PENGEMBANGAN MODEL ANTAR MUKA BASIS DATA BERBASIS FUNGSI MESSAGE DIGEST 5 (MD5)

Muhammad Darul Muslim[1], Syahril Rizal[2] , Suyanto[3]
Dosen Universitas Bina Darma[1], Mahasiswa Universitas Bina Darma[2]
Jalan Jenderal Ahmad Yani No.12 Palembang
darul_1989@yahoo.com[1], syahril_rizal@mail.bidadarma.ac.id[2], suyanto@mail.bidadarma.ac.id[3]

ABSTRAK

*Permasalahan dalam penggunaan MD5 adalah hasil MD5 tidak bisa dikembalikan lagi seperti asalnya, sehingga jika diterapkan pada pembuatan password dalam basis data, 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 situs web 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 ganda MD5 atau lebih dan juga bisa disisipkan kunci pada hasil MD5 tersebut dalam basis data. 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

1. 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*. 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*).

1.2. Tujuan

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

1.3. 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.

2. METODOLOGI PENELITIAN

2.1 Analisis Kebutuhan

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

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*

2.2 Perancangan

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 basis data dan membantu menjaga keamanan basis data yang telah dibuat dan sangat penting tidak dengan mudah dibaca oleh orang yang tidak berhak. Perancangan pengembangan model antar muka basis data berbasis fungsi MD5 terdiri dari *flowchart* admin, database dan rancangan antar muka.

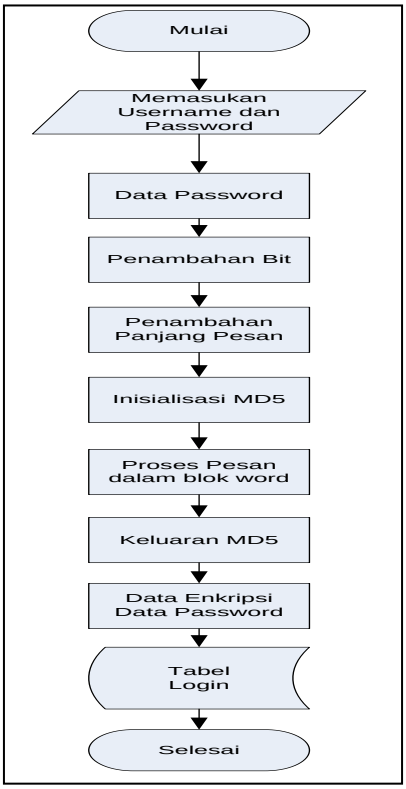
Perancangan berfokus pada penyajian dari aspek-aspek perangkat lunak tersebut yang akan nampak bagi pelanggan/pemakai, perancangan kilta membawa kepada kontruksi sebuah prototipe.

2.2.1 Flowchat

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.

Flowchart merupakan kegiatan yang dilakukan oleh admin dalam proses MD5. Proses tersebut seperti gambar di bawah ini.



Gambar 2.1 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.

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

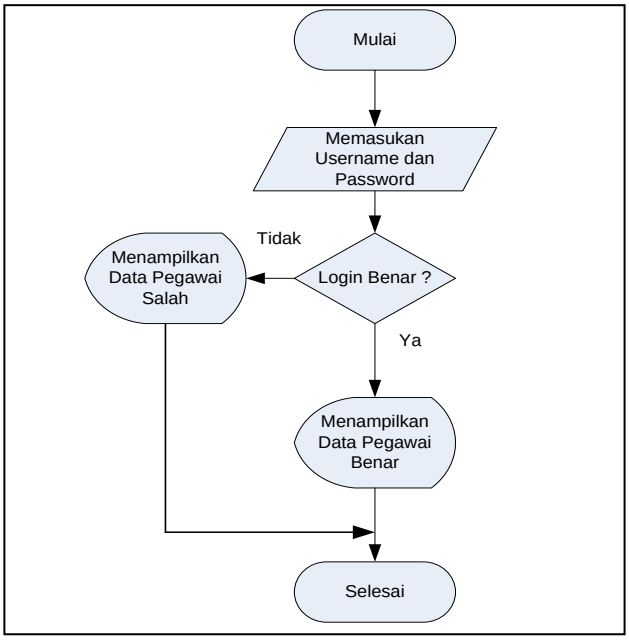
```
{Algoritma Input Login Dengan MD5}

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 2.2 Flowchart Enkripsi

2.2.2 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 2.3 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
```

