PENGEMBANGAN MODEL ANTAR MUKA BASIS DATA BERBASIS FUNGSI MD5

SKRIPSI

OLEH:

MUHAMMAD DARUL MUSLIM
08142118

PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS BINA DARMA
PALEMBANG

TAHUN 2012

PENGEMBANGAN MODEL ANTAR MUKA BASIS DATA BERBASIS FUNGSI MD5

SKRIPSI

Diajukan Sebagai Syarat Memperoleh Gelar Sarjana Komputer

OLEH:

MUHAMMAD DARUL MUSLIM
08142118

PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS BINA DARMA
PALEMBANG

TAHUN 2012

HALAMAN PENGESAHAN

PENGEMBANGAN MODEL ANTAR MUKA BASIS DATA BERBASIS FUNGSI MD5

OLEH :

MUHAMMAD DARUL MUSLIM
08142118

SKRIPSI

Telah Diterima Sebagai Salah Satu Syarat Untuk Memperoleh
Gelar Sarjana Komputer

Palembang, Agustus 2012
Program Studi Teknik Informatika
Fakultas Ilmu Komputer
Universitas Bina Darma Palembang

Pembimbing I **Dekan,**

(Syahril Rizal, S.T., M.M., M.Kom) **(M. Izman Herdiansyah, S.T., M.M., Ph.D)**

Pembimbing II

(Suyanto, M.M., M.Kom)

HALAMAN PERSETUJUAN

Skripsi Berjudul **"Pengembangan Model Antar Muka Basis Data Berbasis Fungsi MD5"** Oleh **"Muhammad Darul Muslim"** telah dipertahankan didepan komisi penguji pada hari **Sabtu** tanggal **11 Agustus 2012.**

Komisi Penguji

1. Syahril Rizal, S.T., M.M., M.Kom	**Ketua**	**(……...)**
2. Suyanto, M.M., M.Kom	**Sekertaris**	**(……...)**
3. M. Izman Herdiansyah, S.T., M.M., Ph.D	**Anggota**	**(……...)**
4. Abdullah, S.Kom., M.MSi.	**Anggota**	**(……...)**

Mengetahui,
Program Studi Teknik Informatika
Fakultas Ilmu Komputer
Universitas Bina Darma Palembang
Ketua,

(Syahril Rizal, S.T., M.M., M.Kom)

PERNYATAAN

Saya yang bertanda tangan dibawah ini menyatakan dengan sesungguhnya bahwa seluruh data dan informasi yang disajikan dalam skripsi ini, kecuali yang disebutkan dengan jelas sumbernya, adalah hasil investigasi saya sendiri dan belum pernah atau tidak sedang disajikan sebagai syarat memperoleh sebutan professional lain atau sebutan yang sama ditempat lain. Apabila pernyataan ini tidak benar, saya bersedia menerima sanksi kecuali yang disebutkan dengan jelas sumbernya.

Palembang, Agustus 2012
Yang membuat pernyataan,

MUHAMMAD DARUL MUSLIM
08142118

MOTTO DAN PERSEMBAHAN

MOTTO

"Jadilah Manusia Berguna di Manapun Berada dan Berusaha Tidak Akan Menyombongkan Diri Dalam Kegunaannya"

PERSEMBAHAN

Dengan Mengharapkan Keridhoan Allah SWT
Kupersembahkan Untuk :

- *Ayah dan Ibu Tercinta Yang Selalu Mendo'akan dan Mengorbankan Segalanya Untuk Keberhasilanku.*
- *Para Pendidikku.*
- *Untuk Sahabatku Yang Telah Memberikan Semangat dan Membantuku.*
- *Kepada Dosen Pembimbing Skripsi ini.*
- *Untuk Yang Tersayang Yang Telah Membantu Moril dan Selalu Memberi Semangat.*
- *Almamaterku.*

DAFTAR ISI

Halaman

DAFTAR GAMBAR

Halaman

DAFTAR TABEL

Halaman

KATA PENGANTAR

Puji syukur kehadirat Allah SWT karena berkat rahmat dan karunia-Nya jualah, skripsi penelitian ini dapat diselesaikan guna memenuhi salah satu syarat untuk diteruskan menjadi skripsi sebagai proses akhir dalam menyelesaikan pendidikan dibangku kuliah.

Dalam penulisan skripsi ini, tentunya masih jauh dari sempurna. Hal ini dikarenakan keterbatasnya pengetahuan yang dimiliki. Oleh karena itu dalam rangka melengkapi kesempurnaan dari penulisan skripsi ini diharapkan adanya saran dan kritik yang diberikan bersifat membangun.

Pada kesempatan yang baik ini, tak lupa penulis menghaturkan terima kasih kepada semua pihak yang telah memberikan bimbingan, pengarahan, nasehat dan pemikiran dalam penulisan skripsi ini, terutama kepada :

1. Prof. Ir. H. Bochari Rahman, M.Sc. selaku Rektor Universitas Bina Darma Palembang.

2. M. Izman Herdiansyah, S.T., M.M., Ph.D., selaku Dekan Fakultas Ilmu Komputer.

3. Syahril Rizal, S.T., M.M., M.Kom., selaku Ketua Program Studi Teknik Informatika dan pembimbing utama.

4. Suyanto, M.M., M.Kom., selaku Pembimbing Pendamping yang telah memberikan bimbingan penulisan proposal ini.

5. Orang tua, saudara-saudaraku, seluruh teman dan sahabat-sahabatku yang selalu memberikan dorongan dan masukan serta bantuan baik moril maupun materil yang tak ternilai harganya.

Palembang, Agustus 2012

Penulis

ABSTRAK

Permasalahan dalam penggunaan MD5 adalah hasil MD5 tidak bisa dikembalikan lagi seperti asalnya, sehingga jika di terapkan pada pembuatan *password* dalam *database*, maka user tidak bisa lagi melakukan login. Penyebab MD5 pada dasarnya algoritma hash hanya untuk satu arah saja. Penggunaan hasil MD5 secara standard sudah tidak aman lagi, karena telah banyak cara-cara untuk menampilkan hasil MD5 yang aslinya, salah satunya menggunakan *website* http://md5crack.com/crackmd5.php. Solusi dari permasalahan tersebut perlu dibangun dekripsi MD5 pada *database*, agar jika user lupa *password* bisa lihat *password* aslinya. Sedangkan untuk keamanan dari dekripsi tersebut dari *cracker* yang tidak bertanggung jawab perlu dibuat *double* MD5 atau lebih dan juga bisa disisipkan kunci pada hasil MD5 tersebut dalam *database*. Keuntungan dari yang didapat dari solusi diatas adalah optimalisasi menggunaan MD5. Dari beberapa penjelasan di atas, penulis sangat tertarik untuk membuat penelitian proposal skripsi dengan judul "**Pengembangan Model Antar Muka Basis Data Berbasis Fungsi MD5**".

Kata Kunci : Model, Antar Muka, MD5

BAB I
PENDAHULUAN

1.1 Latar Belakang

Kemajuan teknologi dan perkembangan dunia digital yang sangat pesat, sehingga saat ini membuat lalu lintas penggunaan data digital semakin ramai. Hampir setiap orang melakukan aktifitas penggunaan data setiap harinya. Data yang digunakan harus mempunyai tingkat keamanan yang harus sangat diperhatikan. Hal inilah yang menuntut adanya sistem pengamanan data sehingga data tidak sampai disalah gunakan oleh pihak ketiga dan merugikan banyak orang. Sampai saat ini telah banyak ditemukan teknik-teknik dalam melakukan pengamanan data *password*, baik teknik klasik maupun *modern*.

Fungsi hash adalah salah satu algoritma yang digunakan untuk melakukan pengamanan data. Fungsi *hash* ini mendasari beberapa algoritma pengaman seperti *MAC, Base 64*, dan *MD5*. Pada dasarnya, fungsi *hash* mengkompresi pesan dengan panjang yang berbeda beda menjadi pesan acak yang mempunyai panjang yang terdefinisi.

Dalam perkembangannya, fungsi *Hash* atau Enskripsi ini telah banyak mengalami perbaikan, misalnya saja *Hash Message Digest* (*MD*) yang bermula

dari *MD2, MD4* dan sekarang *MD5*. *Hash Message Digest 2* (MD2) pertama kali dirancang pada tahun 1989 dan dirancang untuk komputer berbasiskan 8-bit. Fungsi ini memiliki kelemahan utama yang biasa disebut dengan *collision*. Kelemahan ini didapat berdasarkan sifat injektifnya.

Kemudian di tahun 1990 oleh *rivest*, diciptakanlah *MD4* yaitu revisi dari *MD2*. *MD4* digunakan terutama untuk memeriksa integritas dari sebuah pesan. Enkripsi ini menggunakan panjang 128 bit dan menggunakan fungsi *hash. MD4* memiliki *flaw* fatal dalam proses eksekusinya sehingga kode 32 bit *heksadesimal* yang dihasilkannya dapat ditembus walaupun waktu yang diperlukan untuk membaca kode relatif lama.

