.94.86
```

```
;; Query time: 193 msec
```

```
;; SERVER: 192.168.43.1#53(192.168.43.1)
```

```
;; WHEN: Thu Mar 19 19:28:26 2020
```

```
;; MSG SIZE rcvd: 62
```

Kemudian untuk menyimpan script tekan ctrl X dan Y kemudian Enter

```

Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.

C:\Documents and Settings\Administrator>ping www.seloshop.net
Pinging www.seloshop.net [192.168.200.1] with 32 bytes of data:
Reply from 192.168.200.1: bytes=32 time<1ms TTL=64
Reply from 192.168.200.1: bytes=32 time<1ms TTL=64
Reply from 192.168.200.1: bytes=32 time<1ms TTL=64
Reply from 192.168.200.1: bytes=32 time=2ms TTL=64

Ping statistics for 192.168.200.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 2ms, Average = 0ms

C:\Documents and Settings\Administrator>ping ftp.seloshop.net
Pinging ftp.seloshop.net [192.168.200.1] with 32 bytes of data:
Reply from 192.168.200.1: bytes=32 time<1ms TTL=64
Reply from 192.168.200.1: bytes=32 time<1ms TTL=64
Reply from 192.168.200.1: bytes=32 time<1ms TTL=64
Reply from 192.168.200.1: bytes=32 time=1ms TTL=64

Ping statistics for 192.168.200.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\Documents and Settings\Administrator>ping mail.seloshop.net

```

Gambar 4.1 Pengujian client

4.2.2 Setting Web Server

Setting web server ini adalah sebagai pembuatan sebuah alamat web yang ingin digunakan dalam suatu *web page login* yang dibuat. Maka diperlukan langkah sebagai berikut :

```

root@ubuntu:/etc/bind# apt-get install apache2 links
Reading package lists... Done
Building dependency tree
Reading state information... Done

```

```

Links is already the newest version.
apache2 is already the newest version.
0 upgrade, 0 newly installed, 0 to remove and 120 not
upgraded.
root@ubuntu:/etc/bind# links perpus.net

```

Kemudian setelah memasukkan perintah *links* perpus.net dilanjutkan dengan pengeditan *website* perpustakaan yang akan dibuat seperti pada perintah dibawah ini.

```

html<<body><h1>selamat datang di website perpus</h1>
p>server ini masih dalam tahap uji coba</p>
p>isi/konten server ini belum dibuat,mohon bersabar</p>
/body></html>

```

Kemudian untuk membuat file **info.php** ketikkan *script* sebagai berikut.

```

root@ubuntu:/etc/bind# nano /var/www/info.php

```

Kemudian tambahkan *script* dibawah ini

```

>?
phpinfo();
?>

```

Setelah memasukkan script tersebut maka akan dilakukan penginstalan *php5-mysql* dan *mysql-server* seperti dibawah ini.

```

root@ubuntu:/etc/bind# apt-get install php5-mysql
Reading package list... Done
Building dependency tree
Reading state information... Done

```

php5-mysql is already the newest version.

0 upgrade, 0 newly installed, 0 to remove and 167 not
upgrade.

```
root@ubuntu:/etc/bind# apt-get install mysql-server
```

```
Reading package list... Done
```

```
Building dependency tree
```

```
Reading state information... Done
```

```
The following extra package will be installed:
```

```
libdbd-mysql-perl libdbi-perl libhtml- template-perl  
libnet-daemon-perl
```

```
libplrpc-perl libtera-ready-perl mysql-client-5.5 mysql-  
client-core
```

```
mysql-server-5.5 mysql-server-core- 5.5 perl perl-base  
perl-modules
```

```
Suggested packages:
```

```
libipc-sheredcahce-perl tinyca mailx perl-doc libtern-  
readline-gnu-perl
```

```
libtern-readline-perl-perl make libpod-plainer-perl
```

```
The following NEW packages will be installed:
```

```
libdbd-mysql-perl libdbi-perl libhtml- template-perl  
libnet-daemon perl
```

```
mysql-server mysql-server-5.5 mysql- server-core-5.5
```

```
The following packages will be upgraded:
```

```
perl perl-base perl-modules
```

8 upgrade, 11 newly installed, 0 to remove and 164 not
upgade

need to get 34.4 MB of archives.

after this operation, 89.2 MB of additional disk space will
used.

do you want to continue [Y/n]? Y

Setelah selesai penginstalan maka masukkan *password* untuk *root* dimana *password* ini agar dapat masuk ke database dari *phpmyadmin*. Mencoba masuk ke *mysql* dengan *user* dan *password* maka dilakukan penginstalan *phpmyadmin* untuk *web server* dengan melakukan perintah dibawah ini.

