PENGEMBANGAN SISTEM KEAMANAN UNTUK TOKO ONLINE BERBASIS KRIPTOGRAFI AES MENGGUNAKAN BAHASA PEMROGRAMAN PHP DAN MYSQL

Benni Candra , Jusuf Wahyudi, Hermawansyah

Program Studi Teknik Informatika Fakultas Ilmu Komputer Universitas Dehasen Bengkulu
Jl. Meranti Raya No. 32 Kota Bengkulu 38228 Telp. (0736) 22027, 26957 Fax. (0736) 341139

ABSTRACT

Online Shop Security System based AES Cryptography is an application in the form of an online store website that was developed to improve safety and comfort for the user. Online store security system implemented at the time of login in the form of a verification code. This online store security system restricts website access only on one specific computer so that data is more secure than those who are not responsible.Online Shop Security System based AES cryptography was developed using Adobe Dreamweaver web editor with web promgramming PHP and MySQL database server. Web design in the form of headers, banner and other web components edited using the program Adobe Photoshop image processing applications. The processing of data using SQL syntax.Results of research and testing show that the System Security Online store based AES cryptography can display information well and is user friendly both for users and administrators, and is also equipped with a security system that can improve user comfort in accessing the online store.
Keywords: System, Security, Kriftografi, AES

INTISARI

Sistem Keamanan Toko Online berbasis Kriptografi AES merupakan aplikasi dalam bentuk website toko online yang dikembangkan untuk meningkatkan keamanan dan kenyamanan bagi pengguna. Sistem keamanan Toko Online diimplementasikan pada saat login dalam bentuk kode verifikasi. Sistem keamanan toko online ini membatasi akses website hanya pada satu komputer tertentu sehingga data menjadi lebih aman dari pihak yang tidak bertanggung jawab.Sistem Keamanan Toko Online berbasis Kriptografi AES dikembangkan menggunakan *webeditorAdobe Dreamweaver* dengan *web promgramming PHP* dan *database server MySQL*. Desain web berupa header, banner dan komponen web lainnya diedit menggunakan program aplikasi pengolah gambar *Adobe Photoshop*. Proses pengolahan data menggunakan sintaks SQL.Hasil penelitian dan pengujian menunjukan bahwa Sistem Keamanan Toko Online berbasis Kriptografi AES dapat menampilkan informasi dengan baik dan bersifat *user friendly* baik untuk pengguna maupun admin serta juga dilengkapi dengan sistem keamanan yang dapat meningkatkan kenyaman pengguna dalam mengakses toko online.
Kata Kunci: Sistem, Keamanan, Kriftografi, AES

I. PENDAHULUAN

Toko online adalah sarana untuk melaksanakan kegiatan publikasi dan transaksi barang dan jasa melalui internet, dimana pengunjung dapat melihat foto, harga dan deskripsi produk atau jasa yang ditawarkan tersebut dalam sebuah halaman web. Kelebihan toko online antara lain adalah memudahkan calon pembeli untuk mencari informasi barang tanpa harus datang kelokasi penjual. Biaya operasi yang relatif minim, berbeda dengan membuka toko konvensional yang harus menyewa tempat dengan harga mahal. Toko online dapatdihandel kapanpun dan dimanapun. Memiliki jangkauan pasar yang cukup luas, karena dapat menjangkau wilayah manapun selama masih terdapat koneksi internet dan juga dapat beroperasi tanpa batasan waktu, bahkan ada toko online yang buka 24 jam nonstop.

Toko online dalam kegiatan operasionalnya menggunakan jaringan internet yang rentan pada segi keamanan karena dapat diakses oleh siapa saja dengan kepentingan yang beragam. Oleh karena itu toko online memerlukan sistem keamanan untuk menjaga privasi baik untuk admin maupun pelanggan. Sistem keamanan ini menjamin admin dalam mengupdate data produk, nomor rekening transaksi dan data lain terkait toko online serta menjamin data pelanggan seperti data pemesanan, history transaksi dan data poin atau bonus pelanggan bagi toko online yang menerapkan sistem bonus bagi pelanggan.

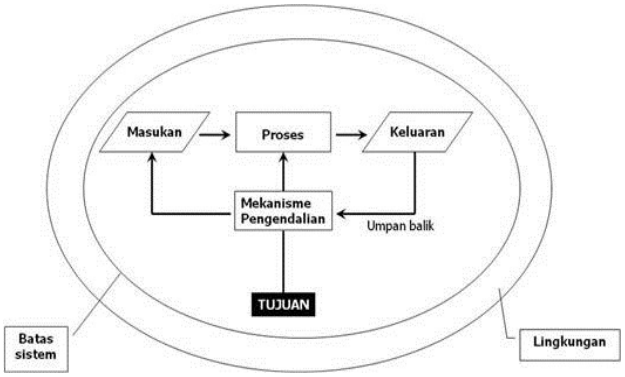
Sistem keamanan yang dibahas dalam penelitian ini adalah sistem keamanan pada sesi login baik bagi admin maupun pelanggan. Login dibatasi hanya dapat dilakukan pada komputer yang telah diverifikasi, artinya proses login hanya dapat dilakukan pada komputer tertentu. Proses login yang dilakukan diluar komputer yang telah didaftarkan tidak akan dapat dilakukan walau menggunakan *username* dan *password* yang valid, dengan demikian keamanan admin dan pelanggan lebih terjamin.

