IMPLEMENTASI PENGAMANAN DATABASE MENGGUNAKAN MD5

Khairil[1], Prama Wira Ginta[2]
Dosen Tetap Fakultas Ilmu Komputer Universitas Dehasen Bengkulu

ABSTRACT

Technological represent a[n very important requirement in technological era in this time, growth of computer technology at the moment of vital importance to public service service world, industry, white colars, education, commerce world and technique. For that computer as processor of data have important role of speed facet, mainstay, and also careful in processing data so that yield maximal information. To manage institution data effectively, institution which [is] education service menggelola have to check quickly and accurate in serving educative [by] children [of] institution. Data management modernly even also become important condition [of] efficacy. Managing and controlling service process in study so that goals can be realized as according to expectation. See problems and situation like that, information technology implementation and exploiting (selected by TI) solution must be compatible, so that can assist some education institution in improving performa, which tip of [at] make-up of and revenue of net profit. To be able to improve performa.

Key Word: Implementation Security of Database Use MD5

INTISARI

Teknologi merupakan sebuah kebutuhan yang sangat penting dalam era teknologi saat ini , perkembangan teknologi komputer pada saat sangat penting untuk pelayanan publik dunia layanan , industri , perkantoran , pendidikan , dunia perdagangan dan teknik . Untuk itu komputer sebagai pengolah data memiliki peran penting kecepatan segi , andalan , dan juga berhati-hati dalam pengolahan data sehingga menghasilkan informasi yang maksimal . Untuk mengelola data lembaga secara efektif , lembaga yang pelayanan pendidikan menggelola harus memeriksa dengan cepat dan akurat dalam melayani edukatif anak-anak dari lembaga . Manajemen data secara modern pun menjadi syarat penting [dari] keberhasilan . Mengelola dan mengendalikan proses pelayanan dalam penelitian sehingga tujuan dapat direalisasikan sesuai dengan harapan. Lihat masalah dan situasi seperti itu , penerapan teknologi informasi dan pemanfaatan dengan solusi harus sesuai , sehingga dapat membantu beberapa lembaga pendidikan dalam meningkatkan performa , yang ujung make- up dan pendapatan dari laba bersih . Untuk dapat meningkatkan performa.

Kata Kunci: Implementation Security of Database Use MD5

BAB I. PENDAHULUAN

A. Latar Belakang

Teknologi merupakan suatu kebutuhan yang sanggat penting dalam era teknologi saat ini, perkembangan teknologi komputer pada saat ini sanggatlah penting bagi dunia jasa layanan publik, perindustrian, perkantoran, pendidikan, teknik dan dunia perdagangan. Untuk itu komputer sebagai pengolah data mempunyai peranan penting dari segi kecepatan, kehandalan, maupun kecermatandalam memproses data sehingga menghasilkan informasi yang maksimal.

Untuk mengelola data perusahaansecara efektif dan aman, perusahaan yang menggelola layanan komunikasi harus teliti cepat dan akurat dalam melayani customer prusahaan tersebut. Manajemen data secara modern pun menjadi syarat penting keberhasilan. Mengelola dan mengontrol proses layannan data dalam

pengamanan data pesan dan data vaucher sehingga keamanan data dapat terealisasikan sesuai dengan harapan.

Melihat situasi dan permasalahan seperti itu, pemanfaatan dan implementasi teknologi informasi (TI) yang dipilih mestilah solusi yang cocok, sehingga bisa membantu beberapa institusi pendidikan dalam meningkatkan performa, yang berujung pada peningkatan *revenue* dan *net profit.* Untuk dapat meningkatkan performa,dengan kondisi yang ada diperusahaan PT Telkomsel diperlukan alur informasi yang cepat, tepat dan tertib dari NO (*Network Oprasion*), dan dari customer perusahaan. Tersajinya informasi secara cepat, tepat, dan akurat, dapat membantu manajemen dalam proses pengamanan data pesan dan data voucher di PT Telkomsel Bengkulu.

MD5 adalah untuk melindungi data dari modifikasi yang tidak terdeteksi, dapat dihitung hasil fungsi hash dari data tersebut, selanjutnya dapat menghitung hasil fungsi hashnya lagi dan membandingkannya dengan hasil fungsi hash yang sebelumnya apabila terjadi perubahan selama pengiriman.

Sistem inplementasi keamanan secara online berbasis web sanggat bermanfaat bagi pihakPT Telkomsel Bengkulu untuk dapat mengamankan data dari hal hal yang dapat merugikan perusahaan**.** untuk membuat Implementasi Pengamanan Database untuk mempermudah keamanan databasedalam melakukan pengamanan data pesan customer dan data voucher. Pokok pembahasan yang diangkat adalah,Implementasi Pengamanan Database Menggunakan MD5yang difokuskan pada:

1. Implementasi Pengamanan Database.
2. Bahasa Pemrograman yang digunakan adalah PHP dan MySql v.5.2.6
3. Pembuatan Desain menggunakan Dreamweaver 8.0

BAB II. LANDASAN TEORI

A. Sistem

Sistem adalah sekumpulan unsur atau elemen yang saling berkaitan dan saling mempengaruhi dalam melakukan kegiatan bersama untuk mencapai suatu tujuan .Contohnya sistem komputer terdiri dari *hardware, software*, dan *brainware.*Sutanta (2005:17).

Karakteristik sistem ialah bahwa properti dan perilaku komponen aplikasi barcampur. Keberhasilan berfungsinya setiap komponen aplikasi bergantung dari berfungsinya beberapa komponen: Sutanta (2005:19)

1. Komponen *(Elemen)* yaitu komponen dari suatu aplikasi dikenal sebagai subsistem.
2. Batasan (*Boundary*) yaitu Daerah yang membatasi antara aplikasi yang dengan yang lainnya ataudengan lingkungan luar.
3. Lingkungan luar sistem (*Environment*) yaitu Segala sesuatu di luar dari batas aplikasi yang mempengaruhi operasi dari suatu sistem.
   Contoh : Vendor, Pelanggan, Pemilik, Pemerintah, Bank, Pesaing
4. Penghubung Sistem (*Interface*) yaitu Suatu media penghubung antara 1 subsistem dengan subsistem lainnya.
5. Masukan (*Input)* yaitu Energi yang dimasukkan ke dalam aplikasi, Pada aplikasi sistem, masukan dapat berupa :
   a. Data transaksi
   b. Data non transaksi (misalnya: surat pemberitahuan)
   c. Intruksi

   Keluaran (*Output*) yaitu Hasil dari pemprosesan, dapat berupa keluaran yang berguna (informasi, produk) atau keluaran yg tidak berguna (limbah), Pada sistem informasi, keluaran dapat berupa :
   a. Informasi
   b. Saran
   c. Cetakan laporan

   Sasaran aplikasi*(Objective*) yaitu Suatu tujuan yang ingin dicapai oleh suatu aplikasi yang terintegrasi dengan aplikasi aplikasi komputer.

