

**Bisnis Rental Mobil Melalui Internet (E-Commerce)
Menggunakan Algoritma Sha-1 (Secure Hash Algorithm-1)
Dahlan Abdullah¹, Cut Ita Erliana²**

¹Program Studi Teknik Informatika,²Jurusan Teknik Industri
Fakultas Teknik, Universitas Malikussaleh
Reuleut, Aceh Utara, Aceh-Indonesia
dahlan.unimal@gmail.com, cutitha@gmail.com

ABSTRAK: Pada penulisan ini penulis mencoba membuat sebuah Aplikasi Rental Mobil dengan menggunakan Algoritma SHA-1 (*Secure Hash Algorithm-1*), yang akan di implementasikan pada sistem *login*. Tujuan dari pembuatan aplikasi ini yaitu untuk membantu perusahaan atau usaha rental mobil dalam mempromosikan jasanya yang dapat diakses secara online sehingga memberikan pelayanan yang maksimal untuk masyarakat atau pelanggan. Proses rental mobil dimulai dengan pencarian informasi tentang mobil, daftar *user*/pelanggan, proses transaksi dan pembuatan kuitansi pembayaran. Penyimpanan data dilakukan pada database dengan klasifikasi masing-masing penyimpanan. PHP merupakan bahasa pemrograman yang digunakan dalam pembuatan Aplikasi Rental Mobil ini.

Kata kunci : Aplikasi, Login, Rental, Secure Hash Algorithm-1.

1.1. Latar belakang

Perkembangan teknologi informasi saat ini telah berpengaruh pada hampir semua aspek kehidupan manusia. Sekarang ini internet tidak menghiraukan batas-batas geografis suatu negara, bukan hal yang sulit bagi seseorang untuk berkomunikasi jarak jauh, mengirimkan data, mencari informasi dan sebagainya. Semua hal tersebut dapat dilakukan dengan internet secara cepat, efisien dan relatif murah. Namun di sisi lain, ternyata internet merupakan jalur yang tidak terlalu aman karena merupakan media komunikasi umum yang dapat digunakan secara bebas oleh siapapun sehingga sangat rawan penyadapan informasi oleh pihak-pihak yang tidak bertanggung jawab. Oleh karena itu masalah keamanan, kenyamanan dan otorisasi dalam berinternet menjadi masalah krusial yang sampai hari ini masih menjadi perbincangan hangat. Banyak pertanyaan yang muncul, Apakah transaksi via internet bisa terjamin keamanannya? Apakah data yang dikirimkan via internet sampai pada tujuan yang tepat tanpa diketahui pihak yang tidak diinginkan? Bagaimana mencegah penyadapan informasi? Bagaimana mengantisipasi seseorang mencuri data? Banyak metode yang dapat dilakukan untuk menjawab pertanyaan-pertanyaan diatas. Salah satunya dengan metode penyandian atau yang lebih dikenal dengan metode kriptografi. Banyak sekali metode penyandian atau metode kriptografi yang dikembangkan oleh pakar-pakar kriptografi hingga saat ini. Hal ini dilakukan dikarenakan penyadap dan pencuri informasi atau yang lebih dikenal dengan sebutan *cracker* semakin handal dalam mempenetrasi suatu sistem untuk menggali berbagai macam informasi. Oleh karena itu dalam rangka melawan tindakan keji tersebut, pakar-pakar kriptografi

terus mengembangkan metode ini secara berkesinambungan. Banyak sekali metode penyandian yang telah diciptakan oleh pakar-pakar kriptografi dunia, sebut saja Algoritma DES, Algoritma 3DES, Algoritma IDEA, Algoritma Blowfish, Algoritma RSA, Algoritma MD4, Algoritma MD5, Algoritma SHA-1, Algoritma McEliece dan sebagainya. Algoritma-algoritma diatas telah diuji kemampuannya oleh pakar-pakar kriptografi, namun tidak semua metode kriptografi diatas bertahan dari serangan para penyadap informasi atau dalam istilah kriptografi sering disebut dengan cryptanalist. Sebut saja algoritma DES, sempat bertahan cukup lama yakni selama 20 tahun akhirnya harus rela di-*crack* hanya dalam tempo 3,5 jam dengan biaya 1 juta US Dollar pada tahun 1993. Namun para pakar kriptografi tidak berdiam diri, karena setelah kejadian itu para pakar kriptografi mengembangkan varian baru dari algoritma DES seperti Algoritma 3DES, Algoritma RDES dan sebagainya.