II. TINJAUAN PUSTAKA

A) Sistem Keamanan

Sistem adalah kumpulan elemen, komponen, atau subsistem yang saling berintegrasi dan berinteraksi untuk mencapai tujuan tertentu. Jadi setiap sistem memiliki subsistem-subsistem, dan subsistem terdiri ata komponen-komponen atau elemen-elemen. Sebagai contoh sistem komputer memiliki subsistem *software*, *hardware*, dan pengguna (*brainware*). Sedangkan subsistem *hardware* terdiri dari subsistem peranti input, peranti proses, dan peranti *output* (Supriyanto, 2007:238).

Karakteristik sistem adalah sistem yang mempunyai komponen-komponen, batas sistem, lingkungan sistem, penghubung, masukan, keluaran, pengolah dan sasaran. Untuk lebih jelasnya dapat dilihat pada Gambar dibawah ini yang merupakan karakteristik sistem.



Gambar 1. Karakteristik Sistem

Dari Gambar 1 dapat dijelaskan bahwa karakteristik sistem dapat dibagi menjadi 8 bagian, yaitu:

1) Komponen

Elemen-elemen yang lebih kecil yang disebut sub sistem, misalkan sistem komputer terdiri dari sub sistem perangkat keras, perangkat lunak dan manusia.Elemen-elemen yang lebih besar yang disebut supra sistem.

2) Boundary (Batasan Sistem)

Batas sistem merupakan daerah yang membatasi antara suatu sistem dengan sistem yang lainnya atau dengan lingkungan luarnya. Batas sistem ini memungkinkan suatu sistem dipandang sebagai suatu kesatuan.

3) Environment (lingkungan Luar Sistem)

Lingkungan dari sistem adalah apapun di luar batas dari sistem yang mempengaruhi operasi sistem. Lingkungan luar sistem dapat bersifat menguntungkan dan dapat juga bersifat merugikan sistem tersebut. lingkungan luar yang mengutungkan merupakan energi dari sistem dan dengan demikian harus tetap dijaga.

4) Interface (Penghubung Sistem)

Penghubung merupakan media perantara antar sub sistem. Melalui penghubung ini memungkinkan sumber-sumber daya mengalir dari satu subsistem ke subsistem lainnya. Output dari satu sub sistem akan menjadi input untuk subsistem yang lainnya.

5) Input (Masukan)

Masukan adalah energi yang dimasukkan ke dalam sistem. Masukan dapat berupa maintenance input dan sinyal input. Maintenance input adalah energi yang dimasukkan supaya sistem tersebut dapat beroperasi.

6) Output (Keluaran)

Keluaran adalah hasil dari energi yang diolah dan diklasifikasikan menjadi keluaran yang berguna dan sisa pembuangan. Keluaran dapat merupakan masukan untuk subsistem yang lain atau kepada supra sistem.

7) Proses (Pengolahan Sistem)

Suatu sistem dapat mempunyai suatu bagian pengolah atau sistem itu sendiri sebagai pengolahnya. Pengolah yang akan merubah masukan menjadi keluaran. Suatu sistem produksi akan mengolah masukan berupa bahan baku dan bahan-bahan yang lain menjadi keluaran berupa barang jadi.

8) Objective and Goal (Sasaran dan Tujuan Sistem)

Suatu sistem pasti mempunyai tujuan atau sasaran. Kalau suatu sistem tidak mempunyai sasaran, maka operasi sistem tidak akan ada gunanya. Sasaran dari sistem sangat menentukan sekali masukan yang dibutuhkan sistem dan keluaran yang akan dihasilkan sistem. Suatu sistem dikatakan berhasil bila mengenai sasaran atau tujuannya.

Masalah keamanan merupakan salah satu aspek terpenting dari sebuah sistem informasi. Masalah keamanan sering kurang mendapat perhatian dari para perancang dan pegelola sistem informasi. Masalah keamanan sering berada di urutan setelah tampilan, atau bahkan di urutan terakhir dalam daftar hal-hal yang dianggap penting. Apabila mengganggu performansi sistem, masalah keamanan sering tidak diperdulikan bahkan ditiadakan (Ariyus, 2008: 6)

Beberapa kemungkinan serangan keamanan sistem antara lain adalah *intrusion*yaitu penyerangan jenis ini seseorang penyerang akan dapat menggunakan sistem komputer yang kita miliki, *denailofservices*merupakan penyerangan ini mengakibatkan pengguna yang sah tidak dapat mengakses sistem, *joyrider*adalah penyerangan jenis ini disebabkan oleh orang yang merasa iseng dan ingin memperoleh kesenangan dengan cara menyerang suatu sistem, *vandal*merupakan jenis serangan ini bertujuan untuk merusak sistem yang sering dituju untuk site-site besar, *scorekeeper* merupakan jenis serangan ini hanyalah bertujuan untuk mendapatkan reputasi dengan cara mengacak-acak

system sebanyak mungkin dan mata-mata adalah jenis serangan ini bertujuan untuk memperoleh data atau informsi rahasia dari pihak pesaing. Tujuan utama adanya sistem keamanan adalah untuk membatasi akses informasi dan *resources* hanya ditujukan untuk pemakai yang memiliki hak.

Beberapa ancaman keamanan yang dapat mengancam suatu sistem adalah *leakgace*yaitu pengambilan informasi oleh penerima yang tidak berhak.*Tampering*atau pengubahan informasi yang tidak legal dan *vandalism*yaitu gangguan operasi sistem tertentu, dimana pelaku tidak mengharapkan kuntungan apapun.

Teknik keamanan adalah hal penting dalam menjaga kerahasiaan data. Proses enkripsi di dalam teknik keamanan merupakan proses pengkodean pesan untuk menyembunyikan isi file. Sedangkan algoritma enkripsi modern menggunakan kunci kriptografi dimana hasil enkripsi tidak dapat di dekripsi tanpa kunci yang sesuai.