B. Jaringan GSM

Hanya GSM sub-system yang mengetahui terminal mobile yang digunakan sebagai jaringan untuk mobile t[illegible]idak seperti *data services* y[illegible]anya menggunakan PC atau notebool[illegible] *data card*. Di dalam mobile telepon [illegible]akan *alphanumeric driver* sebagai alat bantu yang praktis digunakan untuk mengirim dan menerima pesan. Bagian utama dari terminal mobile ini adalah

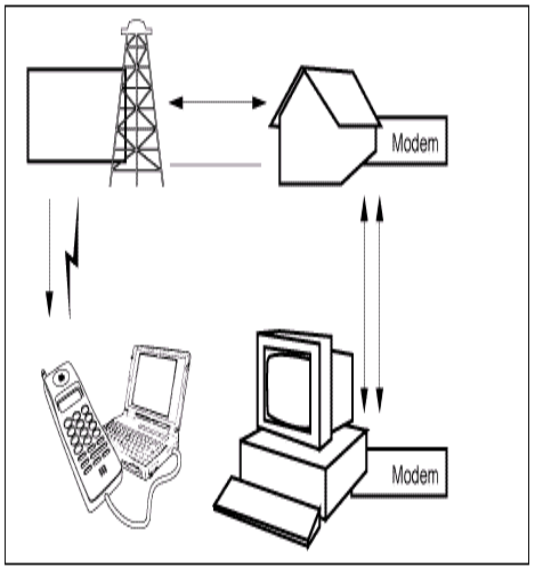
1. Mobile Transmission Equipment

Berdasarkan gambar 2.1, pada terminal ini dapat dibagi lagi menjadi tiga bagian yang terpisah yaitu

a. Terminal input/output modul yang saling terhubung antara pemakai (mikropon, speaker, keyboard) dengan sekelilingnya (PCMCIA card, loader, dan lainnya.)
b. Radio modem (modulator/demodulator) menangani perubahan analog ke digital konversi
c. Radio frekwensi modul yang menerima dan mengirim sinyal diatas jaringan cellular dengan radio interface

2. Customer Identification Module

Module adalah bentuk kartu chip atau disebut juga dengan kartu SIM (*Subscriber Identity Module*). SIM ini berisi semua informasi relatip untuk pemakai. Biasanya digunakan untuk menyimpan memory pesan dan nomor telepon. SIM Card dari suatu jaringan operator sangat diperlukan pada pengguna telepon mobile karena tanpa SIM Card telepon mobile tidak mau diaktifkan.



Gambar 2.1 Bagan Mobile Transmission Equipment

2.1.1 Proses Kerja SIM Card

SIM (*Subscriber Identity Module*) adalah salah satu penggunaan dari Smart Card atau kartu pintar. Penggunaan lain dari Smart Card misalnya untuk kartu kredit dan kartu pengenal, tetapi paling populer adalah SIM Card. Kepandaian kartu ini adalah kemampuan melakukan pengolahan data, bukan hanya sekedar menyimpan data. Smart Card dapat mengerjakannya karena mempunyai unit pemproses yang lebih dikenal sebagai CPU (Central Processing Unit) lengkap dengan ROM, EEPROM, dan RAM.

Hubungan istilah tersebut dengan komputer, memang tidak jauh. Memang, chip pada Smart Card tidak ubahnya seperti CPU komputer. Bedanya memori dalam Smart Card jauh lebih kecil. Ukuran memori yang ada misalnya 8KB, 16KB, 32KB, dan 64KB. Besar kecilnya memori ini berdampak pada jenis aplikasi yang bisa dimasukkan dalam SIM Card, serta berpangaruh juga pada besarnya *address book* dan SMS yang bisa direkam dalam SIM.

SIM Card bisa dipandang terdiri dari *hardware* dan *software*. *Hardware* adalah fisik dari chip tersebut, dengan vendor antara lain KartuHalo, simPATI, ProXL, Setelindo GSM, dan IM3 Bright. Sedangkan pada sisi *software* adalah program yang ada dalam chip, vendornya adalah Telkom dan Indosat. Operator seluler akan memesan pada vendor *software* untuk memasukkan data dan program yang diinginkan ke dalam chip SIM Card. Data yang ada dalam chip itulah yang digunakan untuk identifikasi pemegang chip atau pelanggan kepada operator seluler.

Data dalam chip disimpan dalam *file* yang disusun seperti halnya folder pada sistem operasi windows yang dikenal. Ada tiga tipe struktur file yaitu *linear fixed* (disusun dengan panjang record tetap), *cyclic* (panjang record tetap, dengan record terakhir dihubungkan dengan record awal), dan *transparent* (record disusun berderet sambung menyambung). Beberapa *file*, secara tidak langsung, sudah cukup akrab bagi pengguna ponsel, yaitu *address book* atau *phone book* dan SMS. *File* yang lain digunakan untuk menyimpan bermacam-macam parameter yang diperlukan, misalnya menyimpan IMSI (Internasional Mobile Subscriber Identify) dan ICCID (IC Card Identification). Demikian pula jika ada tambahan fasilitas menu. Misalnya menu Satelindo@access dan IM3-Access, sebagian informasi disimpan dalam file pada SIM Card tersebut. Di masa depan, *update file* bisa dilakukan operator secara langsung, jadi tidak perlu menukarkan SIM Card yang dimiliki.

Layanan pesan singkat ini dapat menyimpan dan mengirim, dengan kata lain pesan singkat tersebut tidak langsung sampai kepada penerima, melainkan diterima oleh SMSC (*Short Message Service Center*). Setelah pesan diterima dengan SMSC,

pencarian dilakukan untuk menemukan HP yang dituju. Jika HP tersebut ditemukan, pesan segera dikirimkan dalam hitungan detik. Jika sasarannya tak ditemukan, upaya pencarian terus dilakukan hingga ketemu, sampai batas waktu yang ditentukan oleh pengirim terlewati. Pemberitahuan keberhasilan atau kegagalan permintaan pengiriman dapat disetel sendiri oleh penggunanya. Masing-masing jaringan telepon mobile mendukung layanan SMS yang mempunyai satu atau lebih Service Centre untuk mengatur dan menangani pesan singkat tersebut.

2.1.2 Securitas pada SIM

File dalam SIM Card memiliki hak akses tertentu, artinya tidak semua orang bisa membacanya dengan mudah meskipun mempunyai *card reader*. Ada dua tipe akses secara garis besar, yaitu akses baca dan akses tulis. Untuk masing-masing tipe akses, juga terdapat dua macam hak secara garis besar, yaitu 'always' atau selau dapat dibaca oleh siapapun, dan *password*. Sebetulnya password yang dikenal pengguna ponsel adalah PIN1 dan PUK. Selain kedua password itu, ada yang lain misalnya PIN2 dan ADMIN. Sebagian password memang hanya dipegang oleh operator seluler dan vendor aplikasi SIM. Berkait dengan *password*, itulah keunggulan Smart Card. Kemampuan untuk menyimpan, mengolah dan mentransmisikan data menjadikan mempu mendeteksi apakah pemakai orang yang mencoba mengakses kartu tersebut adalah orang yang sah, dan sebaliknya juga mampu mengirimkan data yang rahasia ke pihak lain, dalam hal ini operator seluler, mampu mengenali bahwa kartu itu adalah kartu yang sah.