2.1. Aplikasi

Aplikasi adalah suatu subkelas perangkat lunak komputer yang memanfaatkan kemampuan komputer langsung untuk melakukan suatu tugas yang diinginkan pengguna. Contoh utama aplikasi adalah pengolah kata, lembar kerja, memanipulasi foto, merancang rumah dan pemutar media. Beberapa aplikasi yang digabung bersama menjadi suatu pake disebut sebagai suatu paket atau suite aplikasi (*application suite*). Contohnya adalah Microsoft Office dan OpenOffice.org, yang menggabungkan suatu aplikasi pengolah kata, lembar kerja dan beberapa aplikasi lainnya. Aplikasi-aplikasi dalam suatu paket biasanya memiliki atarmuka pengguna yang memiliki kesamaan sehingga

memudahkan pengguna untuk mempelajari dan menggunakan tiap aplikasi. Sering kali, mereka memiliki kemampuan untuk saling berinteraksi satu sama lain sehingga menguntungkan pengguna. Contohnya, suatu lembar kerja dapat dibenamkan dalam suatu dokumen pengolah kata walaupun dibuat pada aplikasi lembar kerja yang terpisah.

Jenis-jenis *Software* Aplikasi :

1. *Software* aplikasi hiburan, contohnya yaitu winamp untuk mendengarkan musik, games dan sebagainya untuk hiburan.
2. *Software* aplikasi pendidikan yaitu *software* digunakan untuk mempelajari atau mereferensikan tentang pendidikan atau pengetahuan.
3. *Software* aplikasi bisnis yaitu *software* yang digunakan untuk aplikasi bisnis
4. *Software* aplikasi khusus
5. *Software* aplikasi untuk produktivitas kerja.

2.2. Rental Mobil

Rental mobil merupakan usaha yang menawarkan jasa penyewaan mobil kepada pihak yang membutuhkan, baik perorangan maupun perusahaan. Penyewa tidak bertanggung jawab terhadap maintenance mobil, namun pemilik rental mobil sangat penting menjaga kondisi mobil karena kunci sukses rental mobil adalah menjaga biaya-biaya perawatan mobil untuk selalu lebih rendah. Selain dianggap lebih praktis, untuk mendapatkan mobil sewaan ini memang tergolong mudah, asalkan konsumen dapat memenuhi beberapa persyaratan yang ditentukan perusahaan atau pihak penyewa mobil. Keuntungan lain, masyarakat tidak perlu repot-repot untuk membeli mobil.

Komponen-komponen yang dipersiapkan untuk membuka usaha rental mobil adalah :

1. Prasarana dan sarana, seperti:
 - a. Tempat atau lokasi yang strategis
 - b. Tenaga ahli yang cukup berpengalaman di bisnis rental mobil
 - c. Modal usaha yang cukup
 - d. Perijinan
2. Perencanaan dan Pengendalian Keuangan
 - a. Proyeksi arus kas (jangan lupa masukkan biaya cadangan penyusutan kendaraan)
 - b. Melakukan administrasi dan pembukuan yang teratur, seperti catatan data-data pelanggan, catatan barang inventaris kantor, catatan keluar masuknya uang/hari (buku kas harian) dan lain-lain
 - c. Catatan laba rugi/ bulanan
3. Perencanaan Strategi Pemasaran

- a. Penetapan harga sewa mobil dan cara pembayaran
 - b. Penentuan target market, masyarakat dari kelas ekonomi apakah yang menjadi sasaran anda
 - c. Variasi jasa yang ditawarkan untuk member nilai lebih pada rental mobil anda
 - d. Promosi untuk menarik perhatian konsumen.
4. Administrasi yang bagus dan legalitas dari kontrak perjanjian sewa kendaraan
 5. Atasi kerugian kendaraan dengan asuransi mobil

2.3. Kriptography

Kriptography (*Cryptography*) berasal dari bahasa Yunani yaitu dari kata *Crypto* dan *Graphia* yang berarti penulisan rahasia. Kriptography adalah suatu ilmu yang mempelajari penulisan secara rahasia, yang mana pengertian kriptography menurut (Schneier, 1996) adalah ilmu sekaligus seni untuk menjaga keamanan pesan (*message*) Kriptography merupakan bagian dari suatu cabang ilmu matematika yang disebut *Cryptology*. Kriptography bertujuan menjaga kerahasiaan informasi yang terkandung dalam data sehingga informasi tersebut tidak dapat diketahui oleh pihak yang tidak sah. Dalam menjaga kerahasiaan data, kriptography mentransformasikan data jelas (*plaintext*) ke dalam bentuk data sandi (*ciphertext*) yang tidak dapat dikenali. *Ciphertext* inilah yang kemudian dikirimkan oleh pengirim (*sender*) kepada penerima (*receiver*). Setelah sampai di penerima, *ciphertext* tersebut ditransformasikan kembali ke dalam bentuk *plaintext* agar dapat dikenali.