```
root@ubuntu:~# apt-get install phpmyadmin
```

```
Reading package list... Done
```

```
Building dependency tree
```

```
Reading state information... Done
```

```
The following extra package will be installed:
```

```
  dbconfig-common libncrypt4 php5-ncrypt
```

```
suggested packages:
```

```
  libncrypt-dev ncrypt
```

```
The following NEW packages will be installed:
```

```
  dbconfig-common libncrypt4 php5-ncrypt  phpmyadmin
```

```
0 upgrade, 4 newly installed, 0 to remove and 164 not  
upgraded.
```

```
Need to get 5,894 kb of archives.
```

```
After this operation, 17.7 MB of additional disk space will  
be used.
```

```
Do you want to continue [Y/n]? Y
```

Setelah itu maka akan pilih *apache2* lalu kemudian restart Apache2 dengan perintah berikut.

```
root@ubuntu:~# /etc/init.d/apache2 restart
*Restaring web server apache2
apache2: could not reliably determine the server's fully
qualified domain name,
using 127.0.1.1 for servername
... waiting apache2: could not realibly determine the
server's fully qualified domain name, using 127.0.1.1 for
servername
```

Setelah selesai melakukan penginstalan *setting dns server* dan *setting web server* serta *tools-tools* tambahannya maka akan mendapatkan hasil akhir dari *web page login* tersebut. Adapun penjelasan-penjelasan penggunaan dari *web page login* yang berbasis *web server* lokal tersebut adalah sebagai berikut :

4.3 Pengujian Aplikasi

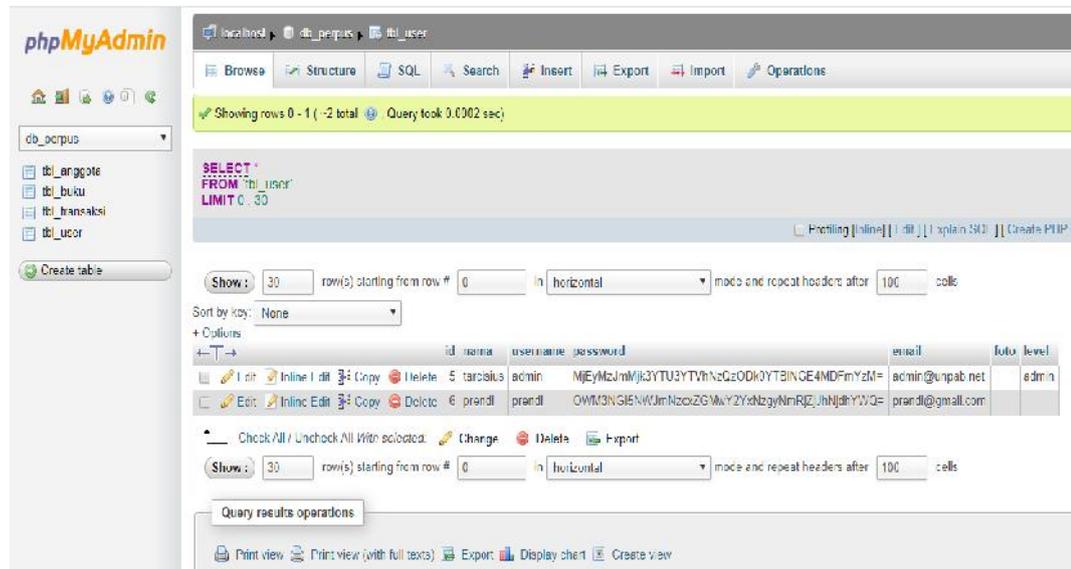
Tabel 4.1 Pengujian Web Login

No	Pengujian Skenario	Test case	Hasil yang Diharapkan	Hasil pengujian	kesimpulan
1	Username dan Password tidak diisi kemudian klik tombol Login	Username: (kosong) Password: (kosong)	Sistem akan menolak dan menampilkan pesan “Harap isi username dan password”	Sesuai harapan	Valid
2	Mengetikkan username dan	Username : admin	Sistem akan menolak dan akan		

	tidak mengisi password kemudian klik Login	Password : (kosong)	menampilkan “password belum diisi”	Sesuai harapan	Valid
3	Mengetikkan password dan tidak mengisi username kemudian klik Login	Username : (kosong) Password : admin	Sistem akan menolak dan menampilkan “username belum diisi”	Sesuai harapan	Valid
4	Mengetikkan username dan password tidak sesuai kemudian klik Login	Username : Adm Password : admin12	Sistem akan menolak dan akan menampilkan “username atau password yang anda masukkan salah”	Sesuai harapan	Vaid
5	Mengetikkan username dan password yang benar kemudian klik Login	Username : admin Password : admin	Sistem menerima akses login kemudian akan menampilkan halaman utama admin	Sesuai harapan	Vaid