Alasan diperlukannya jaminan keamanan seperti itu tentu saja untuk menjaga kemungkinan dari tindakan yang merugikan kedua belah pihak. Apalagi untuk *mobile banking* atau *mobile commerce*, tanpa jaminan keamanan yang memadai tidak akan ada orang yang menggunakannya. Dalam konteks ini, *password* sering disebut *key*. Setiap aplikasi memerlukan *key* yang berbeda-beda. Maksudnya, sebuah SIM Card dapat digunakan untuk berbagai aplikasi, seperti *mobile banking* untuk beberapa bank misalnya, dan dalam SIM Card akan mempunyai *key* sebanyak jumlah bank yang bisa melayani. Tentu saja, bank tersebut harus bekerja sama dengan operator seluler tertentu agar dapat diakses pelanggan operator tersebut.

Meskipun kelihatannya kecil, SIM Card memegang peranan penting untuk kelangsungan komunikasi. Untuk masa depan, peranan SIM Card cukup strategis. Perkembangan teknologi menuntut untuk lebih memahami benda kecil ini, dengan fungsi dan kemampuan maxi.

2.1.3 Proses Autentikasi SIM ke Jaringan GSM

SIM Card dalam HP berfungsi untuk memastikan bahwa hanya pelanggan yang memegang SIM dari operator tersebur yang dapat mengakses jaringan. Agar hal tersebur bisa tercapai, SIM harus dapat menyimpan data, membatasi akses terhadap data yang tersimpan dan menjalankan algoritma kriptografi yang terjamin.

SIM diidentifikasikan oleh sebuah nomor unik dalam keseluruhan sistem GSM, yang disebut IMSI (*International Mobile Subscriber Identification*). Melalui IMSI pelanggan dapat dalam jaringan GSM di seluruh dunia. IMSI juga digunakan untuk menghasilkan sebuah kunci (*key*) yang dipakai untuk enkripsi selama komunikasi berlangsung. Proses enkripsi tidak berlangsung dalam SIM, karena SIM tidak mempunyai kemampuan komputasi dan kecepatan transfer data *real time*. Proses enkripsi dikerjakan ponsel, yang memiliki kemampuan memadai untuk komunikasi *real time.*

Ketika seorang pelanggan hendak melakukan komunikasi percakapan maupun mengirim data berupa SMS, ponsel melakukan *setup link* ke base station dengan penerimaan terbaik, dan mengirimkan IMSI yang ada dalam SIM ke *base station.* Jika IMSI pelanggan terdaftar di *base station* tersebut, HP akan menerima bilangan acak (*random number*), kemudian diteruskan ke SIM. Bilangan acak tersebut digunakan untuk enkripsi data selama komunikasi berlangsung. Sebuah sistem yang terhubung ke *base station* akan melakukan proses yang sama untuk SIM penerima. Jika keduanya sama maka SIM, komunikasi dan penerimaan data dalam jaringan dapat dilakukan.

C. Defenisi MD5 dan Konsep Penggunaannya.

2.2.1. Definisi MD5

Dalam kriptografi, MD5 (Message-Digest algortihm 5) ialah fungsi hash kriptografik yang digunakan secara luas dengan hash value 128-bit. Pada standart Internet (RFC 1321), MD5 telah dimanfaatkan secara bermacam-macam pada aplikasi keamanan, dan MD5 juga umum digunkan untuk melakukan pengujian integritas sebuah file. Sutedjo (2000:26)

MD5 di desain oleh Ronald Rivest pada tahun 1991 untuk menggantikan hash function sebelumnya, MD4. Pada tahun 1996, sebuah kecacatan ditemukan dalam desainnya, walau bukan kelemahan fatal, pengguna kriptografi mulai menganjurkan menggunakan algoritma lain, seperti SHA-1 (klaim terbaru menyatakan bahwa SHA-1 juga cacat). Pada tahun 2004, kecacatan-kecacatan yang lebih serius ditemukan menyebabkan penggunaan algoritma tersebut dalam tujuan untuk keamanan jadi makin dipertanyakan.

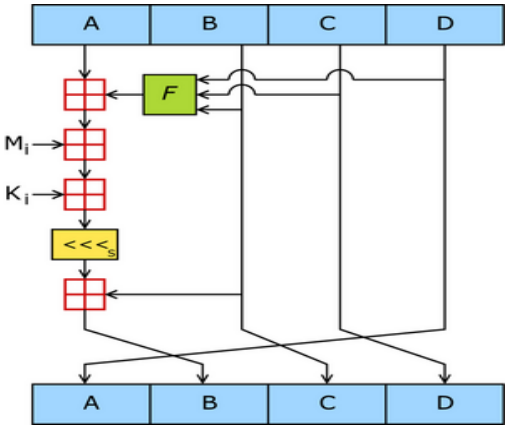
2.2.2. Konsep Penggunaan MD5

Konsep penggunaan md5 antara lain:

1. Kerahasiaan (Confidentiality).
   Sederhananya, kerahasiaan adalah proses penyembunyian data dari orang-orang yang tidak punya otoritas.
2. Integritas (Integrity)
   Proses untuk menjaga agar sebuah data tidak dirubah-rubah sewaktu ditransfer atau disimpan.
3. Penghindaran Penolakan (Non-repuditation)
   Proses untuk menjaga bukti-bukti bahwa suatu data berasal dari seseorang. Seseorang yang ingin menyangkal bahwa data tersebut bukan berasal darinya, dapat saja melenyapkan bukti-bukti yang ada. Karenanya diperlukan teknik untuk melindungi data-data tersebut.
4. Autentikasi (Authentication)
   Proses untuk menjamin keaslian suatu data.
5. Tanda Tangan Data (Data Signature)
   Dapat disebut juga sebagai tanda tangan digital. Berguna untuk menandatangi data digital. Contohnya adalah Digital Signature Algorithm (DSA).
6. Kontrol Akses (Access Control)
   Untuk mengontrol akses terhadap suatu entity.
   Contoh penggunaan kriptografi di dunia internet antara lain: Secure Shell (SSH), SSL (Secure Socket Layer), Secure Hypertext Transfer Protocol (HTTP), dan lain lain.

2.2.3. Cara Kerja MD5

MD5 mengolah blok 512 bit, dibagi kedalam 16 subblok berukuran 32 bit. Keluaran algoritma diset menjadi 4 blok yang masing-masing berukuran 32 bit yang setelah digabungkan akan membentuk nilai hash 128 bit.