Proses tranformasi dari *plaintext* menjadi *ciphertext* disebut proses *Encipherment* atau enkripsi (*encryption*), sedangkan proses mentransformasikan kembali *ciphertext* menjadi *plaintext* disebut proses dekripsi (*decryption*). Untuk mengenkripsi dan mendekripsi data. Kriptography menggunakan suatu algoritma (*cipher*) dan kunci (*key*). *Cipher* adalah fungsi matematika yang digunakan untuk mengenkripsi dan mendekripsi data . Sedangkan kunci merupakan sederetan bit yang diperlukan untuk mengenkripsi dan mendekripsi data. Algoritma kriptography modern tidak lagi mengandalkan keamanannya pada kerahasiaan algoritma tetapi kerahasiaan kunci. *Plaintext* yang sama bila disandikan dengan kunci yang berbeda akan menghasilkan *ciphertext* yang berbeda pula. Dengan demikian algoritma kriptography dapat bersifat umum dan boleh diketahui oleh siapa

saja, akan tetapi tanpa pengetahuan tentang kunci, data tersandi tetap saja tidak dapat terpecahkan.

Sistem kriptography atau *Cryptosystem* adalah sebuah algoritma kriptography ditambah semua kemungkinan *plaintext*, *ciphertext* dan kunci.

2.4. Algoritma SHA

SHA adalah fungsi hash satu-arah yang dibuat oleh NIST dan digunakan bersama DSS (*Digital Signature Standard*). Oleh NSA, SHA dinyatakan sebagai standard fungsi hash satu-arah. SHA dapat dianggap sebagai kelanjutan pendahulunya, MD5, yang telah digunakan secara luas. SHA disebut aman (secure) karena ia dirancang sedemikian rupa sehingga secara komputasi tidak mungkin menemukan pesan yang berkoresponden dengan *message digest* yang diberikan.

SHA merupakan keluarga fungsi hash satu-arah. Fungsi hash SHA yang paling umum digunakan adalah SHA-1 yang telah diimplementasikan di dalam berbagai aplikasi dan protokol keamanan seperti TLS, SSL, PGP, SSH, S/MIME dan Ipsec. Anggota pertama keluarga SHA adalah SHA-0 yang dipublikasikan pada tahun 1993. SHA-0 sering diacu sebagai SHA saja. Berikutnya pada tahun 1995 SHA-1 dipublikasikan. Empat varian lain juga telah dipublikasikan yaitu SHA-224, SHA-256, SHA-384, dan SHA-512. Keempat varian ini dianggap sebagai SHA-2.

1. Penghitungan menggunakan dua buffer dimana masing-masing buffer terdiri dari lima sebesar 32 bit kata dan urutan 80 juga sebesar 32 bit kata. Lima kata pertama pada buffer kata diberi nama A, B, C, D, E sedangkan lima kata kedua diberi nama H_0 , H_1 , H_2 , H_3 , dan H_4 . Kemudian pada 80 kata yang berurutan diberi nama W_0 , W_1 , ..., W_{79} dan pada penghitungan ini juga memakai TEMP.
2. Lakukan pengisian pesan, M dan kemudian parsingkan pesan tersebut ke dalam N 512 bit blok pesan, $M^{(1)}$, $M^{(2)}$, ..., $M^{(n)}$. Caranya : 32 bit pertama dari blok pesan ditunjukkan ke $M_0^{(i)}$, lalu 32 bit berikutnya adalah $M_1^{(i)}$ dan selanjutnya berlaku hingga $M_{15}^{(i)}$.
3. Inisialisasi Nilai Hash (dalam bentuk hex) :

$$H_0 = 67452301 \quad H_3 = 10325476$$

$$H_1 = \text{EFCDAB89} \quad H_4 = \text{C3D2E1F0}$$

$$H_2 = 98BADCFE$$
4. Lakukan proses M_1, M_2, \dots, M_n dengan cara membagi M_i ke dalam 16 kata W_0, W_1, \dots, W_{15} dimana W_0 merupakan left most.