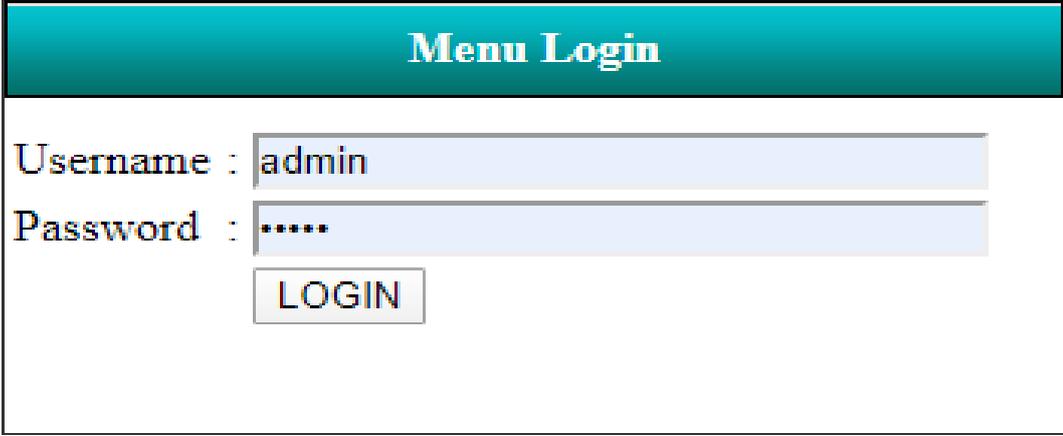
Maka dari tabel diatas agar dapat login kedalam sistem yang dibangun *username* dan *password* harus diisi sesuai dengan yang sudah dibuat oleh admin jika salah satu diantaranya tidak di isi atau salah dalam penulisan maka sistem tidak akan menerima masuk kedalam halaman yang dibangun karna *username* dan *password* sangat saling terkait dalam proses *login* tersebut. Adapun cara mengenkripsi *username* dan *password* dapat dilihat dari gambar dibawah dimana

pada gambar tersebut dijelaskan letak enkripsi dan deskripsi pada *username* dan *password*.



Gambar 4.2 Rancangan *Web Login*

Dari gambar diatas maka dapat dijelaskan bahwa rancangan *web login* yang akan dibangun dengan cara mengenkripsi *username* dan *password* yang mana terletak pada *table user*. Maka proses enkripsi terletak pada admin yang akan dienkripsi menjadi `mjEyMzjmMjk3YTVhNzQzODk0YTBINGE4MDFmymz=` setelah selesai melakukan proses enkripsi maka dilakukan pengujian terhadap web login dengan cara berikut.



Gambar 4.3 Halaman *Login Admin*

Halaman *Login* admin dengan mengisi *username* dan *password* dengan benar. Dimana dalam *form* ini seorang admin harus lah melakukan proses *login* terlebih dahulu untuk dapat mengakses data-data kepentingan dalam db.perpus. Maka setelah itu admin dapat mengakses *from* data-data lainnya.

4.4 Hasil Pengujian Aplikasi

Hasil pengujian akan menampilkan halaman-halaman yang mana sudah di rancang dalam sistem yang dibangun setelah berhasil login dengan memasukkan *username* dan *password* dengan tepat kedalam web page tersebut.

4.4.1 Home



Gambar 4.4 Halaman *Home*

Halaman *home* dimana dalam *form* ini berisi tentang halaman utama pada saat admin melakukan *login*, tampilan *form* ini berupa data waktu, tanggal dan *form* yang telah diinput. Dalam halaman utama tersebut terdapat beberapa *form* beserta fungsi-fungsi dari *form* tersebut.

4.4.2 Halaman Data *From* Buku



The screenshot displays the 'Data Buku' page. At the top, there is a yellow banner with the university logo and name: 'Universitas Pembangunan Panca Budi Beriman, Berilmu, Barkarya'. Below the banner, the user 'tarcisius' is logged in on 'Senin, 13 April 2020'. A sidebar menu on the left contains the following items: » Home, » Buku, » Anggota, » Transaksi, » Laporan, » User, and » Logout. The main content area is titled 'Data Buku' and includes a search bar with the text 'Input Buku' and a search button labeled 'cari'. Below the search bar is a table with the following data:

No	Judul Buku	Pengarang	Penerbit	Jumlah	Edit	Hapus
1	matematika	kokom	Airlangga	4		
2	PHP Dasar	Arfandi	Lokomedia	3		
3	Samudra PHP	Solihin	Hamzah	2		

Below the table, it states 'Jumlah : 3 buku'. At the bottom of the page, there is a footer that reads '2020 - Modified Web By Tarcisius@gmail.com'.

Gambar 4.5 Halaman Data Buku

Halaman data buku dimana dalam *form* ini berisi tentang jenis buku, pengarang, penerbit dan jumlah. Dalam *form* ini juga admin masih dapat menambahkan ataupun mengurangi data buku lainnya sesuai dengan ketentuan yang telah dibuat.

4.4.3 Halaman Data *Form* Anggota

Universitas Pembangunan Panca Budi
Beriman, Berilmu, Barkarya

tarcisius Senin, 13 April 2020

Menu Utama

- » Home
- » Buku
- » Anggota
- » Transaksi
- » Laporan
- » User
- » Logout

Data Anggota

[Input Anggota](#)

No	Nim	Nama	Prodi	Thn Masuk	Edit	Hapus
1	2015804045	Wewen	Komputer Akuntansi	2014		

Jumlah : 1 Anggota

2020 - Modified Web By Tarcisius@gmail.com

Gambar 4.6 Halaman Data Anggota

Halaman data anggota dimana halaman *from* ini terdapat nama anggota, nim, prodi, dan tahun masuk.

4.4.4 Halaman Data *Form* Transaksi

Universitas Pembangunan Panca Budi
Beriman, Berilmu, Barkarya

tarcisius Senin, 13 April 2020

Menu Utama

- » Home
- » Buku
- » Anggota
- » Transaksi
- » Laporan
- » User
- » Logout

Data Transaksi

[Input Transaksi](#)

No	Judul Buku	Peminjam	Tgl Pinjam	Tgl Kembali	Terlambat Kembali	Perpanjang
1	matematika	Wewen Nurwendi	01-11-2015	08-11-2015	1518 hari (Rp 3236000)	perpanjang

Jumlah : 1 Transaksi

2020 - Modified Web By Tarcisius@gmail.com

Gambar 4.7 Halaman Data Transaksi

Halaman data transaksi dimana dalam *form* ini terdapat nama peminjam, judul buku yang dipinjam, tanggal pinjaman, tanggal kembali, keterlambatan pengembalian dan perpanjangan waktu pengembalian. Dalam *form* ini admin juga dapat menambah data-data buku yang dipinjam atau dikembalikan.

4.4.5 Halaman Data *Form* Laporan



Gambar 4.8 Halaman Data Laporan

Halaman data laporan dimana dalam *form* ini terdapat data seluruh laporan yang terdapat pada db.perpus tersebut seperti laporan buku, laporan anggota dan laporan transaksi. Dimana didata laporan tersebut admin akan menginput seluruh laporan dan menyimpan agar tidak kehilangan data-data dari setiap laporan.

4.4.6 Halaman Data *Form* User

Halaman data *user* dimana dalam *form* ini terdapat data setiap admin seperti nama, email, dan level. Dimana dalam *form* ini admin dapat menambahkan admin