Gambar 1. Algoritma MD5

Pesan diberi tambahan sedemikian sehingga panjang menjadi k-bit, dimana k = 512n – 64 bit. n merupakan blok masukan. Tambahan ini diperlukan hingga pesan menjadi k bit. Kemudian 64 bit yang masing kosong, dibagian akhir, diisi panjang pesan. Inisiasi 4 variabel dengan panjang 32 bit yaitu a,b,c,d. Variabel a,b,c,d dikopikan ke variabel a,b,c,d yang kemudian diolah melalui 4 tahapan yang sangat serupa. Setiap tahapan menggunakan 16 kali operasi berbeda, menjalankan fungsi nonlinear pada tiga variabel a,b,c, atau d. Hasilnya ditambahkan ke variabel keempat, subblok pesan dan suatu konstanta. Kemudian dirotasi kekiri beberapa bit yang kemudian ditambahkan ke salah satu dari a,b,c, atau d. Kemudian nilai a,b,c, dan d menggantikan nilai a,b,c, dan d. Kemudian dikeluarkan output yang merupakan gabungan dari a,b,c, dan d. Fungsi kompresi yang digunakan oleh algoritma md5 adalah sebagai berikut :

a ← b + ((a + g (b,c,d) + X[k] + T[i] <<< s), dimana g adalah salah fungsi primitif F,G,H,I seperti dibawah ini :

$$F(X,Y,Z) = (X \wedge Y) \vee (\neg X \wedge Z)$$
$$G(X,Y,Z) = (X \wedge Z) \vee (Y \wedge \neg Z)$$
$$H(X,Y,Z) = X \oplus Y \oplus Z$$
$$I(X,Y,Z) = Y \oplus (X \vee \neg Z)$$

2.2.4. Algoritma MD5

Algoritma MD-5 secara garis besar adalah mengambil pesan yang mempunyai panjang variabel diubah menjadi 'sidik jari' atau 'intisari pesan' yang mempunyai panjang tetap yaitu 128 bit. 'Sidik jari' ini tidak dapat dibalik untuk mendapatkan pesan, dengan kata lain tidak ada orang yang dapat melihat pesan dari 'sidik jari' MD-5. Sutendy (2005:35) Message digest atau intisari pesan harus mempunyai tiga sifat penting, yaitu :

1. Bila P diketahui, maka MD(P) akan dengan mudah dapat dihitung.
2. Bila MD(P) diketahui, maka tidak mungkin menghitung P.
3. Tidak seorang pun dapat memberi dua pesan yang mempunyai intisari pesan yang sama. H(M) H(M').

2.2.5. Pengertian Web

Web adalah sebuah alamat komputer yang menyimpan file-file yang ditulis dalam *hyper text markup language* (HTML) dan memperbolehkan komputer-komputer lain untuk terhubung dan membaca file-file tersebut. Menurut Thomson (2003,167) HTML adalah bahasa yang mencakup sekumpulan kode atau label *(tag)* yang terlampir dalam text. Contohnya, sebuah dokumen HTML memili kita untuk mengindikasikan bagianmana dari dokumen tersebut yangmerupakan judul,dimanaakhirparagrafdan sebagainya.

D. Tinjauan Umum Perangkat Komputer

2.3.1. Tinjauan Perangkat Lunak (*Software*)

Software adalah program yang berisi perintah-perintah untuk melakukan pengolahan data. Sutanta (2005:17).

2.3.2. Tinjauan Perangkat Keras (*Hardware*)

Hardware adalah peralatan dari sistem komputer dan peralatan pendukungnya yang secara phisik terlihat dan dapat dijamah. Sutanta (2005:18).

2.3.3. Tinjauan Pengguna (*Branware*)

Brainware adalah manusia yang terlibat di dalam mengoperasikan serta mengatur sistem komputer. Sutanta (2005:18)

E. Teknik Pemrograman

Pemrograman PHP

PHP (*Hypertext Prepocessor*) merupakan suatu script yang bersifat *ServerSide* yang artinya PHP dieksekusi terlebih dahulu oleh *Web Server*, kemudian hasilnya akan dikirimkan ke browser *client*. PHP juga dapat ditambahkan pada HTML untuk membuat sebuah web menjadi lebih menarik, dinamis dan interaktif.

Ini diciptakan pertama kali oleh seorang mahasiswa Finlandia yang bernama Rasmus Lerdorf. Dia menciptakan PHP dari bahasa Perl dan C, sehingga apabila dilihat sepintas script Perl dan PHP hampir mempunyai persamaan yang cukup banyak. Dari segi penamaan variabelpun sama. Dengan PHP kita dapat mengolah data konsumen yang diambil dengan sebuah form, membuat aplikasi-aplikasi tertentu dalam sebuah web, ataupun membuat *database* dalam sebuah web. Pertengahan tahun 1995 dirilis PHP / FI (FI adalah singkatan dari Form Interpreter) yang memiliki kemampuan dasar membangun aplikasi web, memproses form, dan mendukung database MySQL.

PHP memiliki kelebihan tersendiri dibandingkan dengan ASP maupun Perl, disamping gratis PHP juga mampu berjalan di berbagai sistem operasi. Penulisan script PHP tidak sesulit dengan penulisan script Perl, JSP ataupun ASP. *Database* pasangannya biasanya adalah MySQL. Dan sebagai catatan penting dalam penulisan pemrograman PHP, tidak terlepas dari tag <HTML> karena proses kode PHP disisipkan pada halaman HTML. Untuk saat ini PHP merupakan sebuah alternatif yang tepat dalam membangun sebuah aplikasi berbasis web karena sebagian besar dunia web saat ini masih didominasi oleh platform UNIX dan Variantnya seperti Linux.

Bahasa script standar yang digunakan oleh PHP adalah *Microsoft VBScript* dan *JavaScript*.

a. Tag PHP

Seperti halnya disebutkan sebelumnya, bahwa parser PHP akan membaca file HTML (*Hyper Text Markup Language*)

sampai ditemukan tag khusus yang memberitahukan untuk menerjemahkan teks berikutnya sebagai kode PHP. Parser PHP akan menjalankan semua kode yang dibacanya dari tag awal tadi sampai ditemukan tag penutup kembali. Dengan cara inilah maka kode script PHP dapat ditempatkan pada dokumen HTML (*HTML – Embedded*). Semua teks yang berada di luar tag awal dan akhir PHP akan diangap sebagai teks HTML biasa dan akan dikirimkan langsung ke browser client untuk ditampilkan.

Ada 4 (empat) pasangan tag yang dapat digunakan untuk menyatakan sebuah blok kode PHP. Diantara keempat ini, 2 (dua) pasangan tag berikut umumnya digunakan dan dimengerti oleh interpreter, yaitu :

a. <?php statement; ?>
b. <?statement; ?>
c. <script language=”php”> statement; </script>
d. <%statement; %>

Cara kedua hanya dapat jalan jika pilihan short tags diaktifkan. Ini dapat dilakukan dengan menggunakan fungsi short_tags() (hanya pada PHP 3). Kemudian cara pertama adalah yang paling tepat dan aman digunakan (selain cara ketiga). Sedangkan cara keempat kadang menjadi rancu karena tag ini sama dengan tag yang digunakan pada script ASP dan tag ini hanya tersedia pada PHP versi 3.0.4 ke atas.

1. Statement

Sebuah statement merupakan sebuah perintah yang diakhiri dengan tanda titik koma (;). Tanda tag penutup script PHP juga dapat sebagai penutup atau menyatakan akhir dari suatu statement PHP.

Tipe Data

PHP memiliki 8 (delapan) tipe dasar, yaitu :

a) Bolean
b) Integer
c) Float (floating point)
d) String
e) Array
f) Object
g) Resource
h) Null

Biasanya tipe variabel pada PHP tidak ditentukan oleh programmer. Akan tetapi ditentukan berdasarkan untuk apa variabel itu digunakan pada saat program dijalankan. PHP memiliki kemampuan yang baik dalam mengoperasikan variabel. Jika kita mengoperasikan variabel dengan tipe data yang berbeda, PHP dapat melakukan operasi tersebut tanpa ada kesalahan pada saat proses pengeksekusian.