5. Hitung : For $t = 16$ to 79
 $W_t = S^1(W_{t-3} \hat{\wedge} W_{t-8} \hat{\wedge} W_{t-14} \hat{\wedge} W_{t-16})$
6. Inisialisasi 5 variabel A, B, C, D, dan E dengan nilai Hash :
 $A = H_0 ; B = H_1 ; C = H_2 ; D = H_3 ; E = H_4$.
7. Hitung : For $t = 0$ to 79

$$\text{TEMP} = S^5(A) + f_t(B,C,D) + E + W_t + K_t$$

$$E = D ; D = C ; C = S^{30}(B) ; B = A ; A = \text{TEMP}.$$

8. Hitung Nilai Hash :

$$H_0 = H_0 + A ; H_1 = H_1 + B ; H_2 = H_2 + C ; H_3 = H_3 + D ;$$

$$H_4 = H_4 + E.$$

9. Hasil dari message digest sebesar 160 bit dari pesan, M adalah : $H_0 H_1 H_2 H_3 H_4$

2.5. PHP

PHP adalah salah satu bahasa server-side yang didesain khusus untuk aplikasi web. PHP dapat disisipkan diantara bahasa HTML dan karena bahasa server-side, maka bahasa PHP akan dieksekusi di server, sehingga yang dikirimkan ke browser adalah "hasil jadi" dalam bentuk HTML, dan kode PHP tidak akan terlihat. PHP menawarkan koneksitas yang baik dengan beberapa basis data, antara lain Oracle, MySQL, mSQL, Sybase, Solid, PostgreSQL, Adabas, File Pro, Velocis, dBase, Unix dbm dan tak terkecuali semua database ber-interface ODBC.

2.6. DFD

Data Flow Diagram (DFD) adalah alat pembuatan model yang memungkinkan professional sistem untuk menggambarkan sistem sebagai suatu jaringan proses fungsional yang dihubungkan satu sama lain dengan alur data, baik secara manual maupun komputerisasi. DFD ini sering disebut juga dengan nama Bubble chart, Bubble diagram, model proses, diagram alur kerja, atau model fungsi.

DFD ini adalah salah satu alat pembuatan model yang sering digunakan, khususnya bila fungsi-fungsi sistem merupakan bagian yang lebih penting dan kompleks dari pada data yang dimanipulasi oleh sistem. Dengan kata lain, DFD adalah alat pembuatan model yang memberikan penekanan hanya pada fungsi sistem.

DFD ini merupakan alat perancangan sistem yang berorientasi pada alur data dengan konsep dekomposisi dapat digunakan untuk penggambaran analisa maupun rancangan sistem yang mudah dikomunikasikan oleh professional sistem kepada pemakai maupun pembuat program.

2.7. Sistem Basis Data

Database merupakan sekumpulan data yang terdiri atas satu atau lebih table yang terintegrasi satu sama lain dan disimpan dengan beberapa cara pengorganisasian, dimana setiap pemakai (user) diberi wewenang (otorisasi) untuk dapat mengakses (mengubah), menghapus, menganalisis, menambah, serta memperbaiki data dalam tabel-tabel tersebut. Database itu sendiri dapat dianggap sebagai suatu penyusunan data agar dapat diakses dengan mudah dan cepat, yang disimpan secara terstruktur dalam suatu media penyimpanan.

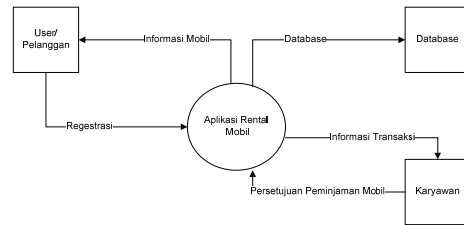
2.8. MySQL

MySQL adalah sebuah system manajemen database relasi (*relational database management system*) yang bersifat “terbuka” (*open source*). MySQL menggunakan bahasa standar SQL (*Structure Query Language*) sebagai bahasa interaktif dalam mengelola data. Perintah SQL sering juga disebut Query. Karena menggunakan bahasa standar yang sama, maka tidak akan menjadi kendala besar bila suatu saat nanti anda berhubungan dengan database selain MySQL. Tentu saja, tetap ada sedikit perbedaan sintaks bahasa antara paket program SQL tersebut.