Kriptografi adalah suatu ilmu yang mempelajari bagaimana membuat suatu pesan menjadi aman selama pengiriman dari pengirim sampai ke penerima. Pesan yang akan di enkripsi disebut plaintext sedngkan pesan yang telah di enkripsi disebut chipertext.

Serangan pada sistem terdistribusi tergantung pada pengaksesan saluran komunikasi yang ada atau membuat saluran baru yang menyamarkan sebagai koneksi legal. Penyerangan yang ada yaitu penyerangan pasif dan aktif. Selain itu juga terdapat pula metode-metode penyerangan terhadap suatu sistem. Klasifikasi metode penyerangan tersebut adalah *Eavesdropping*, *Masquerading*, *Messagetampering*, *Replaying*, *Denailofservices* atau teknik membanjiri saluran atau resources dengan pesan yang bertujuan untuk menggagalkan pengaksesan pemakaian lain.

B) Toko Online

*OnlineStore*atauTokoOnlineadalah sebuah toko atau tempat berjualan yang sebagian besar aktivitasnya berlangsung secara online di internet. Dari pengertian tersebut, dapat diindentifikasi bahwa tidak semua aktivitasdi online storeberlangsung secaraonline.Terdapat aktivitas pengiriman barang, hal ini harus dilakukan secar a manual dari lokasi pengelola ke alamat pembeli. Biasanya pengiriman dibebankan pada konsumen, meski ada juga toko yang membebaskannya untuk produk-produk tertentu, atau pada saat menggelar program promosi (Susrini, 2010: 13)

Toko online merupakan suatu media penjualan dan pembelian barang atau jasa melalui internet. Web toko online ini merupakan salah satu sarana untuk memudahkan penjual untuk menjual produknya dan memudahkan para pembeli, karena pembeli tidak perlu datang ke toko.Keuntungan toko onlinetidak hanya bisa dirasakan oleh penjual. Bagi pembeli, onlinestore adalah sebuah alternatif yang menyenangkan dalam berbelanja. Keberadaan online storesering kali menjadi penolong bagi yang sering melakukan aktivitas di dunia maya. Sebagai pembeli, umumnya adalah pembeli yang tidak punya cukup waktu untuk mendatangi toko, pembeli yang meninginkan kepraktisan dan lebih hemat waktu.Kerugian onlinestore yang utama yaitu modal, pengartian modal tersebut yaitu meliputi modal keuangan, modal ilmu, dan modal waktu, karena koneksi internet di Indonesia yang masih tergolong mahal maka dibutuhkan modal keuangan yang cukup untuk bisa menjalankan danmengelola toko online tersebut.

C) Kriptografi

Kriptografi adalah ilmu dan seni untuk menjaga keamanan pesan, kriptografi juga merupakan ilmu yang mempelajari teknik-teknik matematika yang berhubungna dengan aspek keamanan informasi seperti kerahasiaan, integritas data serta otentikasi (Munir, 2006: 2)

Ada empat tujuan mendasar dari ilmu kriptografi ini yang juga merupakan aspek keamanan informasi yaitu:

a). Kerahasiaan, adalah layanan yang digunakan untuk menjaga isi dari informasi dari siapapun kecuali yang memiliki otoritas atau kunci rahasia untuk membuka/mengupas informasi yang telah disandi.

b). Integritas data, adalah berhubungan dengan penjagaan dari perubahan data secara tidak sah. Untuk menjaga integritas data, sistem harus memiliki kemampuan untuk mendeteksi manipulasi data oleh pihak-pihak yang tidak berhak, antara lain penyisipan, penghapusan, dan pensubsitusian data lain kedalam data yang sebenarnya.

c). Autentikasi, adalah berhubungan dengan identifikasi/pengenalan, baik secara kesatuan sistem maupun informasi itu sendiri. Dua pihak yang saling berkomunikasi harus saling memperkenalkan diri. Informasi yang dikirimkan melalui kanal harus diautentikasi keaslian, isi datanya, waktu pengiriman, dan hal lainnya.

d). Non-repudiasi., atau nirpenyangkalan adalah usaha untuk mencegah terjadinya penyangkalan terhadap pengiriman atau terciptanya suatu informasi oleh yang mengirimkan/membuat.

Berdasarkan kunci yang digunakan untuk enkripsi dan dekripsi, kriptografi dapat dibedakan menjadi 2 (dua) macam, yaitu kriptografi simetri dan kriptografi asimetri.

a) Kriptografi Simetri (*Symetric Cryptography*) kunci untuk proses enkripsi sama dengan kunci untuk proses dekripsi. Keamanan sistem kriptografi simetri terletak pada kerahasiaan kunci. Istilah lain untuk kriptografi simetri adalah kriptografi kunci privat (*private key cryptography*) atau kriptografi

konvensional. Sebelum melakukan pengiriman pesan, pengirim dan penerima harus memilih suatu suatu kunci tertentu yang sama untuk dipakai bersama, dan kunci ini haruslah rahasia bagi pihak yang tidak berkepentingan sehingga algoritma ini sering disebut juga sebagai algoritma kunci rahasia (secret-key algorithm).

b) KriptografiAsimetri (*Asymetric Cryptography*), pada sistem kriptografi asimetri, kunci untuk proses enkripsi tidak sama dengan kunci untuk proses dekripsi. Istilah lain untuk kriptografi asimetri adalah kriptografi kunci publik (public key cryptography), sebab kunci untuk enkripsi tidak rahasia dan dapat diketahui oleh siapapun, sementara kunci untuk dekripsi hanya diketahui penerima. Kunci publik disebarkan secara umum sedangkan kunci privat disimpan secara rahasia oleh si pengguna. Walau kunci publik telah diketahui namun akan sangat sukar mengetahui kunci privat yang digunakan.