dengan level yang ditentukan oleh admin yang pertama. Seperti pada gambar dibawah ini.

The screenshot shows the 'Data User' page of a web application. The header includes the logo of Universitas Pembangunan Panca Budi and the motto 'Beriman, Berilmu, Barkarya'. The page displays a table of users with the following data:

No	Nama	Email	Level	Edit	Hapus
1	tarcisius	admin@unpab.net	admin		
2	prendi	prendi@gmail.com			

Below the table, it indicates 'Jumlah : 2 User'. The page also features a search bar and a footer with the text '2020 - Modified Web By Tarcisius@gmail.com'.

Gambar 4.9 Halaman Data *User*

4.5 Perhitungan Manual Enkripsi Md5 dan Base64

Adapun contoh perhitungan manual enkripsi Md5 dan base64 adalah sebagai berikut:

1. Perhitungan manual enkripsi Md5 dan Base64

Perhitungan manual md5 yang akan di enkripsi adalah username dan password contohnya :

Username = admin

Password = admin

Maka perhitungan manual enkripsi md5 dari kata “admin” adalah 21232f297a57a5a743894a0e4a801fc3. Setelah mendapatkan hasil enkripsi md5 dari admin maka lanjutkan dengan perhitungan manual enkripsi

base64, yang akan dienkripsi adalah hasil dari enkripsi md5. Contohnya sebagai berikut:

Encoding Base64 dari hasil md5 21232f297a57a5a743894a0e4a801fc3 adalah sebagai berikut:

Ambil nilai binary hasil perhitungan enkripsi md5 dari Ascii setiap karakter 21232f297a57a5a743894a0e4a801fc3 contohnya :

2, ascii: 50, binary: 00110010

1, ascii: 49, binary: 00110001

2, ascii: 50, binary: 00110010

3, ascii: 51, binary: 00110011

2, ascii: 50, binary: 00110010

f, ascii: 102, binary: 01100110

2, ascii: 50, binary: 00110010

9, ascii: 57, binary: 00111001

7, ascii: 55, binary: 00110111

a, ascii: 97, binary: 01100001

5, ascii: 53, binary: 00110101

7, ascii: 55, binary: 00110111

a, ascii: 97, binary: 01100001

5, ascii: 53, binary: 00110101

a, ascii: 97, binary: 01100001

7, ascii: 55, binary: 00110111

4, ascii: 52, binary: 00110100

3, ascii: 51, binary: 00110011

8, ascii: 56, binary: 00111000

9, ascii: 57, binary: 00111001

4, ascii: 52, binary: 00110100

a, ascii: 97, binary: 01100001

0, ascii: 48, binary: 00110000

e, ascii: 101, binary: 01100101

4, ascii: 52, binary: 00110100

a, ascii: 97, binary: 01100001

8, ascii: 56, binary: 00111000

0, ascii: 48, binary: 00110000

1, ascii: 49, binary: 00110001

f, ascii: 102, binary: 01100110

c, ascii: 99, binary: 01100011

3, ascii: 51, binary: 00110011

Deretan binary dijadikan 1 baris “21232f297a57a5a743894a0e4a801fc3” :