Sejarah MySQL yang merupakan hasil buah pikiran dari Michael “Monty” Widenius, David Axmark, dan Allan Larson dimulai tahun 1995. Mereka bertiga kemudian mendirikan perusahaan bernama MySQL AB di Swedia. Tujuan awal ditulisnya program MySQL adalah untuk mengembangkan aplikasi web yang akan digunakan oleh salah satu klien MySQL AB. Memang pada saat itu, MySQL AB adalah sebuah perusahaan konsultan database dan pengembangan software (masih menggunakan nama perusahaan TcX DataKonsult AB). Situs Internet MySQL AB dapat dikunjungi di <http://www.mysql.com>.

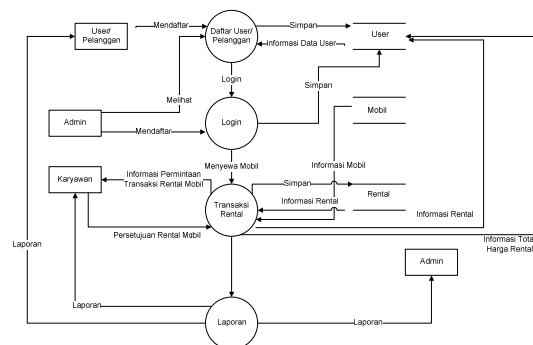
3.1. Diagram Context & DFD Level 0

Diagram dibawah ini adalah sebuah diagram sederhana yang menggambarkan hubungan antara entity luar, masukan dan keluaran dari sistem. Diagram konteks direpresentasikan dengan lingkaran tunggal yang mewakili keseluruhan sistem.



Gambar 1. Diagram konteks

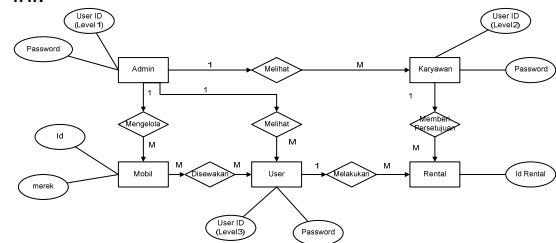
DFD level merupakan turunan dari Diagram konteks. Gambar di bawah ini merupakan DFD level 0 yang memperlihatkan proses-proses penginputan yang terdapat pada Sistem Rental Mobil yang sedang dirancang, meliputi proses Admin dan user.



Gambar 2. DFD Level 0

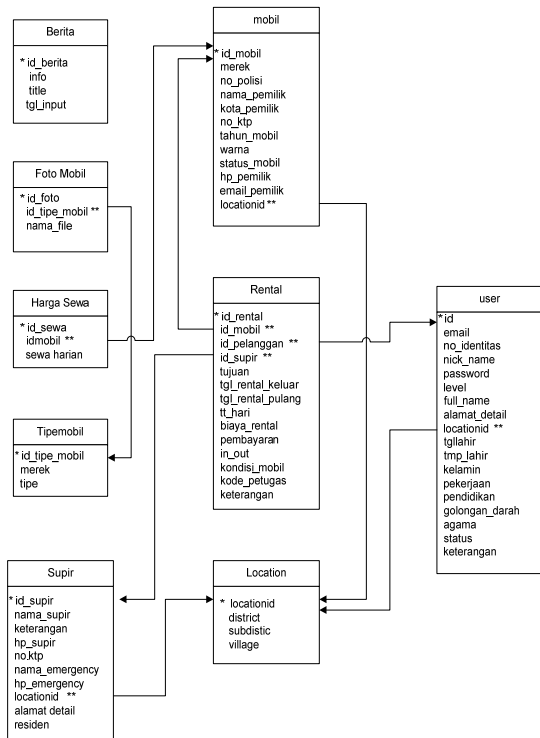
3.2. Entity Relationship Diagram (ERD)

ERD adalah model konseptual yang mendeskripsikan hubungan antar penyimpanan. ERD digunakan untuk memodelkan struktur data dan hubungan antar data yang relatif kompleks, perancangannya sebagaimana terlihat pada gambar berikut ini.



Gambar 3. Entity Relational Model

3.3. Relasi Antar Tabel



Gambar 4. Relasi Antar Tabel

4.1. Implementasi Sistem

Implementasi Aplikasi Rental Mobil ini digunakan untuk dapat menyewa mobil secara online. Sistem ini digunakan untuk pengamanan data pada saat login pada penggunaan password user.