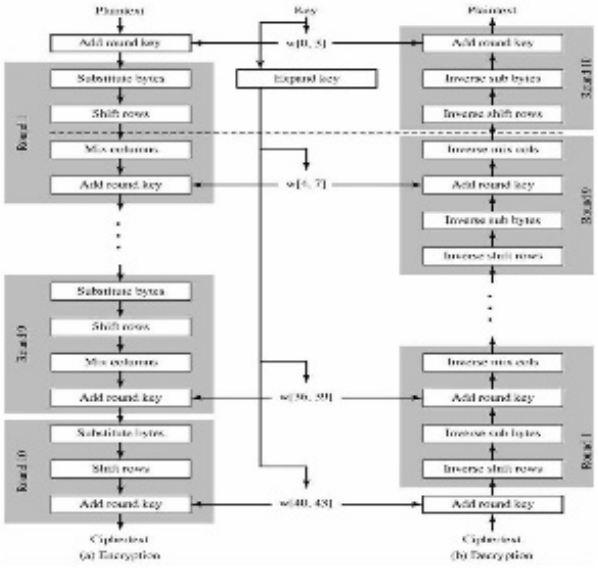
D) AES (Advanced Encryption Standard)

Algoritma AES (Advanced Encryption Standard) atau Algoritma Rijndael menggunakan substitusi dan permutasi, dan sejumlah putaran (chiper berulang). Setiap putaran menggunakan kunci internal yang berbeda (kunci setiap putaran disebut roundkey). Algoritma AES beroperasi dalam orientasi byte dan tidak menggunakan jaringan Feistel. Algoritma AES mendukung panjang kunci 128 bit sampai 256 bit dengan step 32 bit. Panjang kunci dan ukuran blok dapat dipilih secara independen. Setiap blok dienkripsi dalam sejumlah putaran tertentu (Munir, 2006:158).

Pada Algoritma AES setiap masukan 128 bit plaintext dimasukkan ke dalam state yang berbentuk bujursangkar berukuran 4×4 byte. State ini di-XOR dengan key dan selanjutnya diolah 10 kali dengan subtitusi-transformasi linear-Addkey. Dan di akhir diperoleh ciphertext. Proses enkripsi pada Algoritma AES terdiri dari 4 jenis transformasi bytes, yaitu *SubBytes*,*ShiftRows*, *Mixcolumns*, dan *AddRoundKey*.Gambaran umum Enkripsi dan Dekripsi pada algoritma kriptografi AES dapat dilihat pada Gambar 2.

E) PHP

PHP (PHP: Hypertext Preprocessor) adalah sebuah HTML-embedded scripting language, yaitu scripting language yang 'ditempelkan' dalam dokumen HTML, seperti halnya JavaScript atau VBScript. Tujuannya kurang lebih juga sama, yaitu untuk menciptakan halaman web yang interaktif dan dinamis. PHP atau PHP:Hypertext Preprocessor sebetulnya bermula dari Personal Home Page tools. PHP adlaah salah satu bahasa scripting yang ditaruh



Gambar 2. Proses Enkripsi dan Dekripsi Algoritma AES

di dalam HTML. Sintaks PHP mirip dengan Perl, namun lebih sederhana. Saat ini PHP termasuk salah satu yang terpopuler. PHP dapat dijalankan lewat CGI atau sebagai modul Apache (Supriyanto, 2007: 362).

F) MySQL

MySQL mendukung hampir semua bahasa pemrograman populer saat ini, seperti C, C++, Java, Perl, PHP, dan Phyton. MySQL menerapkan metode yang sangat cepat dalam hal relasi antar tabel pada *database*-nya. Dengan metode *one-sweep multijoin*, MySQL sangat efisien dalam mengelola informasi yang diminta yang berasal dari banyak tabel sekaligus. (Riyanto, 2009:307)

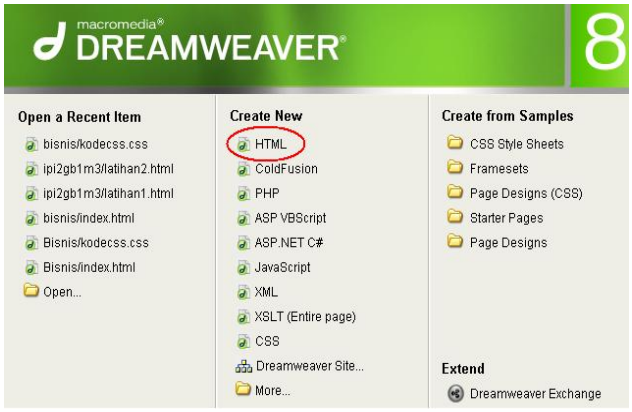
MySQL adalah server basis data yang kompak dan kecil yang ideal untuk banyak aplikasi basis data on-line. MySQL mendukung SQL standar (ANSI), meskipun tidak selengkap subset yang menjadi standar seperti PostgreSQL.MySQL dapat dijalankan di banyak platform dan memiliki kemampuan multithreading pada server UNIX.

G) Dreamweaver

Macromedia Dreamweaver adalah sebuah software design yang menawarkan cara mendesain website dengan dua langkah sekaligus dalam satu waktu, yaitu mendesain dan memprogram. Dreamweaver memiliki satu jendela mini yang disebut HTML source, tempat kode-kode HTML tertulis. Setiap kali mendesain web, seperti menulis kata-kata meletakkan gambar, membuat tabel dan proses lainnya, tag-tag HTML akan langsung tertulis. (Suyanto, 2005)

Pada halaman awal Dreamweaver terdapat beberapa menu yang dapat dipilih yaitu menu *OpenaRecentItem*, Pada menu ini akan ditampilkan beberapa

file yang sebelumnya pernah kita buka. Menu *CreateNew*, pada menu ini kita dapat memilih dokumen baru apa yang akan kita buat. Menu lainnya adalah *CreatefromSamples*, pada menu ini kita dapat membuat file berdasarkan contoh yang sudah diberikan oleh *Dreamweaver*. Gambar 3. adalah tampilan awal dari *Dreamweaver*.