Sampai dengan tahun 1991, *Profesor Ronald Rivest* menciptakan algoritma *MD5*. *MD5* merupakan fungsi hash pengganti *MD4*, yang dianggap tidak aman lagi setelah adanya serangan yang melemahkan algoritma tersebut. Algoritma *MD5* secara umum lebih lambat dari pada *MD4*, tetapi lebih memberikan perhatian lebih ke tingkat keamanan. *MD5* ini merupakan suatu fungsi untuk merubah teks masukan menjadi nilai *hash* yang panjangnya selalu sama yaitu nilai *hash*nya tetap 128 bit atau 32 karakter *hexa*. Bahkan seseorang yang menginputkan panjang karakter satu atau nol nilai yang dihasilkan akan tetap sama yaitu 32 karakter.

Permasalahan dalam keamanan data di dalam *database* sangat pentingnya untuk menjaga kerahasiaan, terutama data-data yang sensitif yang hanya boleh diketahui isinya oleh pihak administrator atau user tertentu, sehingga perlu

dilakukan penyandian data supaya beberapa pihak yang tidak memiliki kewenangan tidak akan dapat membuka isi dari *database* tersebut. Keamanan data dalam *database* merupakan hal yang sangat penting dalam menjaga kerahasiaan. Salah satu cara yang digunakan untuk pengamanan data adalah menggunakan sistem kriptografi yaitu dengan menyediakan isi informasi (*plaintext*) menjadi isi yang tidak dipahami melalui proses enkripsi (*encipher*), dan untuk memperoleh kembali informasi yang asli, dilakukan proses deskripsi (*decipher*).

Oleh sebab itu penggunaan fungsi hash *MD5* ini sangat penting sekali dalam pengamanan data *password*. Selain itu, algoritma ini juga telah banyak digunakan oleh banyak orang dalam pengamanan data *password*. Karena *password* yang tersimpan dalam *database* merupakan hasil enskrispi dari penggunaan fungsi *MD5*. Permasalahan dalam penggunaan MD5 adalah hasil MD5 tidak bisa dikembalikan lagi seperti asalnya, sehingga jika di terapkan pada pembuatan *password* dalam *database*, maka user tidak bisa lagi melakukan login. Penyebab MD5 pada dasarnya algoritma hash hanya untuk satu arah saja. Penggunaan hasil MD5 secara standard sudah tidak aman lagi, karena telah banyak cara-cara untuk menampilkan hasil MD5 yang aslinya, salah satunya menggunakan *website* http://md5crack.com/crackmd5.php.

Solusi dari permasalahan tersebut perlu dibangun dekripsi MD5 pada *database*, agar jika user lupa *password* bisa lihat *password* aslinya. Sedangkan untuk keamanan dari dekripsi tersebut dari *cracker* yang tidak bertanggung jawab

perlu dibuat *double* MD5 atau lebih dan juga bisa disisipkan kunci pada hasil MD5 tersebut dalam *database*. Keuntungan dari yang didapat dari solusi diatas adalah optimalisasi menggunaan MD5.

Dari beberapa penjelasan di atas, penulis sangat tertarik untuk membuat penelitian proposal skripsi dengan judul "**Pengembangan Model Antar Muka Basis Data Berbasis Fungsi MD5**".

1.2 Perumusan Masalah

Dari uraian permasalahan diatas, maka penulis dapat merumuskan masalah yang dapat diambil dalam penelitian ini adalah **"**Bagaimana mengembangkan suatu antarmuka yang akan mampu melindungi basis data pada *cracker* ? ".

1.3 Batasan Masalah

Agar pembahasa tidak meluas, maka batasan yang dibahas tentang pembangunan model antar muka basis data berbasis fungsi MD5 menggunakan bahasa *scripting PHP* dan *database MySQL*.

1.4 Tujuan Penelitian

Tujuan dari penelitian ini adalah melakukan pengembangan model antar muka basis data berbasis fungsi MD5.

1.5 Manfaat Penelitian

Adapun manfaat dari penelitian ini adalah sebagai berikut :

1. Membantu dan memahami algoritma kriptografi MD5 untuk keamanan *database.*

2. Membantu menjaga keamanan *database* yang telah dibuat dan sangat penting tidak dengan mudah dibaca oleh orang yang tidak berhak.

1.6 Metode Penelitian

1.6.1 Waktu Penelitian

Dalam penelitian ini, peneliti melakukan penelitian pada model antar muka basis data berbasis fungsi MD5. Dan waktu penelitian dilakukan selama bulan Maret 2012 sampai dengan Agustus 2012.

1.6.2 Metode Pengumpulan Data

Dalam melakukan penelitian untuk mendapatkan data dan informasi, maka metode yang digunakan dalam proses pengumpulan data sebagai berikut :

1. Metode Observasi

   Dalam hal ini yang akan dilakukan adalah melihat serta mempelajari permasalahan yang ada dilapangan yang erat kaitannya dengan objek yang diteliti.

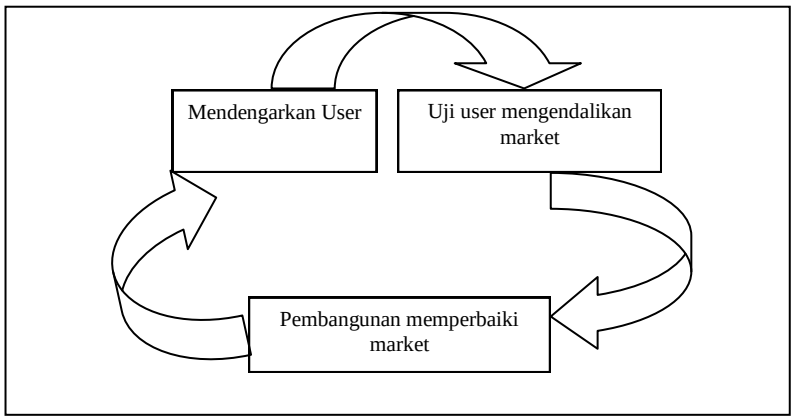
2. Metode Studi Pustaka

   Metode yang dilakukan adalah dengan cara mancari bahan yang mendukung dalam pendefinisisan masalah melalui buku-buku, *internet*.

1.6.3 Metode Pengembangan Perangkat Lunak

Metode pengembangan perangkat lunak ini menggunakan metode *prototyping*. *Prototyping* adalah proses pengembangan suatu *prototyping* secara

cepat untuk digunakan terlebih dahulu dan ditingkatkan terus menerus sampai diterapkan sistem yang utuh (Pressman,2002:39).



Gambar 1.1 *Prototyping* Paradigma

Tahapan-tahapan *prototyping* yaitu :

1. Pengumpulan kebutuhan

   Pelanggan dan pengembang bersama-sama mendefinisikan format seluruh perangkat lunak, mengidentifikasikan semua kebutuhan, dan garis besar sistem yang akan dibuat.

2. Perancangan Kilat

   Perancangan kilat berfokus pada penyajian dari aspek-aspek perangkat lunak tersebut yang akan nampak bagi pelanggan/pemakai, perancangan kilta membawa kepada kontruksi sebuah prototipe.

3. Evaluasi

   Prototipe tersebut dievaluasi oleh pelanggan atau pemakai dan dipakai untuk menyaring kebutuhan pengembangan perangkat lunak.

BAB II
LANDASAN TEORI

2.1 Algoritma MD5

Algortima MD5 merupakan fungsi *hash* satu arah yang diciptakan oleh Ron Rivest. MD5 adalah salah satu aplikasi yang digunakan untuk mengetahui bahwa pesan yang dikirim tidak ada perubahan sewaktu berada di jaringan. Algoritma MD-5 secara garis besar adalah mengambil pesan yang mempunyai panjang variable diubah menjadi intisari pesan yang mempunyai panjang tetap yaitu 128 bit. Inti sari pesan ini tidak dapat dibalik untuk mendapatkan pesan, dengan kata lain tidak ada orang yang dapat meliht pesan dari inti sari MD-5. (Sofwan, 2006:1).

Message Digest 5 (MD5) adalah salah satu penggunaan fungsi hash satu arah yang paling banyak digunakan. MD5 merupakan fungsi hash kelima yang dirancang oleh Ron Rivest. MD5 merupakan pengembangan dari MD-4 dimana terjadi penambahan satu ronde. MD5 memproses teks masukan ke dalam blok-blok bit sebanyak 512 bit, kemudian dibagi ke dalam 32 bit sub blok sebanyak 16 buah. Keluaran dari MD5 berupa 4 buah blok yang masing-masing 32 bit yang mana akan menjadi 128 bit yang biasa disebut nilai hash. (Sunaryo, 2007:3).

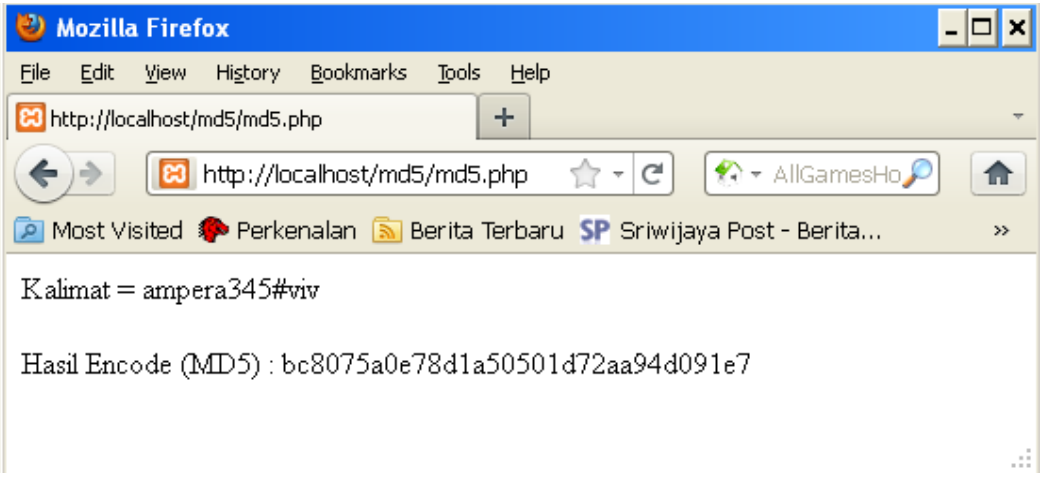
Dari dua pendapat diatas maka *Message Digest 5* (MD5) adalah mengambil pesan yang mempunyai panjang variable diubah menjadi intisari pesan yang mempunyai panjang tetap yaitu 128 bit.