Adapun Halaman-halaman yang digunakan dalam Aplikasi Bisnis Rental Mobil melalui Internet (E-Commerce) adalah sebagai berikut

4.2. Halaman Utama

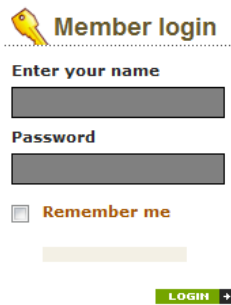
Halaman utama adalah halaman pembuka pada aplikasi sistem rental mobil ini yang digunakan oleh admin, karyawan dan user/pelanggan. Adapun menu yang tersedia pada halaman ini yaitu home yang menjelaskan secara singkat tentang jasa pelayanan penyewaan mobil. Menu pendaftaran yang digunakan untuk mendaftar user. Menu mobil yang ada dan harga mobil yang ditawarkan oleh rental mobil ini. About Us yaitu merupakan sejarah singkat tentang berdirinya rental mobil ini. dan kemudian menu Contact yaitu informasi selular yang dapat digunakan untuk menanyakan lebih lanjut tentang fasilitas yang ditawarkan oleh rental mobil ini.



Gambar 5. Halaman Utama

4.3. Halaman Login

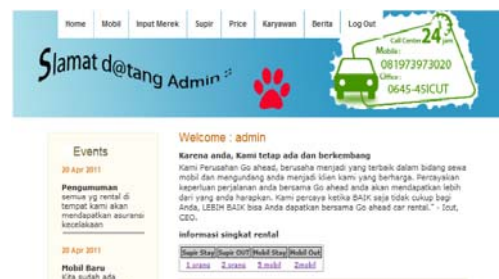
Halaman ini digunakan untuk login Admin, login Karyawan dan login User. Pada saat aktivitas login ini diterapkan penggunaan Algoritma SHA-1, yaitu pada password yang dimasukkan kemudian di enkripsikan menggunakan Algoritma SHA-1.



Gambar 6. Halaman Login Admin

4.4. Halaman Admin/Home

Halaman Admin adalah halaman yang terbuka setelah admin login. Pada halaman utama Admin/Home akan di informasikan berapa Jumlah supir yang ada, supir yang keluar, jumlah mobil yang masih ada dan jumlah mobil yang keluar.



Gambar 7. Halaman Admin/Home

4.5. Halaman Input Data Mobil

Halaman Input Data Mobil adalah Halaman untuk menambahkan data mobil,

apabila pada rental tersebut ada penambahan mobil baru.

Daftar Mobil

Tambah Daftar Mobil

Merek Mobil	Pilih Mobil ▾
Jenis Mobil	
No Polisi	
Nama Pemilik Mobil	
No KTP/SIM/Passpord	
Tahun Mobil	
Warna	Putih ▾
No Contact/HP	
email	
Alamat	ACEH BARAT ▾
Kecamatan	Pilih Kab dulu ▾

Gambar 8. Halaman input data mobil

4.6. Halaman Input Data Merek Mobil

Halaman Input Data Merek Mobil adalah Halaman untuk Menginputkan data kode mobil apa bila ada jenis Merek mobil dan nama mobil yang terbaru yang akan ditambahkan pada sistem aplikasi rental mobil ini.

INFO

== Kode Mobil ==

[1**] =>No Akhir HONDA
107 STREAM

[2**] =>No Akhir TOYOTA
210 HILUX DOUBLE CABIN

[3**] =>No Akhir DAIHATSU
305 GRAN MAX

[4**] =>No Akhir SUZUKI
401 APV

Events

20 Apr 2011
Pengumuman semua va rental di

Semua List Mobil

No	Kode Mobil	Merek Mobil	Jenis	Foto
1	101	HONDA	JAZZ	
2	102	HONDA	CITY	
3	103	HONDA	CIVIC	
4	104	HONDA	CRV	

Gambar 9. Halaman Input Data Merek Mobil

4.7. Halaman Input Data Supir

Halaman Input Data Supir adalah Halaman yang digunakan untuk meninput semua biodata supir pada rental ini.