Gambar 3. Tampilan Awal Dreamweaver

H) Database

Database merupakan kumpulan dari data yang saling berhubungan satu dengan yang lainnya, tersimpan di simpanan luar komputer dan digunakan perangkat lunak tertentu untuk memanipulasinya. Database merupakan salah satu komponen yang penting di sistem informasi, karena berfungsi sebagai basis penyedia informasi bagi para pemakainya. Penerapan database dalam sistem informasi disebut dengan database system. (Jogiyanto, 2005:217)

Model database adalah suatu konsep yang terintegrasi dalam menggambarkan hubungan (*rela-tionships*) antar data dan batasan-batasan (*constraint*) data dalam suatu sistem database. Model data yang palingumum,berdasarkan pada bagaimana hubu-ngan antar recorddalamdatabase, terdapat tigajenis, yaitu:

1) Model Database Hirarki (*HierarchicalDatabaseModel*)
2) Model Database Jaringan (*NetworkDatabaseModel*)
3) Model Database Relasi (*RelationalDatabaseModel*).

I) Data Flow Diagram (DFD)

DFD sering digunakan untuk menggambarkan suatu sistem yang telah ada atau sistem baru yang akan dikembangkan secara logika tanpa mempertimbangkan lingkungan fisik dimana data tersebut mengalir atau dimana data tersebut akan disimpan. DFD merupakan alat yang digunakan pada metodologi pengembangan sistem yang terstruktur. DFD merupakan alat yang dapat menggambarkan arus data di dalam sistem dengan terstruktur dan jelas (Jogiyanto, 2005:700)

III. METODOLOGI PENELITIAN

A) Analisa Sistem Aktual

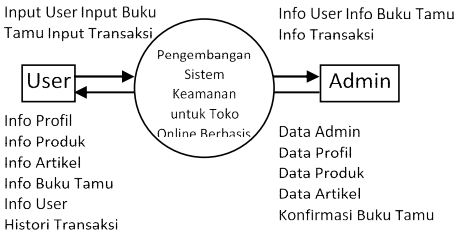
Toko Option Komputer merupakan salah satu toko komputer di Bengkulu yang bergerak di bidang penjualan perangkat komputer dan aksesoris. Saat ini toko komputer melayani transaksi penjualan secara langsung di toko dan juga melayani COD (*Cash On Delivery*). Promosi yang telah dijalankan oleh Toko Option Komputer antara lain dengan penyebaran brosur dan iklan di media massa. Toko Option Komputer juga telah memiliki website, namun hanya berupa web statis sekedar untuk promosi dan belum memfasilitasi untuk transaksi onlinetian adalah:

Analisis sistem aplikasi kriptografi pesan menggunakan algoritma Rivest Code 4 (RC4).Implementasi dan pengujian sistem, yakni melakukan pengujian terhadap sistem yang telah dirancang.

B) Perancangan Sistem Baru

Sistem baru yang dirancang pada penelitian ini adalah Toko Online Penjualan Perangkat Komputer dan Aksesoris pada Toko Option Komputer dengan pendekatan dari segi keamanan data pelanggan (*user*) dan keamanan dalam proses transaksi online. Perancangan sistem baru dilakukan dalam beberapa tahap rancangan yaitu:

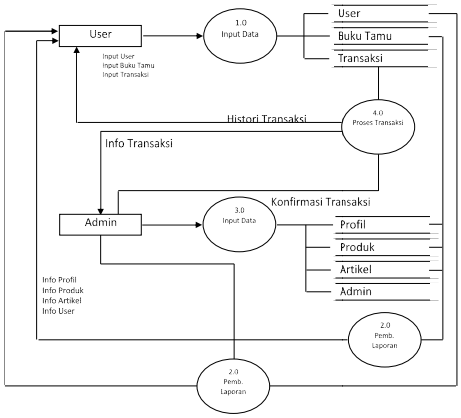
1) Diagram konteks



Gambar 4. Diagram Konteks

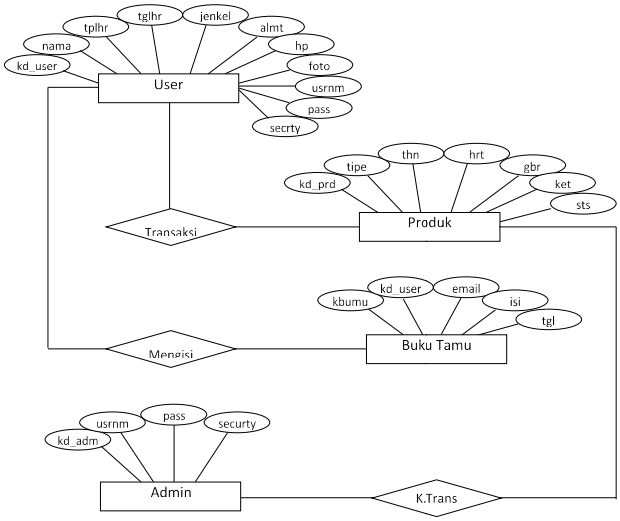
2) Diagram Alir Data (DAD)

Diagram Alir Data yang digunakan dalam penelitian ini dapat dilihat pada gambar berikut.