```
001100100011000100110010001100110011001001100110001100100011100100
110111011000010011010100110111011000010011010101100001001101110011
010000110011001110000011100100110100011000010011000001100101001101
0001100001001110000011000000110001011001100110001100110011.
```

Setiap 6 bit akan mewakili 1 karakter base64 dan panjang kata yang bukan kelipatan 3 akan ada padding “=” sepanjang satu karakter.

Binary = Desimal = Karakter base64

00001100 = 12 = M

00100011 = 35 = j

00000100 = 4 = E

00110010 = 50 = y

00001100 = 12 = M

00110011 = 51 = z

00001001 = 9 = J

00100110 = 38 = m

00001100 = 12 = M

00100011 = 35 = j

00100100 = 36 = k

00110111 = 55 = 3

00011000 = 24 = Y

00010011 = 19 = T

00010100 = 20 = U

00110111 = 55 = 3

00011000 = 24 = Y

00010011 = 19 = T

00010101 = 21 = V

00100001 = 33 = h

00001101 = 13 = N

00110011 = 51 = z

00010000 = 16 = Q

00110011 = 51 = z

00001110 = 14 = O

00000011 = 3 = D

00100100 = 36 = k

00110100 = 52 = 0

00011000 = 24 = Y

00010011 = 19 = T

00000001 = 1 = B

00100101 = 37 = l

00001101 = 13 = N

00000110 = 6 = G

00000100 = 4 = E

00111000 = 56 = 4

00001100 = 12 = M

00000011 = 3 = D

00000101 = 5 = F

00100110 = 38 = m

00011000 = 24 = Y

00110011 = 51 = z

00001100 = 12 = M

Maka hasil *encoding base64* dari 21232f297a57a5a743894a0e4a801fc3

adalah : MjEyMzJmMjk3YTU3YTVhNzQzODk0YTBINGE4MDFmYzM=

BAB V

KESIMPULAN DAN SARAN

5.1 Kesimpulan

Berdasarkan dari uraian yang telah dibahas sebelumnya melalui implementasi dan pengujian sistem, maka penulis dapat mengambil kesimpulan sebagai berikut:

1. Dengan adanya pengamanan *web page login* ini maka dapat meningkatkan keamanan dalam *database* dari *web page login* yang berbasis web server lokal .
2. Kombinasi algoritma md5 dan base64 dapat menjadi sebuah algoritma dengan keamanan yang memadai dan dapat digunakan untuk mengamankan *database* dari sebuah *website* yang dibuat
3. Kombinasi algoritma md5 dan base64 dapat di implementasikan kedalam sebuah sistem enkripsi *database web page login* dengan baik.

5.2 Saran

1. Perkembangan sistem pengamanan *web page login* yang berbasis *web* perlu dilakukan dengan seiring dengan zaman untuk menyesuaikan dengan teknologi yang terus berkembang.
2. Pengamanan *web page login* dengan menggunakan kombinasi algoritma md5 dan base64 perlu dikembangkan dengan menggunakan kombinasi algoritma lainnya agar lebih menjamin keamanan *database* dengan baik

3. Untuk kelancaran dalam penggunaan sistem web page login perawatan komputer harus diperhatikan mulai dari sistem perangkat keras (*Hardware*) maupun perangkat lunak (*Software*)

Daftar Pustaka

- Aulia, N. (2012). *Aplikasi Enkripsi Dan Dekripsi Menggunakan Visual Basic 2012 Dengan Algoritma Triple Des*. May.
- Barus, S., Sitorus, V. M., Napitupulu, D., Mesran, M., & Supiyandi, S. (2018). *Sistem Pendukung Keputusan Pengangkatan Guru Tetap Menerapkan Metode Weight Aggregated Sum Product Assesment (WASPAS)*. *Jurnal Media Informatika Budidarma*, 2(2).
- Batubara, Supina, Sri Wahyuni, and Eko Hariyanto. "Penerapan Metode Certainty Factor Pada Sistem Pakar Diagnosa Penyakit Dalam." *Seminar Nasional Royal (SENAR)*. Vol. 1. No. 1. 2018.
- Ertie Nur Hartiwati. (2014). *Keamanan Jaringan Dan Keamanan Sistem Komputer Yang Mempengaruhi Kualitas Pelayanan Warnet*. *Jurnal Ilmiah Informatika Komputer Universitas Gunadarma*, 27–33.
- Fachri, Barany; Windarto, Agus Perdana; Parinduri, Ikhsan. *Penerapan Backpropagation dan Analisis Sensitivitas pada Prediksi Indikator Terpenting Perusahaan Listrik*. *JEPIN (Jurnal Edukasi dan Penelitian Informatika)*, 2019, 5.2: 202-208.