2.4.1. Fungsi API MySQL

Agar dapat menampilkan hasil query pada browser klient, PHP memerlukanfungsi API (Application Programming Interface). Prasetyo (2003:272).Berikut ini beberapa fungsi API MySQL yang di dukung oleh PHP :

1. Mysql_connect()
   Digunakan untuk melakukan koneksi (hubungan) dengan database MySQLserver.
   Sintaks:
   $conn=mysql_connect(“host”,”username”,”password”)
   $conn : nama variabel penampung status hasil koneksi kepada
   database.
   host : nama host atau alamat server database MySQL.
   Username : nama user yang telah diberi hak untuk dapat
   mengakses server database .
   password : adalah kata sandi untuk username untuk dapat masuk
   ke dalam database.
2. Mysql_select_db()
   Digunakan untuk melakukan koneksi kepada database yang dalam server yangberhasil dikoneksi dengan perintah mysql_connect().
   Sintaks:
   $pilih=mysql_select_db(“namadatabase”,$conn)
   $pilih : berisi status koneksi kepada database
   $conn : koneksi kepada server database yang berhasil.
   namadatabase : nama database yang akan dikenai proses.
3. Mysql_create_db() : Untuk membuat database baru.
4. Mysql_query()

Digunakan untuk melakukan eksekusi perintah SQL untuk memanipulasi database yang berhasil dilakukan koneksinya dengan menggunakan mysql_select_db().
Sintaks:
$hasil=mysql_query("SQLStatement")
$hasil akan berupa record set apabila SQLStatement berupa perintah SELECT.

5. Mysql_fetch_array()
Digunakan untuk melakukan pemrosesan hasil query yang dilakukan dengan perintah mysql_query().
Sintaks:
$array=mysql_fetch_array($hasil)
$array adalah array satu record dari record $hasil yang diproses. Nomor record
sesuai dengan nomor urut dari proses mysql_fetch-array yang sedang dilakukan.
$hasil adalah record set yang akan diproses.

2.4.2. Dreamweaver 8.0

Dreamweaver 8.0 adalah sebuah program Web Editor yang digunakan untuk membuat dan mendesain Web. Dreamweaver 8.0 mempunyai kemampuan dalam membuat dan mendesain web tanpa harus menulis tag-tag HTML satu persatu dan juga mendukung Server side (digunakan untuk memperoses data yang berhubungan ke server), Client side (bahasa pemrograman tambahan sekaligus sebagai pelengkap dari bahasa pemrograman yang lain). Beberapa Bagian terpenting dalam jendela kerja Dreamweaver 8.0 diantaranya:

a. Insert Bar
Fungsi*Insert Bar* merupakan kumpulan menu yang digunakan untuk memasukan sebuah objek atau fungsi ke dalam jendela document.

b. Document Toolbar
Fungsi*Document Toolbar* digunakan sebagai penempatan file-file yang telah dibuka dan sekaligus untuk menampilkan nama dari file tersebut.

c. Document Window
Fungsi *Document Window* merupakan tempat untuk menampilkan objek-objek atau kode program dari tab code, split dan design.

d. Panel Group
Fungsi *Panel Group* untuk mengatur halaman web yang telah dibuat.

e. Property Inscpector
Fungsi *Property Inscpector* untuk mengetahui atau mengubah property dari sebuah objek.

C. Konsep Perancangan Data Base

2.5.1. Database

Database manajemen sistem adalah kumpulan file yang saling berkaitan bersama dengan program untuk pengelolaannya. Kusrini (2007:2).

a. Entity : *Entity* adalah orang, tempat, kejadian atau konsep yang informasinya direkam.

b. ***Atribute :*** *Atribute* merupakan sebutan untuk mewakili suatu entity

c. ***Data Value :*** *Data value* adalah data aktual atau informasi yang disimpan pada tiap data elemen atau atribute.

d. ***Record/Tuple :*** *Record* adalah kumpulan elemen-elemen yang saling berkaitan menginformasikan tentang suatu.

e. ***File :*** *File* adalah kumpulan record-record sejenis yang mempunyai panjang elemen yang sama, atribut yang sama, namun berbeda beda data valuenya.

f. ***Database :*** *Database* adalah kumpulan file-file yang mempunyai kaitan antara file satu dengan file yang lain sehingga membentuk satu bangunan data untuk menginformasikan satu Usaha, instansi dalam batasan tertentu.

2.5.2. Entity Relationalship

Pada model data relational hubungan antar file direlasikan dengan kunci relasi (*relation key*), yang merupakan kunci utama dari masing-masing file. Kusrini (2007:21).

Konsep Entity Relationalship

1) One To One Relationship 2 File
Merupakan hubungan antara file pertama dengan file kedua adalah berbanding satu.

2) One To Many Relationship 1File
Merupakan hubungan antara file pertama dengan file kedua adalah satu berbanding banyak.

3) Many To Many Relationship 2 File
Merupakan hubungan antara file pertama dengan file kedua adalah banyak berbanding banyak.

4) One To One 2 Atribute Dalam 1 File

Merupakan hubungan antara satu atribute dengan atribute yang lain dalam satu file yang sama mempunyai hubungan satu lawan satu.

5) ***Many To One 2 Atribute Dalam 1 File***
Merupakan hubungan antara satu atribute dengan atribute yang lain dalam satu file yang sama mempunyai hubungan satu lawan banyak.

6) ***Many to many 2 atribute dalam 1 file***
Merupakan hubungan antara satu atribute dengan atribute yang lain dalam satu file yang sama mempunyai hubungan banyak lawan banyak.

2.5.3. Jenis Perangkat Permodelan

A. Data Flow Diagram (DFD)

Data flow diagram adalah gambaran sistem secara logical. Gambaran ini tergantung pada perangkat keras, perangkat lunak, struktur data atau organisasi file. Keuntungan menggunakan data flow diagram adalah memudahkan pemakai yang kurang menguasai bidang komputer untuk mengerti sistem yang akan dikerjakan atau dikembangkan. Kusrini (2007:17)

Data flow diagram ini hanya terdiri dari empat simbol yaitu :

1) Elemen-Elemen Lingkungan

Elemen-elemen lingkungan berada diluar sistem. Elemen ini menyediakan bagi input data dan menerima output data sistem. Pada DFD ada perbedaan antara data dan informasi. Semua harus dipandang sebagai data.Simbol Lingkungan Luar :

2) Proses

Proses adalah yang mengubah input menjadi output. Proses dapat digambarkan dengan lingkaran atau segi empat tegal dengan sudut-sudut membulat.

3) Arus Data

Arus data terdiri dari sekelompok elemen data yang berhubungan secara logis yang bergerak dari satu titik atau proses ke titik atau proses lain. Tanda panah digunakan untuk menggambarkan arus itu. Jumlah data yang diwakili oleh satu arus dapat bervariasi dari satu elemen data tunggal hingga satu atau beberapa file.