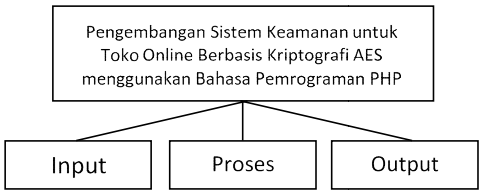
Gambar 5. Diagram Alir Data

3) Rancangan ERD (Entity Relationship Diagram)



Gambar 6. Rancangan ERD

4) HIPO (Hierarki Plus Prosess dan Output)



Gambar 7. Diagram HIPO

IV. PEMBAHASAN

A) Hasil

Website Toko Online Option Komputer terdiri dari tujuh menu utama yaitu *home*, profil, informasi, artikel, user, buku tamu dan admin.

1) Halaman Home

Halaman home merupakan halaman utama web yang tampil pada saat diakses domain web tersebut. Pada penelitian ini dilakukan pengujian secara offline maupun online. Pada pengujian offline, diakses melalui *localhost*, pada pengujian online diakses melalui alamat http://optionkomputer.xp3.biz.Gambar 8 berikut adalah tampilan halaman home.

Gambar 8. Halaman Home

2) Halaman Visi dan Misi

Halaman Visi dan Misi berisi uraian mengenai visi yang hendak dicapai oleh Option Komputer dan juga Misi yang menjadi arahan dalam pencapai Visi Option Komputer. Halaman visi dan misi dapat dilihat padaGambar 9 berikut ini.

Gambar 9. Halaman Visi dan Misi

3) Halaman Struktur Organisasi

Halaman struktur organisasi berisi tampilan bagan struktur organisasi pada Toko Option Komputer yang meliputi jabatan pemilik toko, manajer, sekretaris, bendahara, bagian produk, bagian stok, pemasaran, bagian service, front office dan driver atau sopir. Tampilan halaman struktur organisasi dapat dilihat pada Gambar 10.

Gambar 10. Halaman Struktur Organisasi

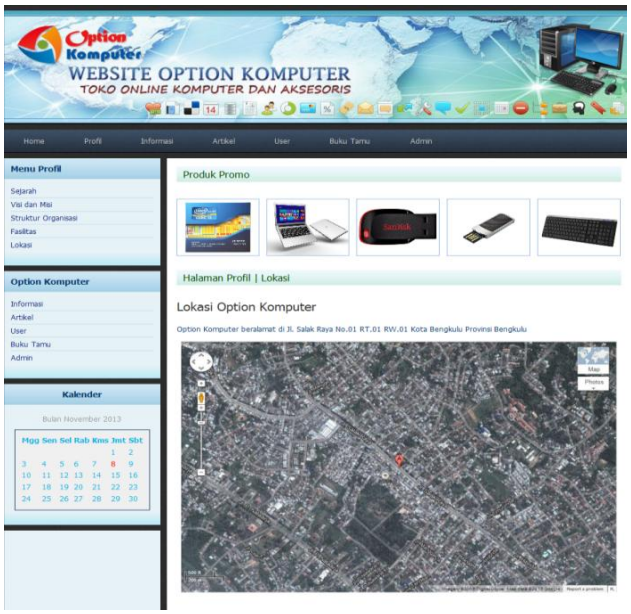
4) Halaman Fasilitas

Halaman fasilitas menampilkan fasilitas-fasilitas yang disediakan oleh Option Komputer untuk member pelayanan prima kepada pelanggan melalui fasilitas seperti pemberian bonus, diskon, diterapkan-nya sistem dropship, sistem COD (*cash on delivery*) dan garansi toko.

Gambar 11. Halaman Fasilitas

5) Halaman Lokasi

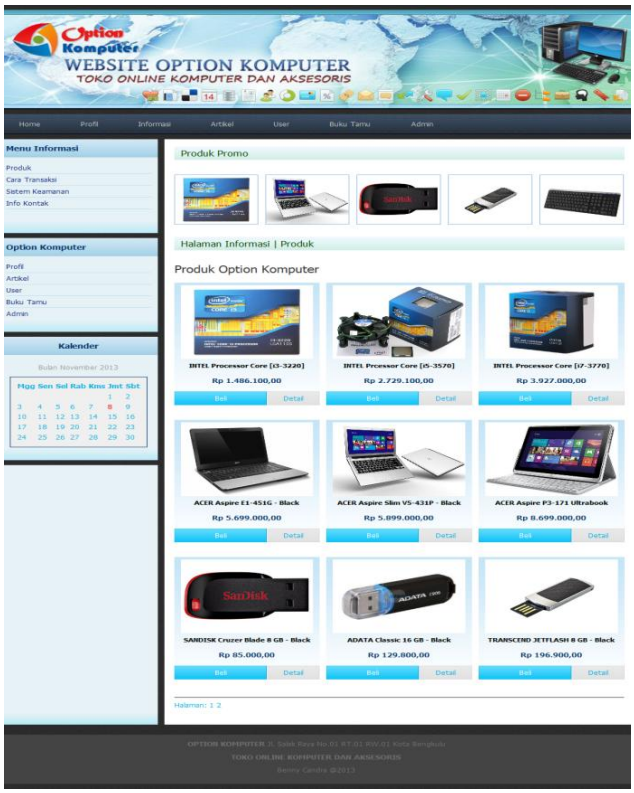
Halaman lokasi merupakan halaman yang berfungsi untuk menampilkan alamat dari toko Option Komputer beserta peta google map. Halaman lokasi ini untuk mempermudah pelanggan baru dalam mencari lokasi toko Option Komputer. Data lokasi ini dapat diperbarui melalui halaman admin. Adapun tampilan halaman lokasi Option Komputer dapat dilihat pada Gambar 12.