- Gunadhi, E., & Nugraha, A. P. (2017). *Penerapan Kriptografi Base64 Untuk Keamanan URL (Uniform Resource Locator) Website Dari Serangan SQL Injection*. *Jurnal Algoritma*, 13(2), 391–398. <https://doi.org/10.33364/algoritma/v.13-2.391>
- Inayatullah. (2007). *Analisis Penerapan Algoritma MD5 Untuk Pengamanan Password*. *Jurnal Algoritma*.
- Kurniawan, H. (2018). *Pengenalan Struktur Baru untuk Web Mining dan Personalisasi Halaman Web*. *Jurnal Teknik dan Informatika*, 5(2), 13-19.
- Khairul, K., IlhamiArsyah, U., Wijaya, R. F., & Utomo, R. B. (2018, September). *Implementasi augmented reality sebagai media promosi penjualan rumah*. *In Seminar Nasional Royal (SENAR)* (Vol. 1, No. 1, pp. 429-434).
- Mubarak, A., & Wahid, F. (2006). *Aplikasi untuk Menentukan IP Address dan Subnetmask Host pada Suatu Jaringan*. *Media Informatika*, 4(1), 1–11. <https://doi.org/10.20885/informatika.vol4.iss1.art1>

- Muslim, M. A. (2006). *Pengembangan Distro Ubuntu untuk Aplikasi Game Centre. Teknologi Informasi DINAMIK, XI(Ubuntu)*, 16–22.
- Nugroho1, A. Y. (2015). Pembuatan aplikasi kriptografi algoritma base 64 menggunakan php untuk mengamankan data text. *Seminar Nasional Informatika, 1(1)*, 134–139.
- Prasetyo, R., & Suryana, A. (2016). Aplikasi Pengamanan Data dengan Teknik Algoritma Kriptografi AES dan Fungsi Hash SHA-1 Berbasis Desktop. *Jurnal Sisfokom (Sistem Informasi Dan Komputer)*, 5(2), 61. <https://doi.org/10.32736/sisfokom.v5i2.40>
- Putra, Randi Rian. "Sistem Informasi Web Pariwisata Hutan Mangrove di Kelurahan Belawan Sicanang Kecamatan Medan Belawan Sebagai Media Promosi." *Jurnal Ilmiah Core IT: Community Research Information Technology 7.2* (2019).
- Ramadhani, S. (2017). Analisis Sistem Keamanan Web Server Dan Database Server Menggunakan Suricata. *Seminar Nasional Teknologi Informasi, Komunikasi Dan Industri (SNTIKI) 9 Fakultas Sains Dan Teknologi, UIN Sultan Syarif Kasim Riau*, 308–317.
- Ridha, M. A. (2014). *Implementasi Kriptografi Menggunakan Algoritma Md5 Berbasis Java*
- Rahim, R., Supiyandi, S., Siahaan, A. P. U., Listyorini, T., Utomo, A. P., Triyanto, W. A., ... & Khairunnisa, K. (2018, June). *Topsis Method Application for Decision Support System in Internal Control for Selecting Best Employees. In Journal of Physics: Conference Series* (Vol. 1028, No. 1, p. 012052). IOP Publishing.
- Sari, R. D., Supiyandi, A. P. U., Siahaan, M. M., & Ginting, R. B. (2017). *A Review of IP and MAC Address Filtering in Wireless Network Security. Int. J. Sci. Res. Sci. Technol*, 3(6), 470-473.
- Sidik, A. P., Efendi, S., & Suherman, S. (2019, June). *Improving One-Time Pad Algorithm on Shamir's Three-Pass Protocol Scheme by Using RSA and ElGamal Algorithms. In Journal of Physics: Conference Series* (Vol. 1235, No. 1, p. 012007). IOP Publishing.
- Siahaan, A. P. U., Aryza, S., Nasution, M. D. T. P., Napitupulu, D., Wijaya, R. F., & Arisandi, D. (2018). *Effect of matrix size in affecting noise reduction level of filtering.*
- Syahputra, Rizki, and Hafni Hafni. "analisis kinerja jaringan switching clos tanpa buffer." *journal of science and social research 1.2* (2018): 109-115.

- Tasril, V. (2018). *Sistem Pendukung Keputusan Pemilihan Penerimaan Beasiswa Berprestasi Menggunakan Metode Elimination Et Choix Traduisant La Realite*. *INTECOMS: Journal of Information Technology and Computer Science*, 1(1), 100-109.
- Wijaya, Rian Farta, et al. "Aplikasi Petani Pintar Dalam Monitoring Dan Pembelajaran Budidaya Padi Berbasis Android." *Rang Teknik Journal* 2.1 (2019).
- Wahyuni, Sri. "Implementasi Rapidminer Dalam Menganalisa Data Mahasiswa Drop Out." *Jurnal Abdi Ilmu* 10.2 (2018): 1899-1902.
- Zen, Muhammad. "perbandingan metode dimensi fraktal dan jaringan syaraf tiruan backpropagation dalam sistem identifikasi sidik jari pada citra digital." *jitekh* 7.2 (2019): 42-50