Contoh dari enkripsi database MD5 seperti gambar dibawah ini.

```
<?
$kalimat="ampera345#viv";
echo "Kalimat = $kalimat<br>";
$hasil_encode=MD5($kalimat);
echo "<br> Hasil Encode (MD5) : $hasil_encode";
?>
```

Gambar 2.1 *Enkripsi* Database MD5

Contoh enkripsi dengan md5 pada variabel bila dijalankan pada *browser* seperti dibawah ini.

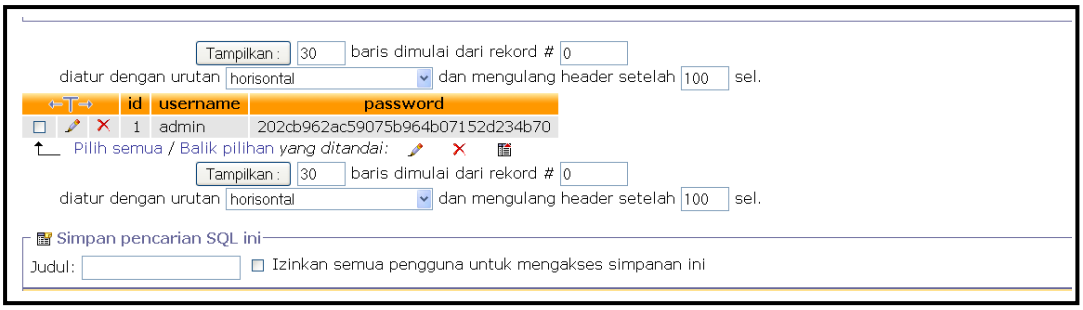


Gambar 2.2 *Enkripsi* Data

Contoh enkripsi dengan MD5 pada database seperti dibawah ini.

Username : admin

Password : 123



Gambar 2.3 *Enkripsi Database*

2.2 Database Management System (DBMS)

Database Management System (*DBMS*) adalah suatu perangkat lunak yang ditujukan untuk menangani penciptaan, pemeliharaan, dan pengendalian akses data. Dengan menggunakan perangkat lunak ini pengelolaan data menjadi mudah lakukan. Salain itu perangkat lunak ini juga menyediakan berbagai peranti yang digunakan. (Kadir, 2008:17).

Database Management System (*DBMS*) adalah sistem pengorganisasian dan pengolahan database pada komputer. Sistem ini dirancang untuk mampu melakukan berbagai data dengan beberapa referensi data yang sama. *DBMS* ini mampu diakses oleh berbagai aplikasi. Terobosan dari *DBMS* adalah *relational database management system (RDBMS)* yang mengorganisasikan data dalam suatu struktur dan memaksimalkan berbagai cara serta menghubungkan antar kumpulan data yang disimpan dalam database. Terobosan berikutnya adalah *distributed relational database management system (DRDBMS)*. Dengan *DRDBMS* memungkinkan informasi berada pada baris data di lokasi, seolah-olah data tersebut berbaris data tunggal dan terpusat. (Febrian,2007:134).

2.2.1 Fungsi DBMS

1. Data *Definition*, DBMS harus dapat mengolah pendefinisian data.
2. Data *Menipulation*, DBMS harus dapat menangani permintaan dari pemakai untuk mengakses data.
3. Data *Security* dan *Integrity*, DBMS harus dapat memeriksa security dan integrity data yang didefinisikan oleh DBA.
4. Data *Recovery* dan *Concurency*, DBMS harus dapat menangani kegagalan-kegagalan pengaksesan database yang dapat disebabkan oleh kesalahan sistem, kerusakan disk.
5. Data *Dictionary*, DBMS harus menyediakan data dictionary.
6. *Performance*, DBMS harus menangani unjuk kerja dari semua fungsi seefisien mungkin.

2.2.2 Keuntungan DBMS

1. Kebebasan data dan akses yang efisien
2. Mereduksi waktu pengembangan aplikasi
3. Integritas dan keamanan data
4. Administrasi keseragaman data
5. Akses bersamaan dan perbaikan dari terjadinya *crashes* (tabrakan dari proses serentak)

Berdasarkan dua pengertian di atas penulis menyimpulkan bahwa *Database Management System* (*DBMS*) adalah suatu perangkat lunak yang ditujukan untuk menangani penciptaan, pemeliharaan, dan pengendalian akses data.

2.3 Antar Muka

Antar muka merupakan salah satu bagian yang terpenting dari sistem. Atar muka sendiri adalah sistem yang dirancang untuk mengolah *input* dan *output* dari data. Seperti contohnya antar muka dibuat untuk pembentukan *output* laporan yang dapat dipreview, diprint, *export/import* (*excel, word, barcode, text* dll). (Febrian, 2007: 10).

Antar muka merupakan informasi dari pengguna (user) dan memberikan informasi kepada pengguna (user) untuk membantu mengarahkan alur penelusuran masalah sampai ditemukan suatu solusi.

Antar muka berfungsi untuk menginput pengetahuan baru ke dalam basis pengetahuan sistem pakar (ES), menampilkan penjelasan sistem dan memberikan panduan pemakaian sistem secara menyeluruh / *step by step* sehingga pengguna mengerti apa yang akan dilakukan terhadap suatu sistem. Yang terpenting adalah kemudahan dalam memakai / menjalankan sistem, interaktif, komunikatif, sedangkan kesulitan dalam mengembangkan / membangun suatu program jangan terlalu diperlihatkan.(Sudarmo, 2006:56).

Berdasarkan dua pengertian di atas penulis menyimpulkan bahwa antar muka merupakan salah satu bagian yang terpenting dari sistem. Antar muka sendiri adalah sistem yang dirancang untuk mengolah *input* dan *output* dari data.

2.4 Crack dan Cracker

Crack adalah suatu program yang dibuat oleh para orang pintar untuk menyiasati program register pada *software* asli. Karena saat anda menginstal program asli yang anda beli selalu diminta nomor register sebagai autentikasi dari pembelian *software* asli. (Febrian, 2007:78).

Crack adalah aplikasi yang digunakan untuk merusak sebagian sistem dari program resmi yang memerlukan lisensi. program resmi butuh lisensi untuk menjalankannya, dengan adanya crack, lisensi itu tidak dibutuhkan lagi. (Sudarmo, 2006:89).

Berdasarkan dua pengertian di atas penulis menyimpulkan bahwa *crack* adalah suatu program yang dibuat oleh para orang pintar untuk menyiasati program register pada *software* asli.

Cracker adalah sebutan untuk mereka yang masuk ke sistem orang lain dan *cracker* lebih bersifat destruktif, biasanya di jaringan komputer, mem-bypass *password* atau lisensi program komputer, secara sengaja melawan keamanan komputer, men-*deface* (merubah halaman muka *web*) milik orang lain bahkan hingga men-*delete* data orang lain, mencuri data dan umumnya melakukan *cracking* untuk keuntungan sendiri, maksud jahat, atau karena sebab lainnya karena ada tantangan. Beberapa proses pembobolan dilakukan untuk menunjukan kelemahan keamanan sistem.. (Febrian, 2007:80).

Cracker adalah sebutan untuk orang yang mencari kelemahan sistem dan memasukinya untuk kepentingan pribadi dan mencari keuntungan dari sistem

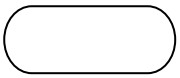
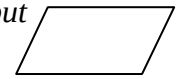
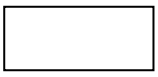
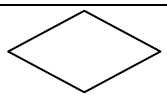
yang dimasuki seperti: pencurian data, penghapusan, dan banyak yang lainnya. Artinya orang itu berusaha untuk sistem komputer orang lain atau menerobos sistem keamanan komputer orang lain untuk mengeruk keuntungan atau melakukan tindak kejahatan. Inilah yang membedakannya dengan *hacker*. (Sudarmo, 2006:83).

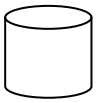
Berdasarkan dua pengertian di atas penulis menyimpulkan bahwa *cracker* adalah sebutan untuk mereka yang masuk ke sistem orang lain dan *cracker* lebih bersifat destruktif, biasanya di jaringan komputer, mem-bypass *password* atau lisensi program komputer.

2.5 Flowchart

Menurut Kristanto (2004:82), *flowchart* berfungsi untuk memodelkan masukan, keluaran, proses maupun transaksi dengan menggunakan simbol-sombol tertentu. Pembuatan *flowchart* harus memudahkan bagi pemakai dalam memahami alur dari sistem atau transaksi.