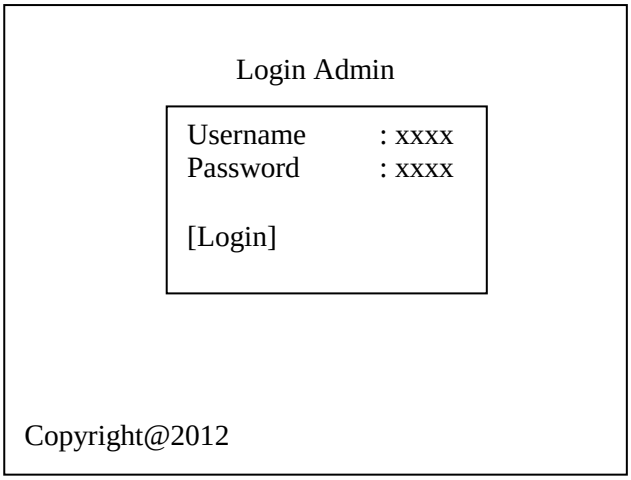
Gambar 2.4 Flowchart Enkripsi

2.2.3 Antar Muka

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

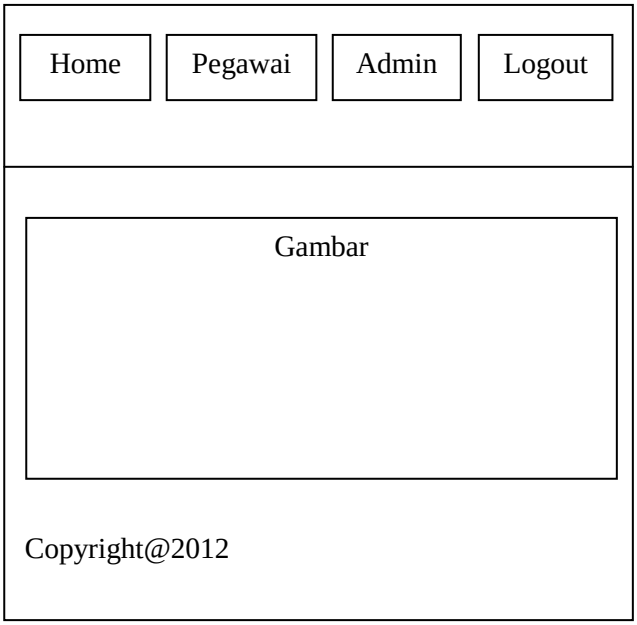
Antar muka berfungsi untuk menginput pengetahuan baru ke dalam basis pengetahuan sistem pakar (ES), menampilkan penjelasan sistem dan memberikan panduan pemakaian sistem secara menyeluruh / *step by step* sehingga pengguna mengerti apa yang akan dilakukan terhadap suatu sistem. Yang terpenting adalah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

1. Rancangan Halaman Login



Gambar 2.5 Rancangan Halaman Login

2. Rancangan Halaman Home Admin



Gambar 2.6 Rancangan Halaman Admin

3. Rancangan Halaman Input Pegawai

HEADER

Pegawai

NIP	: xxxxxxxx
Nama	: xxxxxxxxxxxx
Jenis Kelamin	: xxxxxxxxxxxx
Tanggal Lahir	: dd/mm/yyyy
Kode Pangkat	: xxxxxxxxxxxx
Pangkat TMT	: dd/mm/yyyy
Kode Golongan	: xxxxxxxxxxxx
Kode Jabatan	: xxxxxxxxxxxx
Jabatan TMT	: dd/mm/yyyy
Masa Kerja Tahun	: xxxxxxxxxxxx
Masa Kerja Bulan	: xxxxxxxxxxxx
Latihan Jabatan	: xxxxxxxxxxxx
Latihan Tahun	: xxxxxxxxxxxx
Kode Pendidikan	: xxxxxxxxxxxx
Tahun Lulus	: xxxxxxxxxxxx
Alamat	: xxxxxxxxxxxx
Unit Organisasi	: xxxxxxxxxxxx
Password	: xxxxxxxxxxxx