4) Data Store

Jika data perlu dipertahankan karena suatu sebab, maka digunakan penyimpanan data. Bayangkan penyimpanan data sebagai data yang diam (data at rest). Simbol yang digunakan untuk penyimpanan data adalah satu set garis paralel atau segi empat terbuka.

BAB III
METODOLOGI PENELITIAN

3.1. Subjek Penelitian

Penelitian dilakukan di PT.Telkomsel Bengkulu yang berlokasi di Jl. Kapten Tendean No.86 Km.6,5 Kota Bengkulu 38225.

3.2. Metode Penelitian

Metode yang digunakan dalam pembuatan proposal ini adalah metode pengembangan sistem. Pengembangan merupakan observasi dibawah kondisi buatan (artificial condition), kondisi tersebut dibuat dan dikembangkan sendiri oleh peneliti dari hasil pengamatan dan analisis di lapangan.

3.3. Perancangan Perangkat Lunak dan Perangkat Keras

3.3.1. Perangkat Keras

Perangkat keras yang digunakan dalam penelitian adalah : Komputer dengan spesifikasi: a) CPU : Intel® Pentium ® Dual core, b) LCD : 17 Inchi WXGA, c) *Memory* : 512 GB d) *Harddisk* : 80 GB, e) *Mouse* : *Optic, f) Keyboard* : USB standar, g) *PrinterCanon* IP1800

3.3.2. Perangkat Lunak

Perangkat Lunak yang digunakan pada penelitian adalah sistem operasi *Microsoft Windows 7*, Bahasa Pemrograman *PHP* dan menggunakan databasenya MySQL untuk desain dibantu dengan menggunakan Dreamweaver 8.0

3.4. Metode Pengumpulan Data

Untuk dapat melaksanakan penelitian ini, maka perlu adanya kegiatan mengumpulkan, menganalisis, mengelola, menyajikan data yang dilakukan secara sistematis dan efisien untuk memecahkan persoalan, tentunya diperlukan data yang tepat dan akurat.

Untuk itu dalam melakukan proses pengumpulan data, ada beberapa metode sebagai berikut :

3.4.1. Metode Observasi

Data penelitian dikumpulkan dengan melakukan pengamatan atau observasi terhadap service keamanan data PT.Telkomsel Bengkulu.

3.4.2. Metode Wawancara

Pada penelitian dilakukan wawancara dengan salah satu stafnya adalah Alvindo di PT Telkomsel Bengkulu mengenai sistemKeamanan Data Pesan dan Voucer Pulsadi PT Telkomsel Bengkulu.

3.4.3. Metode Studi Pustaka

Penelitian mengenai sistem informasi via online juga memerlukan data dari literatur yang diperoleh dari buku-buku komputer, buku mengenai informasilaporan majemen. Pada metode studi pustaka, data juga diperoleh dari jurnal, majalah dan dari internet.

3.5. Metode Perancangan Sistem

3.5.1. Analisa Sistem Lama

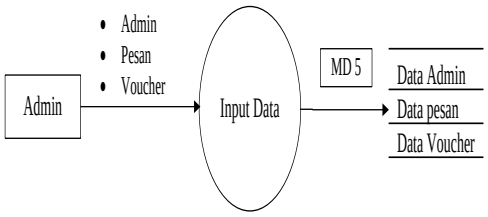
Keamanan data yang di PT Telkomsel Bengkulusaat ini masi dijalankan denggan keamanan data password komputer. Pembuatan keamanan data pesan dan voucer pulsa via database tanpa batas masih belum diterapkan di PT Telkomsel Bengkulu.

Sistem proses pengamanan database, pesan dan voucheryang sedang dijalankan oleh PT Telkomsel Bengkulu saat ini dirasakan memerlukan peningkatan agar dihasilkan layanan yang lebih berkualitas. Informasi mengenai pesan dan vocher pulsa,harus lebih cepat dan akurat, sehingga manajemen dapat berjalansebagaimana yang diharapkan.Sistem pengamanan database sangat perlu untuk diimplementasikan di PT Telkomsel Bengkuluuntuk menunjang kualitas kecepatan, pengamanan dan service yang semangkin bersaing, terutama dalam bidang teknologi informasi.

3.5.2. Pengembangan Sistem Baru

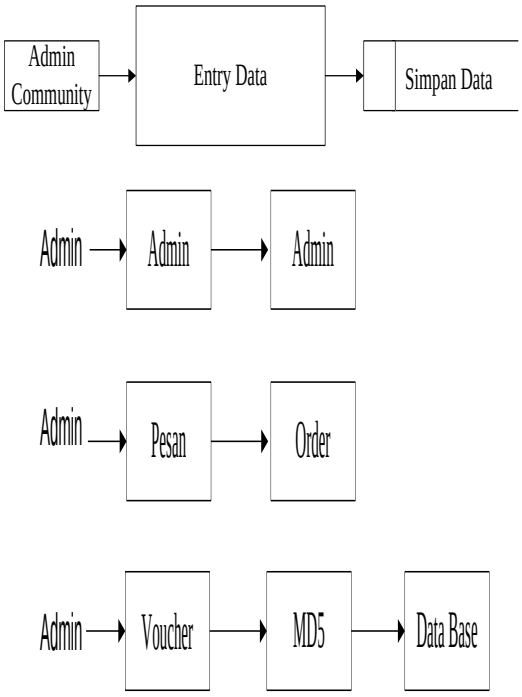
Pengembangan sistem Keamanan Databasedi PT Telkomsel Bengkulu, dimulai dengan pembuatan diagram konteks, dilanjutkan dengan pembuatan diagram alir data, HIPO, ERD, rancangan file database, dan rancangan *input* serta *output* aplikasi.

A. Diagram Konteks



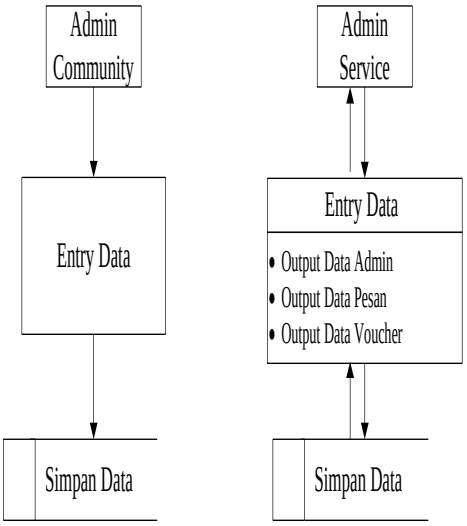
Gambar 3.1 Diagram Konteks

B. Data Flow DiagramLevel 1 Proses 1



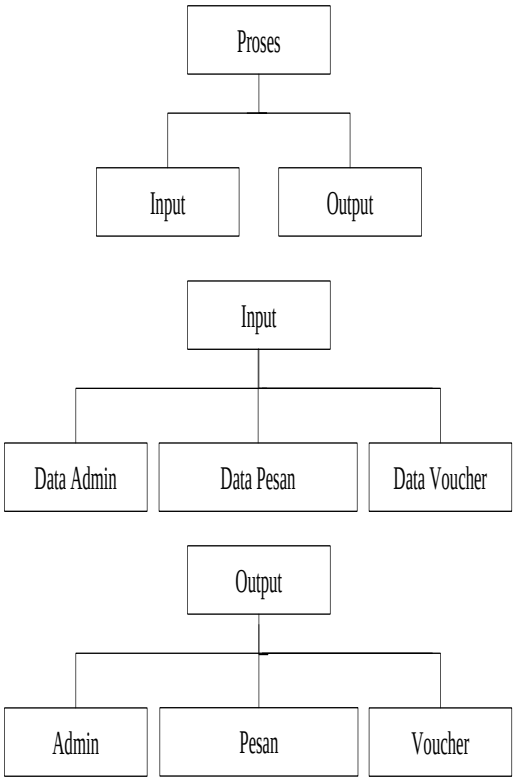
Gambar 3.2 Data Flow DiagramLevel 2 Proses 1