Tabel 2.1 Simbol *Flowchart*

No.	Simbol	Keterangan
1	*Terminator* 	Termisi yang menandakan awal akhir dari suatu aliran.
2.	*Input / Output* 	Merepresentasikan *Input* data atau *Output* data yang diproses atauInformasi.
3.	*Proses* 	Proses yang dilakukan oleh komputer
4.	*Decision* 	Pengambilan Keputusan

5.	*Magnetic Disk* 	Data penyimpanan (data storage)
6.	*Display* 	Menampilkan data pada monitor

Sumber : Kristanto, Rekayasa Perangkat Lunak, Tahun 2004

2.6 Penelitian Sebelumnya

Pada penelitian ini, penulis melampirkan tiga penelitian sebelumnya yang berhubungan atau menggunakan algoritma *MD5*, adapun penelitian terdahulu tersebut seperti pada tabel di bawah ini.

Aghus Sofwan, 2006. Judul "Aplikasi Kriptografi Dengan Algoritma Message Digest 5 (MD5)". Aplikasi untuk menganalisa proses keutuhan atau pun perubahan pesan dengan menggunakan Message Digest 5 (MD5) dan juga dapat menganalisa hasil keluaran dari MD5. Penelitian ini terfokus pada menganalisa proses keutuhan atau pun perubahan pesan dengan menggunakan *Message Digest* 5 (MD5). MD-5 merupakan fungsi hash satu arah yang diciptakan oleh Ron Rivest. MD-5 adalah salah satu aplikasi yang digunakan untuk mengetahui bahwa pesan yang dikirim tidak ada perubahan sewaktu berada di jaringan.

Akhmad Ratriono Anggoro, 2007. Judul "*Kriptografi Message Digest* Sebagai Salah satu Enkripsi Populer". MD5 mudah sekali untuk diimplementasikan, ke semua bahasa pemrograman untuk merealisasikan algoritma *MD5*, sehingga algoritma ini cocok digunakan dalam bidang *kriptografi*. Pada penelitian ini *MD5* dimanfaatkan sebagai teknik *kriptografi*.

Eka Wahyu Hidayat, 2008. Judul "Aplikasi Kriptografi Sederhana Menggunakan Fungsi *Hashing* (MD5) Pada Modul PHP". Pengujian aplikasi MD5 yang dibuat dengan memasukkan bermacam *input* data sehingga dihasilkan suatu nilai hash. Pengujian aplikasi MD5 dengan *input* data. MD adalah salah satu dari sekian banyak algoritma enkripsi yang menggunakan fungsi *hash* sebagai dasarnya.

BAB III
ANALISIS DAN PERANCANGAN

3.1 Pengumpulan Kebutuhan

Adapun objek yang diteliti adalah membahas pengembangan model antar muka basis data berbasis fungsi MD5. Diharapkan dapat membantu dan memahami algoritma kriptografi MD5 untuk keamanan *database* dan membantu menjaga keamanan *database* yang telah dibuat dan sangat penting tidak dengan mudah dibaca oleh orang yang tidak berhak.

Kebutuhan pengembangan model antar muka basis data berbasis fungsi MD5 yang digunakan meliputi alat atau perangkat keras dalam penelitian ini menggunakan seperangkat komputer PC dengan spesifikasi sebagai berikut :

1. *Processor Intel Centrino (Core 2 Duo 2.00GHz)*
2. *Memory RAM DDR 2,5 Gbyte*
3. *Harddisk 250 GB*
4. *DVD ROM, Monitor, Keyboard, Mouse*

Sedangkan bahan atau perangkat lunak yang diperlukan dalam penelitian ini adalah sebagai berikut :

1. Sistem Operasi menggunakan *Windows XP*

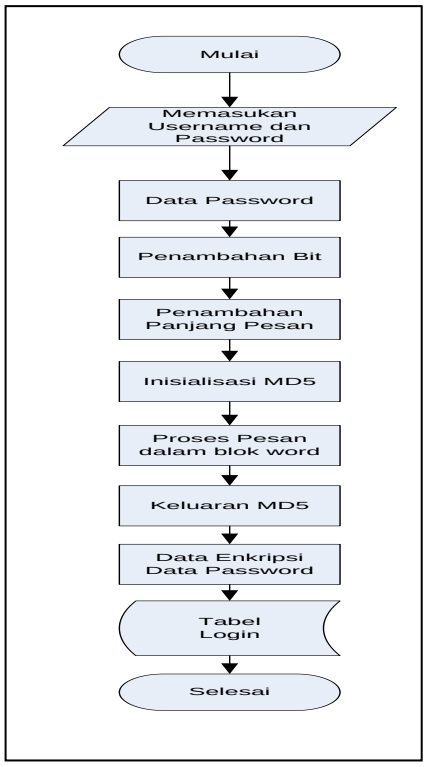
2. Paket *web server AppServ* yang berisi *PHP*
3. *phpMyAdmin*
4. *MySQL*
5. *Dreamweaver 8* sebagai *web editor*
6. *Microsoft Office Word 2007*

3.2 Perancangan Kilat

Perancangan kilat pengembangan model antar muka basis data berbasis fungsi MD5 terdiri dari *flowchart* admin, database dan rancangan antar muka.

3.2.1 Flowchart

Flowchart merupakan kegiatan yang dilakukan oleh admin dalam proses MD5.

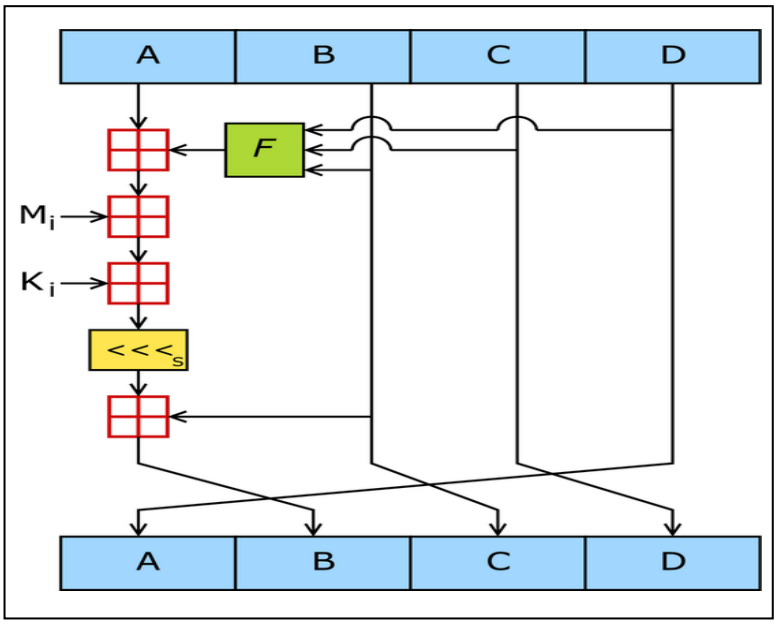


Gambar 3.1 Flowchart Enkripsi

Pegawai memulai aplikasi, pegawai memasukan username dan *password*, pada proses MD5 ini yaitu data *password*, penambahan bit, penambahan panjang pesan, inisialisasi MD5, proses pesan dalam blok *word*, keluaran MD5, data ekripsi data *passwrod* yang disimpan pada tabel login.

3.2.1.1 Algoritma MD5

Algortima MD5 beroperasi pada kondisi 128-bit, dibagi menjadi empat word 32-bit pada A, B, C dan D. Operasi tersebut di inisialisasi dijaga untuk tetap konstan. Algoritma utama kemudian beroperasi pada masingmasing blok pesan 512-bit, masingmasing blok melakukan pengubahan terhadap kondisi pesan. Tahapan pemrosesan blok pesan yaitu batasan putaran dimana tiap putaran membuat 16 operasi serupa berdasar pada fungsi non-linier F, tambahan modular, dan melakukan rotasi ke kiri.



Gambar 3.2 Algoritma MD5

Algoritma MD5 diatas seperti dibawah ini.

```
var int[64] r, k
r[ 0..15] := {7, 12, 17, 22,  7, 12, 17, 22,  7, 12, 17, 22,  7, 12, 17, 22}
r[16..31] := {5,  9, 14, 20,  5,  9, 14, 20,  5,  9, 14, 20,  5,  9, 14, 20}
r[32..47] := {4, 11, 16, 23,  4, 11, 16, 23,  4, 11, 16, 23,  4, 11, 16, 23}
r[48..63] := {6, 10, 15, 21,  6, 10, 15, 21,  6, 10, 15, 21,  6, 10, 15, 21}

for i from 0 to 63
    k[i] := floor(abs(sin(i + 1)) × 2^32)

//Inisialisasi variabel:
var int h0 := 0x67452301
var int h1 := 0xEFCDAB89
var int h2 := 0x98BADCFE
var int h3 := 0x10325476


append "1" bit to message
append "0" bits until message length in bits ≡ 448 (mod 512)
append bit length of message as 64-bit little-endian integer to message

for each 512-bit chunk of message
    break chunk into sixteen 32-bit little-endian words w(i), 0 ≤ i ≤ 15

    var int a := h0
    var int b := h1
    var int c := h2
    var int d := h3

    for i from 0 to 63
        if 0 ≤ i ≤ 15 then
            f := (b and c) or ((not b) and d)
            g := i
        else if 16 ≤ i ≤ 31
            f := (d and b) or ((not d) and c)
            g := (5×i + 1) mod 16
        else if 32 ≤ i ≤ 47
            f := b xor c xor d
            g := (3×i + 5) mod 16
        else if 48 ≤ i ≤ 63
            f := c xor (b or (not d))
            g := (7×i) mod 16
```

```
    temp := d
    d := c
    c := b
    b := ((a + f + k(i) + w(g)) leftrotate r(i)) + b
    a := temp

  h0 := h0 + a
  h1 := h1 + b
  h2 := h2 + c
  h3 := h3 + d
```

var *int* digest := h0 **append** h1 **append** h2 **append** h3

Sedangkan algoritma proses dari data asli ke data ke data enkripsi seperti dibawah ini.