[Simpan]

Copyright@2012

Gambar 2.7 Rancangan Halaman Input Pegawai

4. Rancangan Halaman Input Daftar Admin

HEADER

Input Admin

Id Admin	: (auto)
Nama	: xxxxxxxxxxxxxxxxxx
Username	: xxxxxxxxxxxxxxxxxx
Password	: xxxxxxxxxxxxxxxxxx

[Simpan]

Copyright@2012

Gambar 2.8 Halaman Input Daftar Admin

5. Rancangan Halaman Daftar Admin

HEADER

Daftar Admin

[Input Admin]

Id admin	Nama	User name	Passwrod		
99	xxxxx	xxxxx	xxxxxx	[Edit]	[Delete]
99	xxxxx	xxxxx	xxxxxx	[Edit]	[Delete]
99	xxxxx	xxxxx	xxxxxx	[Edit]	[Delete]

[Kembali]

Gambar 2.9 Rancangan Halaman Daftar

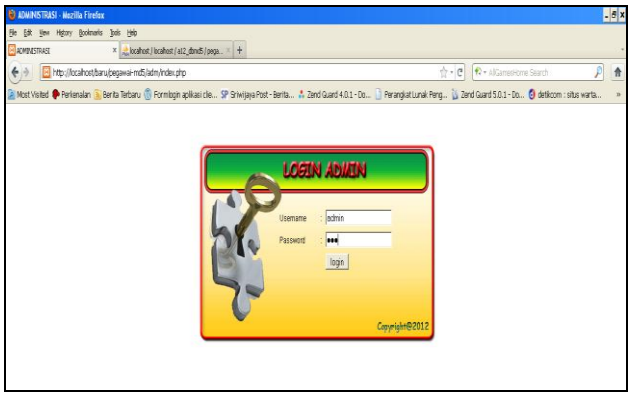
3. HASIL

Hasil dari pengembangan model antar muka basis data berbasis fungsi MD5 pada pembahasan yang dibuat dalam 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 basis data dan membantu menjaga keamanan basis data yang telah dibuat dan sangat penting tidak dengan mudah dibaca oleh orang yang tidak berhak.

3.1. Tampilan Antar Muka

1. Halaman Login

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

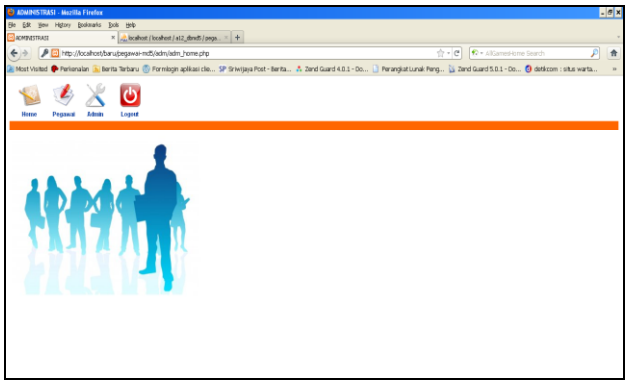


Gambar 3.1 Halaman Login

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.



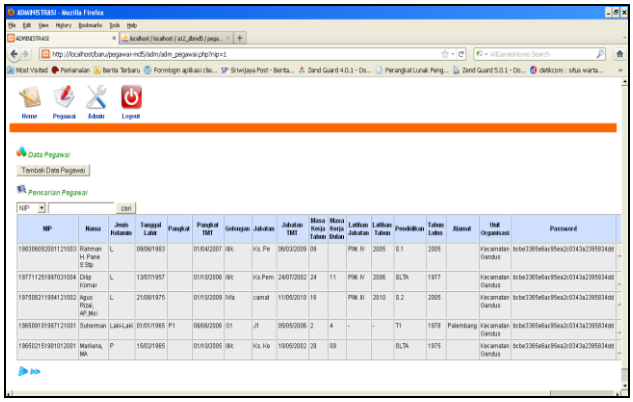
Gambar 3.2 Halaman Menu Utama

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.