Gambar 12. Halaman Lokasi

6) Halaman Informasi

Halaman informasi berguna untuk menampilkan produk-produk yang dijual di toko Option Komputer seperti pada Gambar 14.



Gambar 13. Halaman Informasi Produk

B) Pembahasan

1) Pengolahan Data dan Informasi

Website Toko Option Komputer merupakan *webstore* atau web penjualan yang digunakan sebagai media transaksi jual beli online. Website Toko

Option Komputer merupakan web dinamis dimana data maupun informasi yang ditampilkan dapat diperbaharui. Informasi pada website ini disimpan pada database yang dapat diolah sesuai kebutuhan.

Uraian profil yang meliputi sejarah, visi dan misi, struktur organisasi maupun fasilitas beserta informasi yang meliputi data produk, artikel, buku tamu, manajemen user dan admin merupakan hasil pengolahan data menggunakan PHP dan database MySQL. Beberapa proses pengolahan data yang digunakan antara lain adalah.

a) Koneksi Database

Sebelum dapat dilakukan pengolahan data, dilakukan terlebih dahulu proses koneksi antara halaman web dengan database MySQL. Ada empat parameter dasar yang perlu disetting dalam koneksi database yaitu *host*, *username, password* dan *database*. Server database atau *host* adalah komputer database server, pada pengguna web lokal, parameter *host* ini diinputkan dengan *localhost* yang berarti *host* lokal yang berasal dari komputer tersebut bukan dari remote komputer. *Username* dan *password* adalah informasi aku database MySQL, defaulnya adalah *username root* dan *password* kosong. Parameter *database* diinputkan dengan nama database yang hendak dikoneksikan dengan web.

Skrip berikut adalah kode yang digunakan untuk mengkoneksikan antara web Toko Option Komputer dengan database MySQL.

```
<?php
$my['host']= "localhost";
$my['user']= "root";
$my['pass']= "";
$my['db']   = "tokoonlinedb";
$koneksi    = mysql_connect
($my['host'],$my['user'],
$my['pass']);
if (! $koneksi) {
      echo "koneksi gag-
al".mysql_error();
}
mysql_select_db($my['db'])
or die ("database tidak
ada".mysql_error());
?>
```

Perintah koneksi ke database MySQL adalah $koneksi = mysql_connect ($my['host'],$my['user'],$my['pass']); apabila koneksi berhasil maka variabel $koneksi akan bernilai true dan koneksi berhasil dilakukan, apabila koneksi gagal, maka varibael $koneksi akan bernilai false yang berarti koneksi gagal, pada kondisi ini pada *browser* akan ditampilkan pesan peringatan "koneksi gagal" atau "database tidak ada" sesuai dengan faktor yang menyebabkan gagalnya koneksi.

b) Penyimpanan Data

Penyimpanan data merupakan bagian dari proses pengolahan data yang berfungsi untuk menyimpan data-data yang di perlukan oleh website Toko Option Komputer ke dalam database MySQL. Input data sebagian dilakukan oleh admin pada menu admin. Adapun user melakukan input data pada proses pendaftaran dan input buku tamu. Penyimpanan data dapat dilakukan setelah berhasil melakukan koneksi ke database MySQL.

Sintak yang digunakan untuk menyimpan data ke database MySQL adalah sebagai berikut.

```
mysql_query("INSERT INTO
".$tbl."VALUES
(".$hval.") ")or die(mysql_error());
```

Pada kode di atas, $tbl adalah variabel yang menampung nama tabel yang hendak disimpan, sedangkan variabel $hval adalah nilai atau data dari field-field yang terdapat pada tabel tersebut. Proses penyimpanan data dalam web Toko Option Komputer diimplementasikan pada menu admin bagian input data, untuk user penyimpanan data dapat dijumpai pada proses transaksi dan input buku tamu.

c) Pengubahan Data

Proses pengubahan data sama seperti proses penyimpanan data, namun data yang disimpan bukan data baru, melaikan data hasil perbaikan data lama. Sintak pengubahan data adalah sebagai berikut.

```
mysql_query("DELETE    FROM    ".$tbl."
WHERE
".$kf."='$kd'")or die(mysql_error());
mysql_query("INSERT INTO
".$tbl."VALUES
 (".$hval.") ")or die(mysql_error());
```

Kode program ubah data sama seperti penyimpanan data, hanya saja sebelum data disimpan, data lama dihapus terlebih dahulu dengan perintah "DELETE", dimana variabel $kf adalah nama field referensi dan $kd adalah variabel yang berisi nilai referensi, sehingga data yang akan dihapus adalah yang memenuhi kriteria dimana data *field* $kf di dalam database sama dengan nilai $kd.

d) Pencarian Data

Proses pencarian data merupakan salah satu proses pada pengolahand data yang bertujuan untuk mencari data tertentu pada database MySQL dengan nilai referensi tertentu. Pada web Toko Option Komputer proses pencarian data terlihat pada halaman detail, dimana informasi produk dicari berdasarkan referensi kode produk yang dikirim dari halaman produk pada saat mengklik tombol detail. Sintak pencarian data adalah sebagai berikut.

```
$q=mysql_query("SELECT * FROM ".$tbl."
WHERE ".$kset."='".$set."' ORDER BY
".$ktbl." ASC");
$nval = mysql_num_rows($q);
```

Variabel $tbl merupakan nama tabel, $kset adalah nama field referensi pencarian data, $set adalah variabel yang menyimpan data yang hendak dicari, adapun $ktbl adalah field kunci tabel tersebut. Keterangan kode di atas cari data dari tabel $tbl dimana field $kset memiliki data yang sama dengan $set diurutkan berdasarkan field $ktbl. Hasil pencarian disimpan pada variabel $q.