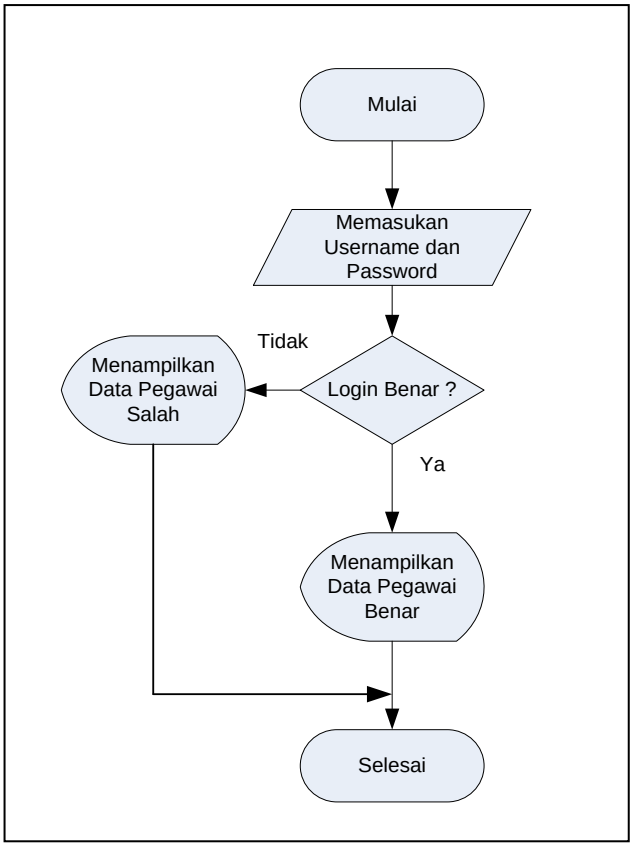
```
{Algoritma Input Login Dengan MD5}

Open Tabel Login
Open Database -> db_pegawai
        Username -> Username
        Passwordmd5 -> MD5(password)
        Insert record username, password from login
        Message = "Input Data Sukses";
Select username, password from login
        HasilMD5 -> password
```

Gambar 3.3 Algoritma *Input Login* dengan MD5

3.2.2 Flowchart Pengalihan Login

Flowchart pengalihan login yaitu mulai aplikasi. Pegawai memasukan username dan password. Jika login benar akan menampilkan data pegawai yang benar dan jika salah login akan menampilkan data pegawai yang salah.



Gambar 3.4 Flowchart Pengalihan Login

Sedangkan algoritma proses pengalihan login seperti dibawah ini.

```
{Algoritma Pengalihan Login }

Open Tabel Login
Open Database -> db_pegawai
        Username -> Username
        Passwordmd5 -> MD5(password)
        Input record username dan password
Search record username dan password form table login
        If username dan password = true
            Go to data pegawai benar
        Else
            Go to data pegawai salah
```

Gambar 3.5 Algoritma Pengalihan *Login*

3.2.3 Basis Data Pengujian

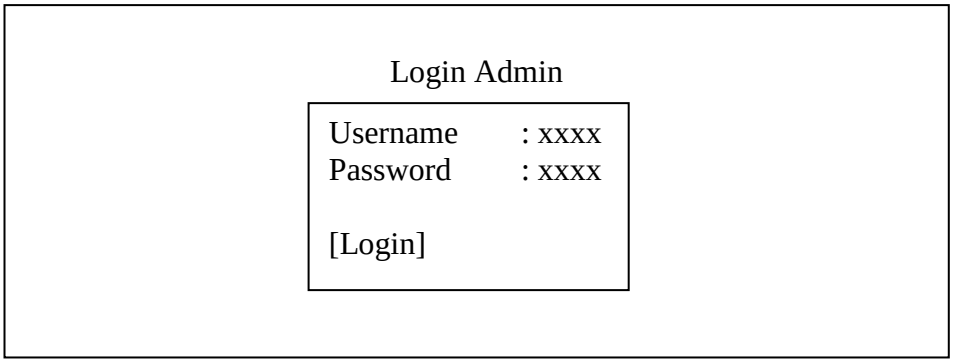
Basis data pengujian merupakan basis data pegawai yang diambil dari Kecamatan Gandu Palembang yang terdiri dari tabel pegawai.

Tabel 3.1 Rancangan Tabel Pegawai

No	Field	Type	Size	Deskripsi
1.	**nip**	Varchar	25	Nomor Induk Pegawai
2.	nama	Varchar	25	Nama Pegawai
3.	jk	Varchar	12	Jenis Kelamin
4.	tgl_lahir	Date	8	Tanggal Lahir
5.	pangkat	Varchar	6	Pangkat
6.	pangkat_tmt	Date	8	Pangkat TMT
7.	golongan	Varchar	6	Golongan
8.	jabatan	Varchar	6	Jabatan
9.	jabatan_tmt	Date	8	Jabatan TMT
10.	mk_th	Varchar	2	Masa Kerja TMT
11.	mk_bl	Varchar	2	.Masa Kerja Tahun
12.	lat_jab	Varchar	25	Latihan Jabatan
13.	lat_th	Varchar	4	Latihan Jabatan Tahun
14.	pendidikan	Varchar	6	Pendidikan
15.	th_lulus	Varchar	4	Tahun Lulus
16.	Alamat	Varchar	50	Alamat
17.	Unit_organisasi	Varchar	50	Unit Organisasi
18.	Password	Varchar	25	Password

3.2.4 Rancangan Antar Muka

1. Rancangan Halaman Login



Gambar 3.6 Rancangan Halaman Login

2. Rancangan Halaman Data Pegawai

Gambar 3.7 Rancangan Halaman Data Pegawai

BAB IV
HASIL DAN PEMBAHASAN

4.1 Hasil

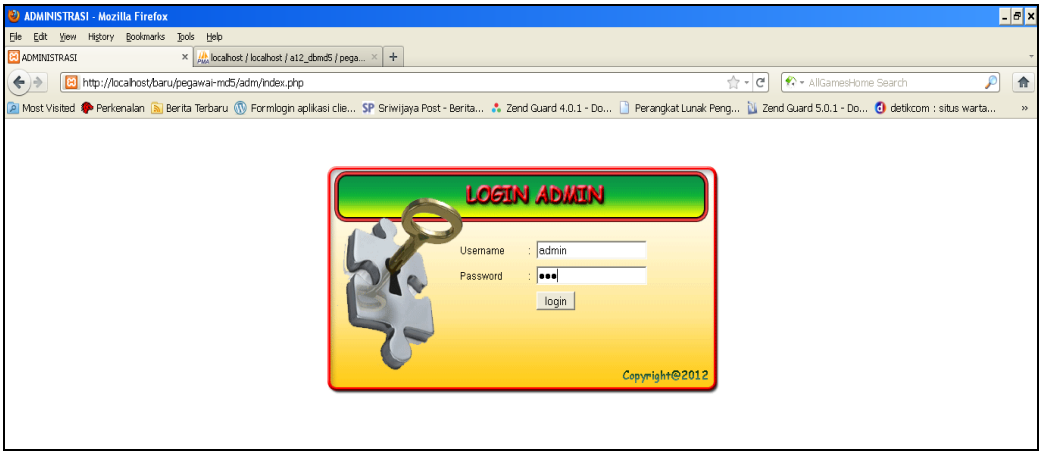
Hasil dari pengembangan model antar muka basis data berbasis fungsi MD5 pada pembahasan bab III yang dibuat skripsi ini adalah tampilan dari masing-masing halaman, bagaimana cara penggunaannya, adapun hasil dari rancangan program ini adalah sebuah pengembangan model antar muka basis data berbasis fungsi MD5. Membantu dan memahami algoritma kriptografi MD5 untuk keamanan *database* dan membantu menjaga keamanan *database* yang telah dibuat dan sangat penting tidak dengan mudah dibaca oleh orang yang tidak berhak.