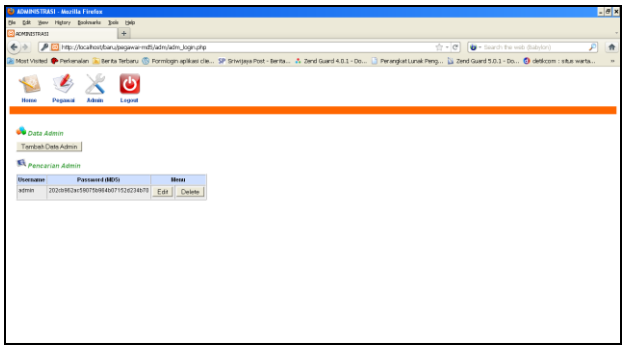
Gambar 3.3 Halaman Data Pegawai

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.



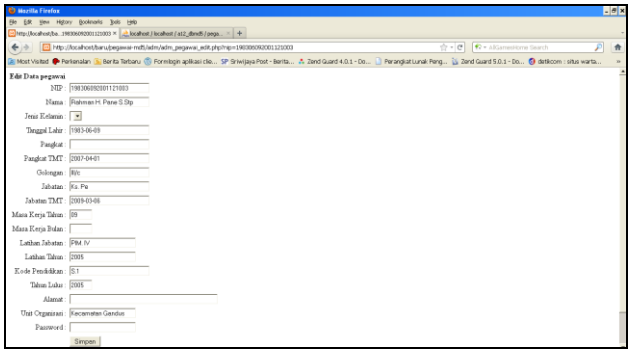
Gambar 3.4 Halaman Data Admin

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.

5.Enkripsi Password Data Pegawai

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

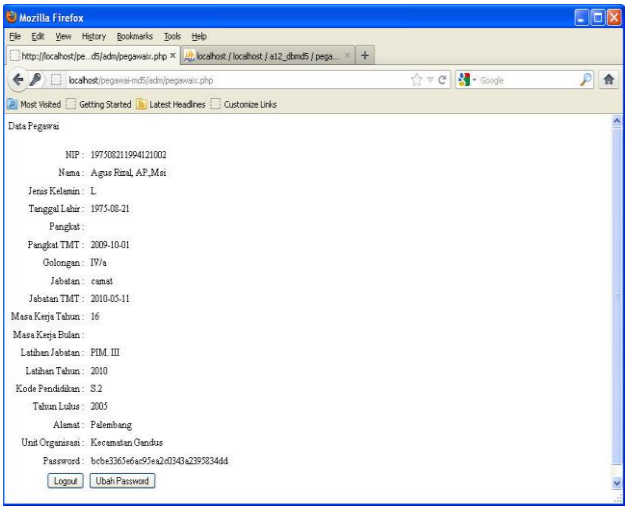


Gambar 3.5 Halaman *Input* Data Pegawai

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

6. Login Data Pegawai Benar

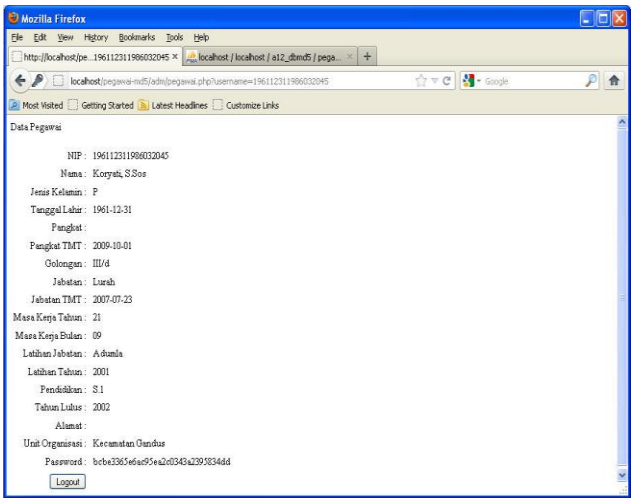
Tampilan pengujian login data pegawai yang benar, seperti dibawah ini.



Gambar 3.6 Halaman Login Pegawai Benar

7. Login Data Pegawai Salah

Tampilan pengujian login data pegawai yang salah, seperti dibawah ini.



Gambar 3.7 Pengujian login yang salah

4. SIMPULAN

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

DAFTAR RUJUKAN

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.