C. Data Flow DiagramLevel 1 Proses 2



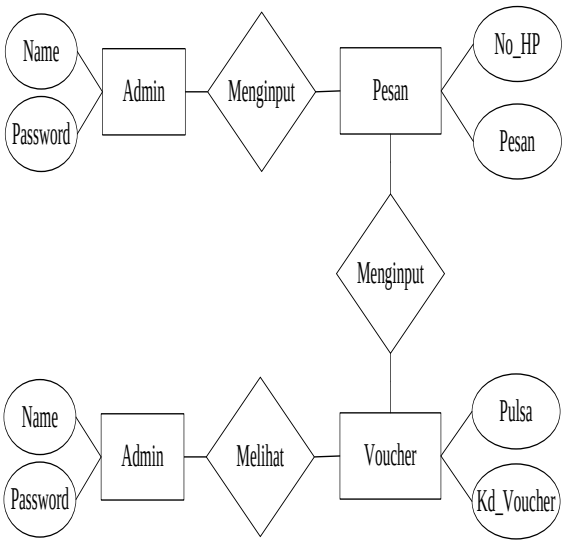
Gambar 3.3 Data Flow DiagramLevel 1

D. HIPO (Hierarki Input Process Dan Output)



Gambar 3.4HIPO (Hierarki Input Process Dan Output)

E. Entity Relationship Diagram (ERD)



Gambar 3.5 Entity Relationship Diagram (ERD)

F. Rancangan File Data

1. Tabel Admin Community
   Nama *File* : Admin Community
   PrimaryKey : user
   Secondarry Key : password

Tabel 3.1.Admin Community

No	Field_ Name	Type	Width	Keterangan
1	User	Varchar	5	Nama Admin Community
2	Password	Int	20	Kata Kunci

2. Tabel Admin Service
   Nama *File* : Admin Service
   PrimaryKey : user
   Secondarry Key : password

Tabel 3.2.Admin Service

No	Field_Name	Type	Width	Keterangan
1	User	Varchar	5	Nama Admin Service
2	Password	Int	20	Kata Kunci

3. Tabel Pesan
   Nama *File* : Pesan
   PrimaryKey : Id_Pesan
   Secondarry Key : Pesan

Tabel 3.3.Pesan

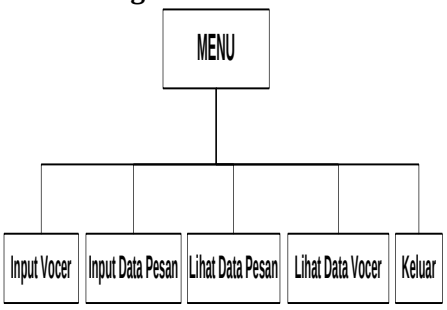
No	Field_Name	Type	Width	Keterangan
1	Id_Pesan	Text	-	No Pesan
2	Tanggal	Date	-	Tanggal
3	No_HP	Int	13	No HP
4	Pesan	Text	-	Pesan

4. Tabel Voucher
   Nama *File* : Voucher
   PrimaryKey : Id_Voucher

Tabel 3.4.Voucher

No	Field_ Name	Type	Width	Keterangan
1	Id_Voucher	Vercar	25	No Voucher
2	Pulsa	Int	6	Harga Pulsa
3	Kd_Voucher	Int	25	Kode Voucher
4	Masa Berlaku	Date	-	Masa Berlaku
5	Jenis	Text	20	Jenis Voucher
6	Area	Text	20	Area Voucher

G. Rancangan Menu



Gambar 3.6 Rancangan Menu

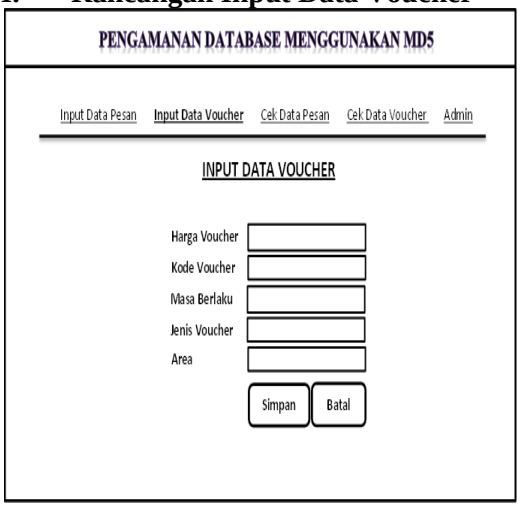
Rancangan Menu di sini sebagai sub untuk menampilkan menu-menu yang berhubungan dengan halaman-halaman menu yang ada pada Implementasi Pengamanna Database Menggunakan MD5 di PT.Telkomsel.

H. Rancangan Login Admin Internal

Gambar 3.6 Rancangan Login Admin Internal

Rancangan Login Admin Internal di sini berfungsi untuk menampilkan login masuk ke dalam web internal di PT Telkomsel Bengkulu.Ditampilkan pada gambar 3.6
Rancangan Input Data Pesan disini berfungsi untuk memasukan data pesan yang akan di enkripsi. Dapat dilihat pada gambar 3.7

I. Rancangan Input Data Voucher



Gambar 3.8 Rancangan Input Data Voucher

Rancangan Input Data Voucher disini berfungsi untuk memasukan data voucher yang akan di encripsi. Dapat pada gambar 3.8

J. Rancangan Cek Data Voucher Encripsi.

Gambar 3.11 Rancangan Cek Data Voucher Encripsi.

Rancangan Cek Data Voucher Encripsi disini berfungsi untuk melihat database yang telah di encripsikan. Dapat dilihat pada gambar 3.11

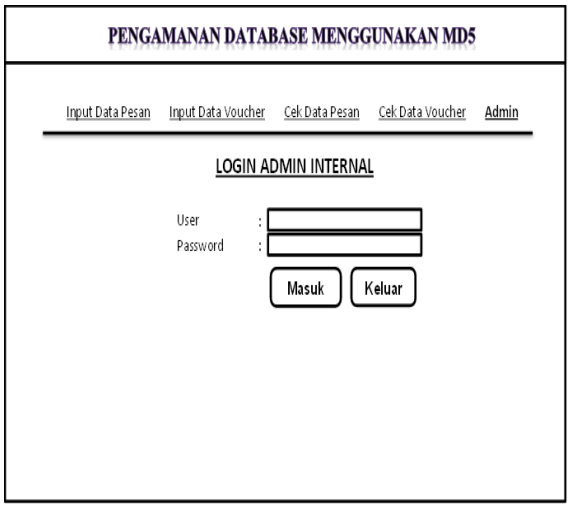
K. Rancangan Login Cek Data Voucher

L.