4.2 Pembahasan

4.2.1 Tampilan Antar Muka

1. Halaman Login

Halaman login merupakan halaman pertama dari model antar muka basis data berbasis fungsi MD5

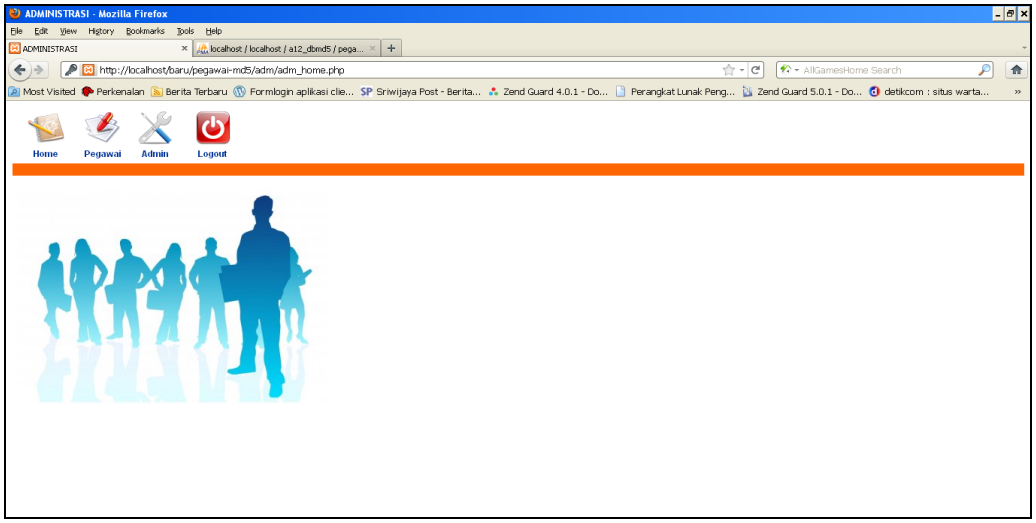


Gambar 4.1 Halaman Login

Halaman login merupakan halaman yang menampilkan username dan password yang akan di isi oleh admin, jika login benar akan menampilkan halaman admin dan jika tidak akan tetap pada halaman login.

2. Halaman Menu Utama

Halaman menu utama merupakan halaman untuk pembaharuan data pegawai dan data admin, tampilannya seperti dibawah ini.



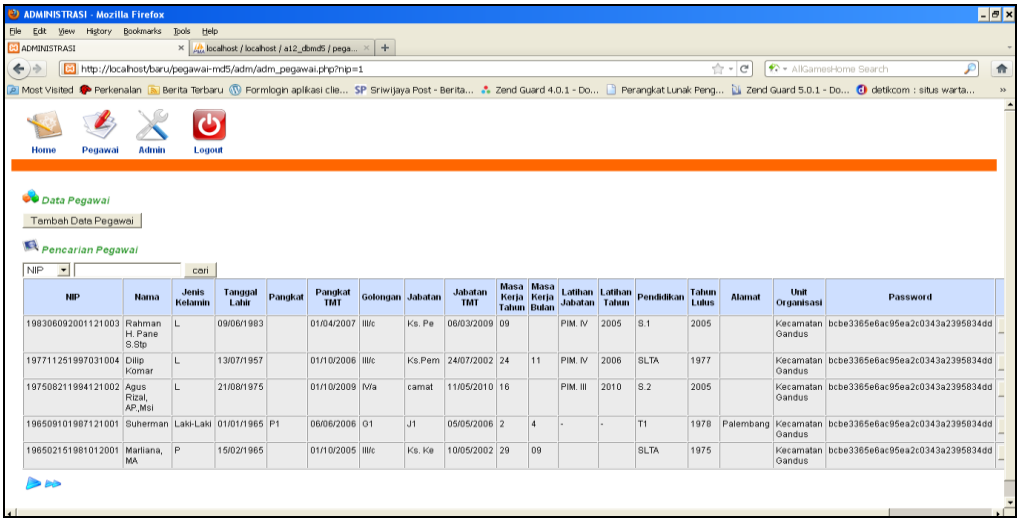
Gambar 4.2 Halaman Menu Utama

Pada halaman menu utama merupakan halaman khusus untuk admin terdapat *link-link* seperti :

1. Link *home* merupakan halaman pertama ketika halaman admin ditampilkan.
2. Link pegawai merupakan halaman yang menampilkan data pegawai
3. Link admin merupakan halaman yang menampilkan data admin
4. Link *logout* merupakan fasilitas untuk keluar dari halaman admin.

3. Halaman Data Pegawai

Halaman data pegawai merupakan halaman untuk pembaharuan data pegawai, tampilannya seperti dibawah ini.



Gambar 4.3 Halaman Data Pegawai

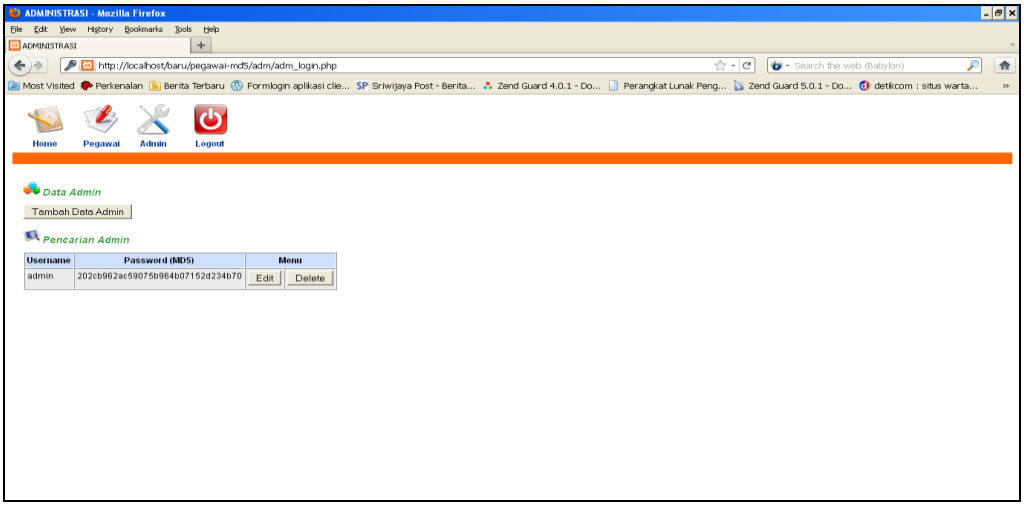
Halaman pegawai merupakan halaman yang menampilkan data pegawai, pada halaman ini terdapat fasilitas-fasilitas seperti.

1. Tombol tambah data untuk menampilkan halaman menambah data pegawai.

2. Tombol cari untuk memproses pencarian data pegawai, jika data ada maka akan tampil pada tabel pegawai dan jika tidak tabel akan kosong.
3. Tombol *edit* merupakan proses untuk memperbaharui data pegawai.
4. Tombol *delete* merupakan proses untuk menghapus data pegawai.

4. Halaman Data Admin

Halaman data admin merupakan halaman untuk pembaharuan data admin, tampilannya seperti dibawah ini.



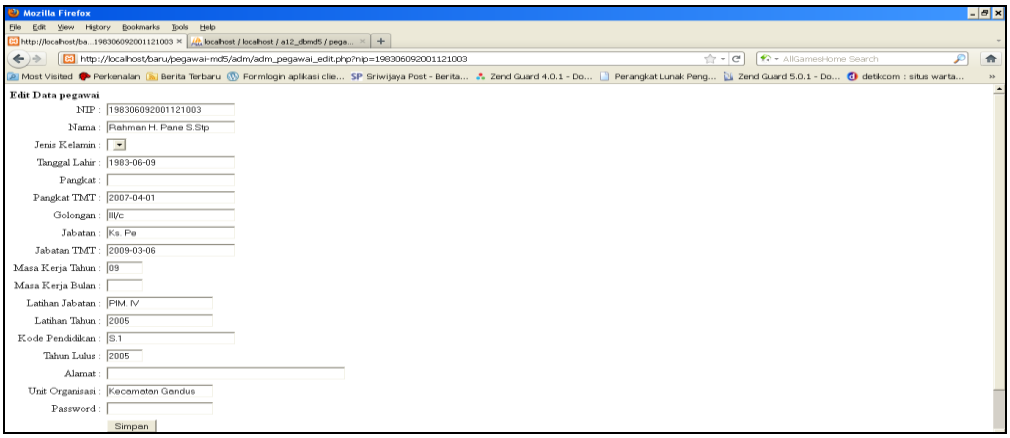
Gambar 4.4 Halaman Data Admin

Halaman admin merupakan halaman yang menampilkan data admin, pada halaman ini terdapat fasilitas-fasilitas seperti.

1. Tombol tambah data untuk menampilkan halaman menambah data admin.
2. Tombol cari untuk memproses pencarian data admin, jika data ada maka akan tampil pada tabel admin dan jika tidak tabel akan kosong.
3. Tombol *edit* merupakan proses untuk memperbaharui data admin
4. Tombol *delete* merupakan proses untuk menghapus data admin

4.2.2 Enkripsi *Password* Data Pegawai

Enkripsi *password* pegawai, dengan cara memasukan data pegawai seperti tabel dibawah ini.



Gambar 4.5 Halaman *Input* Data Pegawai

Halaman ekripsi password data pegawai merupakan halaman yang berfungsi untuk memasukan data pegawai dan pada password akan di ekripsi dengan algoritma MD5.

Script PHP MD5 untuk data pegawai seperti dibawah ini.