Daftar Supir

Tambah Daftar Supir

Nama Supir	
No Hp	
No KTP	
Nama Emergency Call	
Tlp Emergency	
Alamat Detail	
Alamat	ACEH BARAT ▾
Kecamatan	Pilih Kab dulu ▾
Desa	Pilih Kec dulu ▾
TAMBAH	

Gambar 10. Halaman Input Supir

4.8. Halaman Input Harga Sewa Mobil

Halaman Input Harga Sewa Mobil adalah halaman yang digunakan untuk menginput

harga sewa mobil dan mengedit harga sewa mobil apabila suatu saat terjadi perubahan harga.

Daftar Harga Sewa Mobil

Silahkan di setting daftar harga mobil

Merek	No Polisi	Tahun	Warna	Status	Sewa/hari	Set Sewa
HONDA CIVIC	BL8888QB	2000	putih	out	400000	edit
HONDA FREED	BL 100 CA	2010	putih	ada	250000	edit
HONDA STREAM	BK 1797 US	2010	hitam	ada	350000	edit
TOYOTA FORTUNER	BL 098 US	2009	putih	ada	450000	edit
TOYOTA FORTUNER	BL 002 CA	2009	hitam	ada	450000	edit
TOYOTA YARIS	BI 001 CA	2008	merah	ada	300000	edit
DAIHATSU LUXIO	BL1QB	2010	merah	out	300000	edit

Gambar 11. Halaman Input Harga Sewa Mobil

4.9. Halaman Input Data Karyawan

Halaman Input Data Karyawan adalah Halaman yang digunakan untuk menginput data karyawan pada rental mobil ini.

Daftar Karyawan

Tambah Karyawan

User ID	
Email	
Password	
Nama Lengkap	
Alamat Detail	
Alamat	ACEH BARAT ▾
Kecamatan	Pilih Kab dulu ▾
Desa	Pilih Kec dulu ▾
Tgl Lahir	01 ▾ Jan ▾ 1976 ▾
Tempat Lahir	
Kelamin	Jenis Kelamin ▾

Gambar 12. Halaman Input Karyawan

4.10. Halaman Input Berita

Halaman Input Berita adalah Halaman yang digunakan untuk menginput berita-berita terbaru pada rental mobil ini.

Daftar Supir

Tambah Daftar Supir

Title Berita	
Isi Berita	
85 Characters Left	
POSTING	

Gambar 13. Halaman Input Berita

4.11. Halaman Karyawan

Halaman Karyawan adalah Halaman yang terbuka setelah login yang dilakukan karyawan. Disini di informasikan mobil yang sudah dipesan tetapi belum dibayar, dan mobil yang sudah dirental.



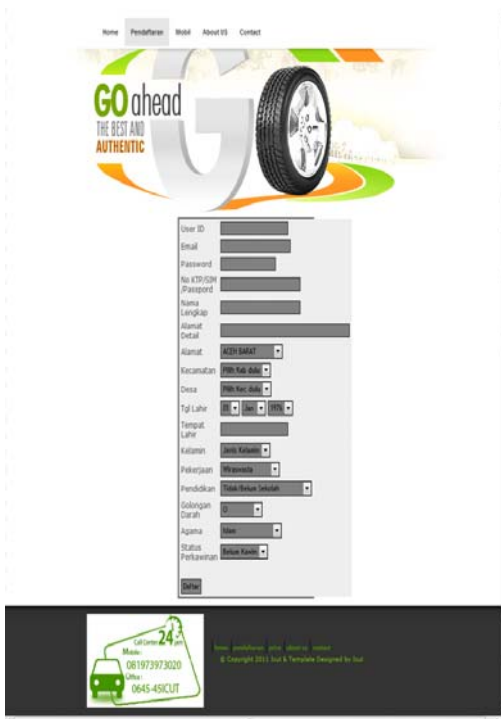
Gambar 14. Halaman Karyawan



Gambar 16. Halaman User/Home

4.12. Halaman Pendaftaran User

Halaman Pendaftaran User adalah halaman yang digunakan untuk mendaftar sebagai user pada rental mobil ini. sehingga user bisa melakukan penyewaan mobil pada usaha rental mobil ini.