Gambar 3.12 Rancangan Login Cek Data Voucher

Pada Halaman Rancanagan Login Cek Data Voucherdisini berfungsi untuk login internal dalam mencek database secara normal.Dapat dilihat pada gambar 3.12

M. Rancangan Admin



Gambar 3.13 Rancangan Admin

Pada Halaman Rancanagan Admin disini berfungsi untuk Login Masuk Registrasi Admin yang dapat login di web internal ini.Dapat dilihat pada gambar 3.13

3.6. Perancangan Pengujian

Perancangan pengujian dengan menggunakan black boxuntuk memastikan pemasukan data keluaran telah berjalan sebagaimana yang diharapkan dan apakah informasi yang disimpan secara eksternal selalu dijaga kemutakhirannya.Pengujian merupakan proses eksekusi program atau perangkat lunak dengan tujuan mencari kesalahan dari program yang telah dibuat. Suatu program yang diuji akan dievaluasi apakah keluaran atau output yang dihasilkan telah sesuai dengan yang diinginkan atau tidak.

BAB IV

HASIL DAN PEMBAHASAN

A. Hasil Perancangan Sistem

Dari rancangan hingga implementasi sistem, saya telah mempersentasikan program ini di PT.Telkomsel Regional Bengkulu denggan hasil baik. Dua pokok bahasan yang di pertanyakan dan diutamakan dalam program ini adalah Sistem input

data voucer dan pengamanan data MD5 pada databasenya.

B. Pembahasan

Sistem Pengamanan

Rancangan Login Admin Internal

Gambar 4.1 Rancangan Login Admin Internal

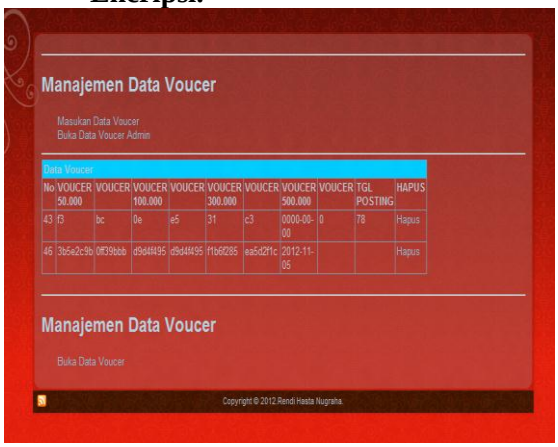
Rancangan Login Admin Internal di sini berfungsi untuk menampilkan login masuk ke dalam web internal di PT Telkomsel Bengkulu.Ditampilkan pada gambar 4.1

Rancangan Input Data Voucher

Gambar 4.2 Rancangan Input Data Voucher

Rancangan Input Data Voucher disini berfungsi untuk memasukan data voucher yang akan di encripsi. Dapat pada gambar 4.2

Rancangan Cek Data Voucher Encripsi.



Gambar 4.3 Rancangan Cek Data Voucher Encripsi.

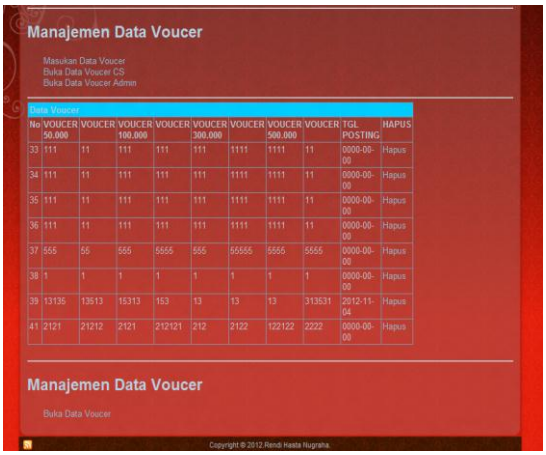
Rancangan Cek Data Voucher Encripsi disini berfungsi untuk melihat database yang telah di encripsikan. Dapat dilihat pada gambar 4.3

Rancangan Admin

Gambar 4.4 Rancangan Admin

Pada Halaman Rancanagan Admin disini berfungsi untuk Login Masuk Registrasi Admin yang dapat login di web internal ini.Dapat dilihat pada gambar 4.4

Rancangan Login Cek Data Voucher



Gambar 4.5 Rancangan Login Cek Data Voucher

Pada Halaman Rancanagan Login Cek Data Voucherdisini berfungsi untuk login internal dalam mencek database secara normal.Dapat dilihat pada gambar 4.5

A. **HASIL PENGUJIAN**

Pengujian Sistem

Dalam pengujian sistem ini dilakukan dengan dua metode yaitu metode pengetesan kotak hitam (*black box test*) dan metode pengetesan (*alfa test*). Akan tetapi disini penulis menggunakan metode pengetesan kotak hitam.

Pengetesan Kotak Hitam (*black box test*)

Pengetesan ini dilakukan oleh mahasiswa Universitas Dehasen Bengkulu danbeberapa staf PT. Telkomsel Regional Bengkulu. Pengetesan dilakukan dengan cara menjalankan program yaitu sebagai media input data voucer. Untuk admindapat pengecekan data asli dari MD5, sebagai media informasi untuk keamanan admin. Berdasarkan uji coba sistem initelah sesuai input dengan output sesuai dengan yang diharapkan dan dapat berjalan dengan baik.

BAB V

KESIMPULAN DAN SARAN

A. Kesimpulan

Dapat disimpulkan hasil penelitian dan pembahasan di atas sebagai berikut:

1. Sistem Keamannan Data Voucerini dibuat dengan pemrograman Macromedia Dreamweaver dan dapat dijalankan pada komputer Multi User dibawah sistem operasi windows.
2. Sistem keamanan yang telah dibuat menyediakan fasilitas bagi admin yaitu untuk melakukan verifikasi data voucer manajemen internal.

B. Saran

Saran untuk sistem informasi ini antara lain adalah sebagai berikut:

1. Diharapkan sistem ini kedepannya dapat dikembangkan lagi bukan hanya keamanan data voucer di PT. Telkomsel Regional Bengkulu.
2. Sebaiknya sistem keamanan pada PT.Telkomsel Regional Bengkulu ini, kedepan dapat menggunakan sistem mobile (HP).

DAFTAR PUSTAKA

Jogiyanto.*PengenalanKomputer*, Yogyakarta:Andi Offset, 2003.

Kusrini, 2007*Strategi Perancangan dan Pengolahan Basis Data*: Andi Offset Yogyakarta.

Sutanta, 2005 *Pengertian Sistem Informasi*: Graha Ilmu Jakarta.

Stendy B. Sakur, 2003 *Aplikasi Web Database dengan Dreamweaver MX*: Andi Offset Yogyakarta.

Sutedjo, Budi. *AlgoritmadanTeknikPemrograman*, Yogyakarta:Andi Offset, 2000.

Yasyin, Suichan. *KamusLengkapBahasa Indonesia*, Surabaya:Amanah, 2000.