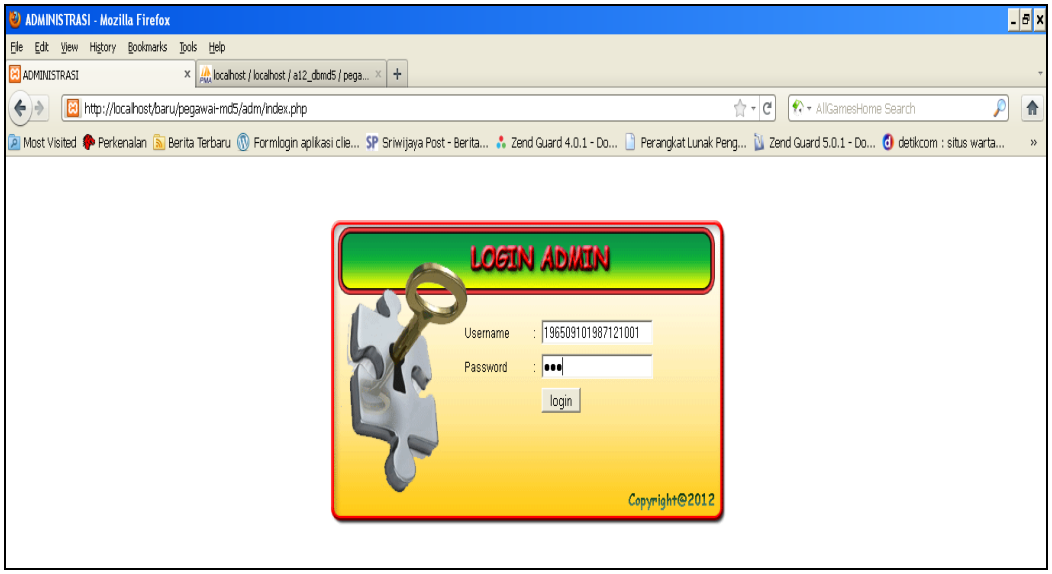
```
$insertSQL = sprintf("INSERT INTO pegawai (nip, nama, jk, tgl_lahir, pangkat, pangkat_tmt, golongan, jabatan,
jabatan_tmt, mk_th, mk_bln, lat_jab, lat_th, pendidikan, th_lulus, alamat, unit_organisasi, password) VALUES (%s, %s,
%s, %s, %s, %s, %s, %s, %s, %s, %s, %s, %s, %s, %s, %s, %s, %s)",
                GetSQLValueString($_POST['nip'], "text"),
                                        GetSQLValueString($_POST['nama'], "text"),
                                        GetSQLValueString($_POST['jk'], "text"),
                                        GetSQLValueString($tanggal, "text"),
                                        GetSQLValueString($_POST['pangkat'], "text"),
                                        GetSQLValueString($pangkat_tmt, "text"),
                                        GetSQLValueString($_POST['golongan'], "text"),
                                        GetSQLValueString($_POST['jabatan'], "text"),
                                        GetSQLValueString($jabatan_tmt, "text"),
                                        GetSQLValueString($_POST['mk_th'], "text"),
                                        GetSQLValueString($_POST['mk_bln'], "text"),
                                        GetSQLValueString($_POST['lat_jab'], "text"),
                                        GetSQLValueString($_POST['lat_th'], "text"),
                                        GetSQLValueString($_POST['pendidikan'], "text"),
                                        GetSQLValueString($_POST['th_lulus'], "text"),
                                        GetSQLValueString($_POST['alamat'], "text"),
                                        GetSQLValueString($_POST['unit_organisasi'], "text"),
                GetSQLValueString(md5($_POST['password']), "text"));
```

Gambar 4.6 *Script PHP* MD5

Pada scripting PHP diatas menjelaskan tentang penyimpanan data dengan *script* (*insert*) dan proses enkripsi data *password* pada tabel pegawai dengan *script* *md5($_POST['password']).*

4.2.3 Login Pengalihan Data

Login pengalihan data pada model antar muka basis data berbasis fungsi MD5, tampilannya seperti dibawah ini.



Gambar 4.7 Halaman Login Pengalihan

Pada halaman login pengalihan ini terdapat script PHP login yang dibangun untuk pengalihan hasil login, jika login benar akan menampilkan data pegawai sebenarnya dan jika login salah akan menampilkan data pegawai yang salah.

Script PHP login pengalihan seperti dibawah ini.

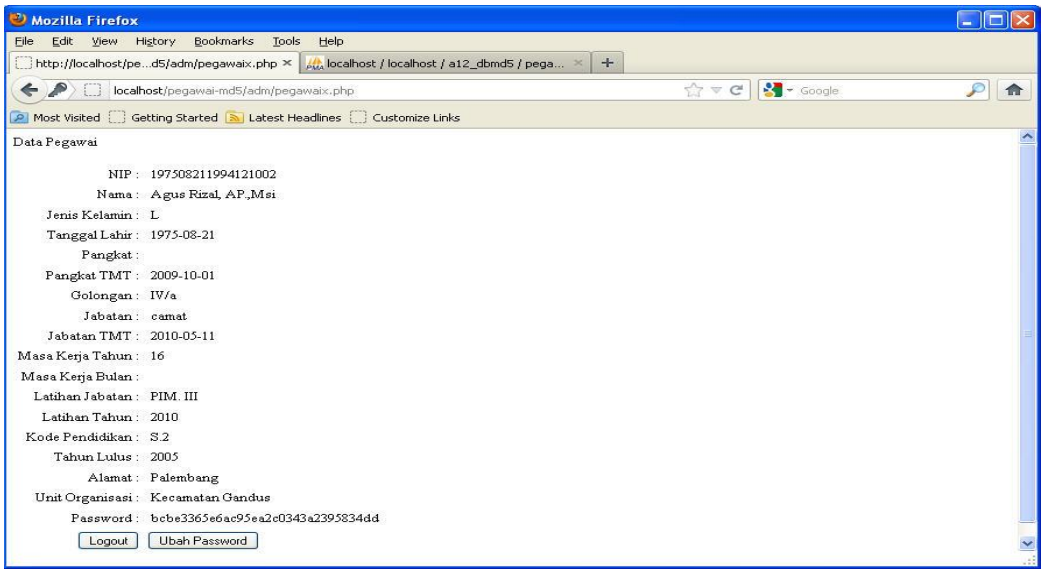
```
$query_rslogin2 = sprintf("SELECT * FROM pegawai WHERE nip = '$username' and
password = '$password'", $colname_rslogin,$colpass_rslogin);
$rslogin2 = mysql_query($query_rslogin2, $conn) or die(mysql_error());
$row_rslogin2 = mysql_fetch_assoc($rslogin2);
$totalRows_rslogin2 = mysql_num_rows($rslogin2);

if ($totalRows_rslogin2>0) {
        session_start();
        $_SESSION['username'] = $row_rslogin2['nip'];
        $_SESSION['userfullname'] = $row_rslogin2['nama'];
        $_SESSION['level'] = 'pegawai';
        header("location:pegawaix.php"); //login benar
}else{
        header("location:pegawai.php?username=$username"); //login salah
}
```

Gambar 4.8 *Script PHP Login*

Pada *script* PHP diatas menjelaskan tentang pengecekan data pegawai dengan *script* php (*SELECT * FROM pegawai WHERE nip = '$username' and password = '$password'*), jika data ada maka akan menampilkan *file* pegawaix.php dan jika salah akan menampilkan *file* pegawai.php.

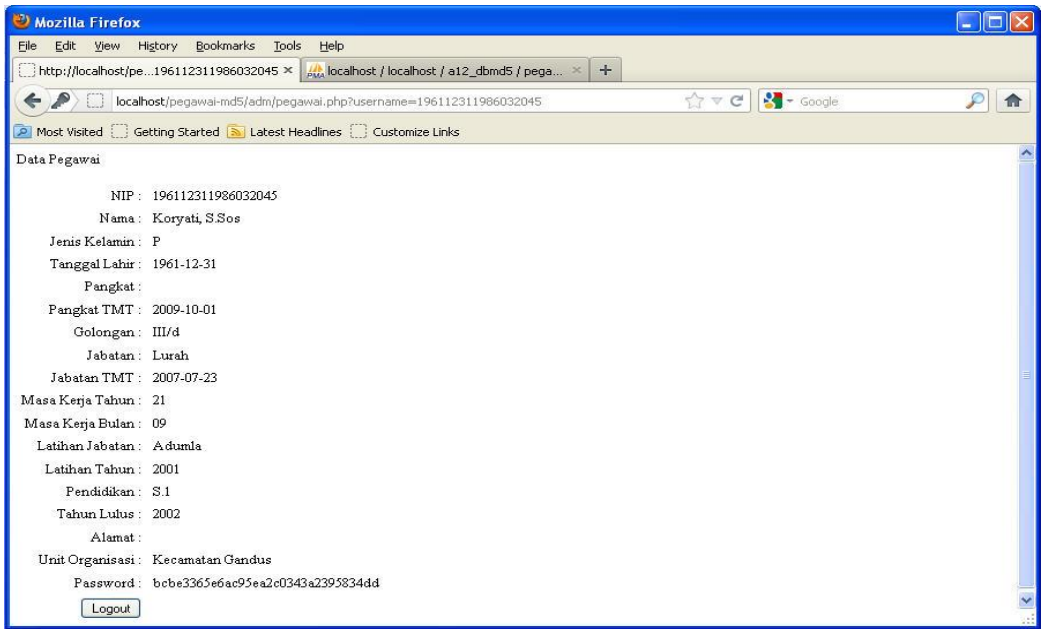
Tampilan login data pegawai yang benar, seperti dibawah ini.