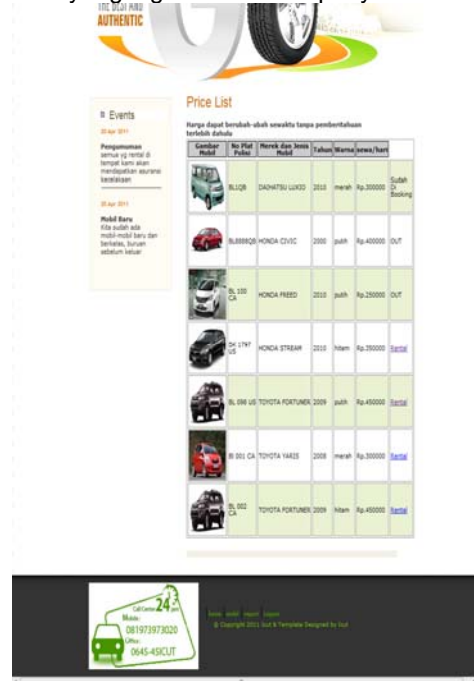
Gambar 15. Halaman Pendaftaran User

4.13. Halaman User/Home

Halaman User/Home adalah Halaman yang terbuka setelah login user.

4.14. Halaman Daftar Mobil yang siap di Rental

Halaman Daftar Mobil yang siap di Rental adalah halaman yang bisa di lihat oleh user yang ingin melakukan penyewaan mobil.



Gambar 17. Halaman Daftar Mobil yang bisa di rental

4.15. Halaman Report Mobil yang telah di Rental

Halaman Report Mobil yang telah di Rental adalah halaman yang ada apa bila user telah melakukan transaksi penyewaan mobil.



Gambar 18. Halaman Report Mobil yang telah di rental

5.1. Kesimpulan

Dari hasil perancangan dan pembuatan program aplikasi rental mobil dengan menggunakan algoritma SHA-1 (*Secure Hash Algorithm-1*) ini, dapat diambil kesimpulan sebagai berikut :

1. Perkembangan teknologi yang semakin maju menuntut semua sistem berjalan secara online, oleh karena itu dibuatlah aplikasi rental mobil yang bisa diakses secara online.
2. Program aplikasi rental mobil ini menggunakan Algoritma Sha-1 pada sistem login user, algoritma Sha-1 merupakan algoritma yang menerima masukan 2^{64} bit (2.147.483.648 gigabyte) dan menghasilkan *message digest* yang panjangnya 160 bit.
3. Penggunaan Aplikasi rental mobil ini memudahkan masyarakat untuk melakukan transaksi rental mobil, aplikasi rental mobil ini diharapkan bisa digunakan pada salah satu usaha rental mobil.

Referensi

- [1] Arbie. 2004. *Managemen Database dengan MySQL*. ANDI. Yogyakarta.
- [2] Hakim, Lukmanul. 2008. *Membongkar Trik Rahasia Para Master PHP*. Lokomedia. Yogyakarta.
- [3] Hermawan, C. Widy. 2008. *Membuat Desain Web Untuk Pemula*. ANDI. Yogyakarta.
- [4] Musyawarah, Rina. 2005. *Belajar Sendiri Membangun Aplikasi Database Berbasis Web untuk Pemula*. PT Elex Media Komputindo. Jakarta.
- [5] Nugroho, Bunafit. 2004. *Aplikasi Pemograman Web Dinamis dengan PHP dan MySQL*. Gava Media. Yogyakarta.
- [6] Setiawan, andi S.Kom, Ade Irma P.S.,S.Kom. 2006. *Pengolahan DataBase MySQL Dengan Script PHP*. CV. YRAMA WIDYA. Bandung.
- [7] Sutarma. 2007. *Membangun Aplikasi Web dengan PHP&MySQL*. Graha Ilmu.Yogyakarta.
- [8] Andri, Yogi. *Studi Pencarian Kolisi Pada SHA-1 Oleh Xiaoyun Wang dkk.* <http://www.informatika.org/~rinaldi/Kriptografi/20062007/Makalah2/Makalah-079.pdf>, Tanggal 19 Maret 2013, Jam 10.30.
- [9] Prasetyo, Muchamad Surya. *Studi dan Implementasi Algoritma Baru Dengan Mengkombinasikan Algoritma MD5 dan SHA-1.* <http://www.informatika.org/~rinaldi/Kriptografi/20082009/Makalah2/MakalahIF3058-2009-b053.pdf>, Tanggal 19 Maret 2013, Jam 09.00.
- [10] Publication, Federal Information Processing Standard Publication 180-2. *Secure Hash Standard.* <http://csrc.nist.gov/publications/fips/fips180-2/fips180-2.pdf>. Tanggal 19 Maret 2013, Jam 14.00.