e) Penghapusan Data

Proses penghapusan data dilakukan untuk menghapus data yang tidak diperlukan dalam sistem atau menghapus data yang salah atau tidak sesuai. Kode penghapusan data adalah sebagai berikut.

```
mysql_query("DELETE FROM ".$tbl."
WHERE
".$kf."='$kd'")or die(mysql_error());
```

Proses hapus data ini diperlukan seperti pada proses hapus data produk, hapus profil dan hapus data history transaksi.

f) Sistem Keamanan berbasis AES

Sistem keamanan pada web Toko Option Komputer diimplementasikan pada saat pendaftaran user dan login baik login user maupun login admin. Prosedur keamanan yang diterapkan adalah web mengirim kode verifikasi yang dihasilkan secara acak. Kode verifikasi ini kemudian diinputkan ke program *AES Security System* yang dikembangkan menggunakan enkripsi AES. Hasil enkripsi program berupa kode keamanan yang diinputkan kembali ke web. Kode keamanan ini harus sesuai dengan profil user atau admin agar dapat berhasil melakukan login.

Kode atau skrip program login dengan implementasi sistem keamanan berbasis enkripsi AES (*Advanced Encryption Standard*) adalah sebagai berikut.

```
$username = $_POST['username'];
$password = $_POST['password'];
$verifikasi = $_POST['verifikasi'];
$security = $_POST['security'];
require_once('aes128.php');
$key=$aes-
>makeKey("*optionkomputer*");
$kd_user = $data-
>kdfieldsetadv('user', 'kd_user',
'kd_user', 'username', $username,
'password', $password);
$dbsecurity = $data-
>kdfield('user','kd_user',$kd_user,'se
curity');
$saes = $aes-
>fromHexString($dbsecurity);
$cpt=$aes->blockDecrypt($saes,$key);
$gab =
substr($cpt,0,10).substr($verifikasi,0
,6);
$ct=$aes->blockEncrypt($gab,$key);
$dbsecurity = $ct;
if (($kd_user <> '') and ($security ==
$dbsecurity)) {
session_start();
$_SESSION['suser'] = $kd_user;
$s = 'location:?h=u_transaksi&n=5';
header($s);
```

Tahap pertama adalah mengambail data-data login yang meliputin data *username*, *password*, kode verifikasi dan kode keamanan. Selanjutnya memanggil library enkripsi AES (*Advanced Encryption Standard*) yaitu file aes128.php dengan perintah require_once('aes128.php'). Tahap berikutnya adalah menginputkan *password* AES, dalam penelitian ini digunakan *password*"*optionkomputer*" password ini diinputkan ke modul sistem keamanan AES dengan perintah aes->makeKey("*optionkomputer*") hasilnya disimpan dalam variabel $key.

Setelah input *password* kemudian memanggil kode user dari database dengan perintah $kd_user = $data->kdfieldsetadv('user', 'kd_user', 'kd_user', 'username', $username, 'password', $password); dilanjutkan dengan memanggil kode keamanan dengan perintah $dbsecurity = $data->kdfield('user','kd_user',$kd_user,'security').

Langkah penting selanjutnya adalah deskripsi kode keamanan dari database untuk disesuaikan dengan kode keamanan dari proses login. Apabila kode keamanan hasil deskripsi sesuai maka proses login berhasil dilakukan dan dilanjutkan dengan mengaktifkan sesi menu user atau menu admin sesuai dengan proses login yang dilakukan. Kode pengaktifan sesi adalah sebagai berikut.

V. PENUTUP

A) Kesimpulan

Website Toko Online Toko Option Komputer yang dilengkapi dengan sistem keamanan berbasis Kriptografi AES dapat dikembangkan dengan menggunakan bahasa pemrograman *web* PHP dan database *MySQL*.

Sistem Keamanan berbasis Kriptografi AES dapat berjalan dengan baik dalam menjaga sistem login sehingga hanya dapat dilakukan pada komputer tertentu yang telah ditetapkan pada saat pendaftaran pelanggan.

Sistem Keamanan pada website Toko Online Option Komputer dapat meningkatkan keamanan

serta kenyamanan pelanggan Option Komputer dalam melakukan transaksi online.

B) Saran

Bagi pihak yang berminat terhadap sistem keamanan untuk toko online menggunakan metode keamanan atau metode kriptografi yang lain, melakukan variasi tampilan, penggunaan bahasa pemrograman, database yang berbeda sehingga dapat dihasilkan toko online yang lebih baik.

DAFTAR PUSTAKA

Ariyus, Dony. 2008. *Pengantar Ilmu Kriptografi Teori Analisis dan Implementasi*. Yogyakarta: Penerbit ANDI.

Jogiyanto, 2005. *Analisis Dan Desain System Informasi: Pendekatan Terstruktur Teori Dan Praktek Aplikasi Bisnis*. Yokyakarta:Penerbit ANDI.

Munir, Rinaldi. 2008. *Kriptografi*. Jakarta: Penerbit Informatika.

Riyanto. 2009. *Pengembangan Aplikasi Sistem Informasi Geografis berbasis Desktop dan Web*. Yogyakarta: Penerbit Gava Media.

Simarmata, Janner dan Paryudi, Iman. 2006. *Basis Data*. Yogyakarta: Penerbit ANDI

Supriyanto, Aji. 2007. *Pengantar Teknologi Informasi*. Jakarta: Salemba Infotek.

Susrini, Ni Ketut, 2010. *Cara Gampang Bikin Toko Online*. Jakarta: PT. Grasindo

Suyanto, 2005. *Pengantar Teknologi Informasi untuk Bisnis*. Yogyakarta: Penerbit ANDI