Gambar 4.9 Halaman Login Pegawai Benar

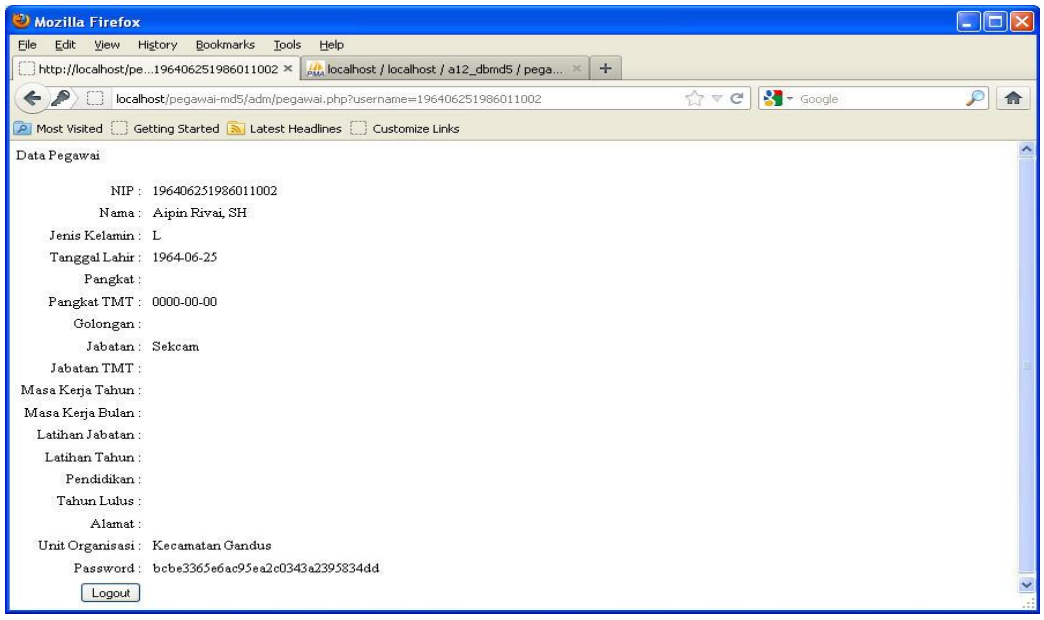
Tampilan login data pegawai yang salah, seperti dibawah ini.

1. Pengujian login Pertama yang salah



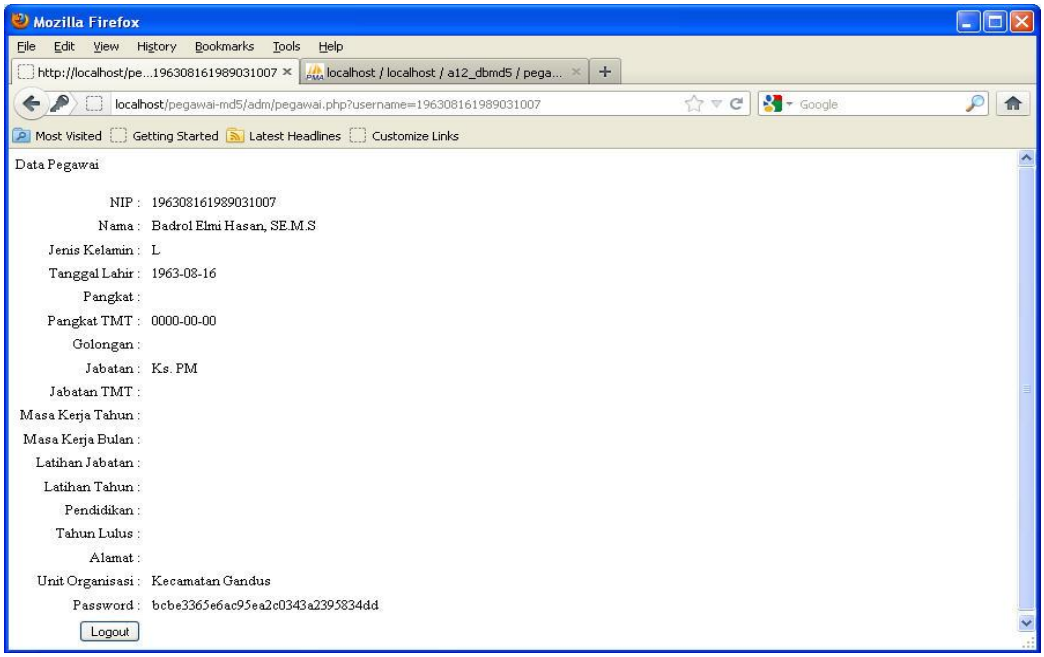
Gambar 4.10 Pengujian login Pertama yang salah

2. Pengujian login kedua yang salah



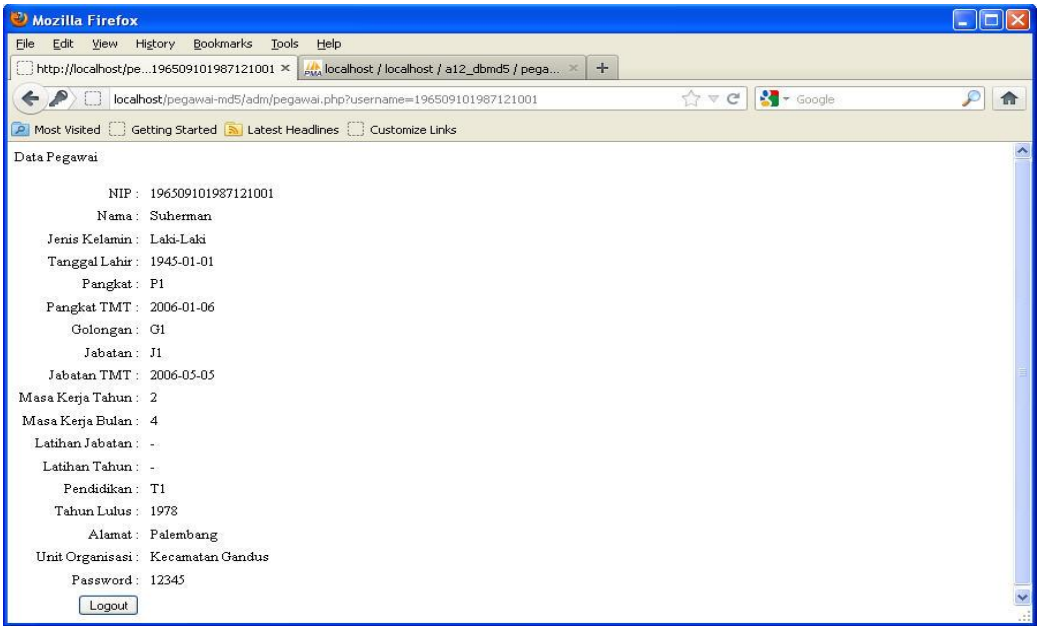
Gambar 4.11 Pengujian login kedua yang salah

3. Pengujian login ketiga yang salah



Gambar 4.12 Pengujian login ketiga yang salah

4. Pengujian login keempat yang salah



Gambar 4.13 Pengujian login keempat yang salah

BAB V
KESIMPULAN DAN SARAN

5.1 Kesimpulan

Berdasarkan dari penelitian yang telah dilaksanakan dan sudah diuraikan dalam pengembangan model antar muka basis data berbasis fungsi MD5, maka penulis dapat menarik kesimpulan sebagai berikut :

1. Penelitian ini menghasilkan pengembangan model antar muka basis data berbasis fungsi MD5.
2. Membantu dan memahami algoritma kriptografi MD5 untuk keamanan *database*, membantu menjaga keamanan *database* yang telah dibuat dan sangat penting tidak dengan mudah dibaca oleh orang yang tidak berhak.
3. Pengembangan model antar muka basis data berbasis fungsi MD5 dibangun menggunakan bahasa *scripting PHP* dan database *MySQL*.

5.2 Saran

Saran dari model antar muka basis data berbasis fungsi MD5yaitu:

1. Diharapkan model antar muka basis data berbasis fungsi MD5 ini dapat dimanfaatkan oleh masyarakat secara optimal.
2. Seiring dengan kemajuan ilmu pengetahuan dan teknologi, maka tidak menutup kemungkinan model antar muka basis data berbasis fungsi MD5 dapat dibangun nantinya dapat dikembangkan lagi.

DAFTAR PUSTAKA

Anggoro, 2007. *Kriptografi Message Digest Sebagai Salah Satu Enkripsi Populer*. Institut Teknologi Bandung.

Hidayat, 2008. *Aplikasi Kriptografi Sederhana Menggunakan Fungsi Hashing (MD5) Pada Modul PHP*, Universitas Siliwangi Tasikmalaya.

Febrian, 2007. *Kamus Komputer & Teknologi Informasi*, Informatika, Bandung

Kadir, A, 2008. *Rekayasa Perangkat lunak*. ANDI, Yogyakarta.

Kristanto, A, 2004. *Rekayasa Perangkat Lunak.* Gava Media, Yogyakarta.

Presman, RS, 2002, *Perangkat lunak* Edisi Terjemah. ANDI, Yogyakarta.

Sofwan, 2006. *Aplikasi Kriptografi Dengan Algoritma Message Digest 5 (Md5)*, Universitas Diponegoro.

Sudarmo, P, 2006. *Kamus Istilah Komputer, Teknologi Informasi & Komunikasi.* Yrama Widya, Bandung.

Sunaryo, 2007. *Enkripsi data hasil analisis komponen utama (pca) atas citra iris mata menggunakan Algoritma MD5,* Universitas Dipenogoro Semarang.