http://ejournal.politeknikmuhpkl.ac.id/index.php/3/issue/view/6

PENGEMBANGAN SISTEM INFORMASI *E-COMMERCE* DENGAN *SECURITY SSL* PADA JANIS'S FOOTWEAR

Sujarwo*

Dosen Fakultas Matematika dan Ilmu Pengetahuan Alam Program Studi Matematika
Universitas Pesantren Tinggi Darul Ulum Jombang
*email : jarwo301@gmail.com

ABSTRACT

E-commerce is one of the business application via the Internet or better known online stores. E-commerce is the application of trade in goods or services via the internet web based. E-commerce provides convenience shoppers to review products even once bought through online. JANIS'S FOOTWEAR is one of the implementations that implement e-commerce. So it is very appropriate if built an online shoe store that can be accessed via the internet. For practically the SSL protocol has been adopted for the protection of data in transit that includes all of the services network using TCP / IP to support the tasks of general application communication between server and client. The results of the research that has been done for the development of the information system of e-commerce with security SSL implement a needs analysis, the aim of the needs analysis is the process of designing a system that is easy to understand so as to enable communication between the developer with the other parties involved with the development of a user's system so it can easy berintraksi (user friendly). E-COMMERCE at JANIS'FOOTWEAR in Madison can be made / designed using the programming language PHP, MySQL database and design editor Macromedia Dreamwever cs3 with SSL security hoping to give more comfort and safety transtraksi purchase.
Keywords: E-Commerce; SSL Security; MD5 encryption

ABSTRAK

E-commerce adalah salah satu penerapan bisnis via internet atau yang lebih dikenal toko online. *E-commerce* merupakan aplikasi perdagangan barang atau jasa berbasis web melalui internet. *E-commerce* memberikan kemudahan pembeli untuk mereview produk bahkan sekaligus membeli melalui online. JANIS'S FOOTWEAR merupakan salah satu dari implementasi yang menerapkan *e-commerce*. Sehingga sangat tepat apabila dibangun toko sepatu online yang bisa diakses melalui internet. Untuk itu protokol SSL praktis telah diadopsi untuk perlindungan data dalam transit yang mencakup semua layanan jaringan yang menggunakan TCP/IP untuk mendukung tugas-tugas aplikasi umum komunikasi antara server dan klien. Hasil penelitian yang telah dilakukan untuk pengembangan sistem informasi e-commerce dengan security SSL menerapkan analisis kebutuhan, Tujuannya dari analisa kebutuhan tersebut adalah proses perancangan sistem yang mudah dimengerti sehingga memungkinkan komunikasi antara *developer* dengan pihak-pihak lain yang terlibat dengan pengembangan sistem *user* sehingga dapat dengan mudah berintraksi *(user friendly)*. E-COMMERCE pada JANIS'FOOTWEAR di Madiun dapat di dibuat/dirancang dengan menggunakan bahasa pemrograman PHP, database MySQL dan desain editor Macromedia Dreamwever cs3 dengan security SSL dengan harapan bisa lebih memberi kenyamanan dan keamanan transtraksi jual beli.
Kata kunci : *E-Commerce;Security SSL ; Enkripsi MD5*

1. PENDAHULUAN

Kemajuan teknologi informasi di Indonesia terutama dalam bidang teknologi informasi memberikan pengaruh besar bagi pengguna sistem informasi di perusahaan. Dalam dunia usaha khususnya bidang pemasaran dan penjualan, internet sebagai media pemasaran yang bersifat global dan Suatu informasi dapat secara mudah dan cepat untuk disebarluaskan dan diperoleh, hal ini memungkinkan para pengusaha menggunakan teknologi internet sebagai suatu bisnis.

E-commerce adalah salah satu penerapan bisnis via internet atau yang lebih dikenal toko online. *E-commerce* merupakan aplikasi perdagangan barang atau jasa berbasis web melalui internet. *E-commerce* memberikan kemudahan pembeli untuk mereview produk bahkan sekaligus membeli melalui online.

JANIS'S FOOTWEAR merupakan salah satu dari implementasi yang menerapkan *e-commerce*, pemilihan sepatu sebagai produk yang diperdagangkan melalui internet dikarenakan tingginya kebutuhan sepatu di semua kalangan. Dengan menggunakan toko online pembeli dapat memperoleh informasi yang lebih detail tentang sepatu termasuk melakukan pemesanan sepatu itu sendiri. Sehingga sangat tepat apabila dibangun toko sepatu online yang bisa diakses melalui internet.

JANIS'S FOOTWEAR merupakan Toko Sepatu yang berorientasi kedepan dalam mengembangkan target pasar dan kualitas pelayanan. Dengan semakin meningkatnya pelanggan baik dari dalam maupun dari luar kota. JANIS'S FOOTWEAR dituntut untuk selalu meningkatkan kualitas pelayanan berupa kemudahan dalam memberikan informasi katalog sepatu dan pemesanan sepatu oleh pelanggannya.

Keamanan data dalam transit melalui Internet menjadi semakin diperlukan karena volume data yang terus tumbuh dan penting. Saat ini setiap pengguna jaringan publik mengirimkan berbagai

jenis data, dari email ke rincian kartu kredit harian, dan karena itu ia ingin mereka harus dilindungi ketika dalam perjalanan melalui jaringan publik. Untuk itu protokol SSL praktis telah diadopsi untuk perlindungan data dalam transit yang mencakup semua layanan jaringan yang menggunakan TCP/IP untuk mendukung tugas-tugas aplikasi umum komunikasi antara server dan klien.

Dari dasar pemikiran diatas, sangat tepat apabila sebuah sistem baru berupa bagaimana mengembangkan sistem informasi E-COMMECE dengan security SSL diterapkan di JANIS'S FOOTWEAR Madiun, guna meningkatkan kualitas pelayanannya.

2. KERANGKA TEORI

2.1 *Tinjauan Pustaka*

A. E-commerce

Banyak istilah mengenai *e-commerce*, ada yang menyebutkan toko online, inventory/penjualan online, *shopping cart*, dan lain-lain. *E-commerce* adalah proses pemesanan produk atau tansaksi jual beli antara pengunjung dengan website.

Alur proses dari sistem *e-commerce* bisa dilihat dari proses jual beli yang sering dijumpai dalam kehidupan sehari-hari. Misalnya saat masuk ke sebuah supermarket, pertama pembeli akan mengambil keranjang belanja dulu yang disediakan oleh pihak supermarket

Proses jual beli di dunia nyata tidak jauh berbeda dengan proses jual beli secara online (*e-commerce*). Perbedaanya pembeli tidak bisa secara langsung memakai barang yang sudah dibeli, sebelum barang tersebut dikirimkan oleh pihak *e-commerce*. *(Lukmanul Hakim, 2009).*

B. Web Server

Web server adalah software yang menjadi tulang belakang dari *world wide web* (www). Web server menunggu permintaan dari client yang menggunakan browser seperti Netscape Navigator, Internet Explorer, Mozilla, dan program browser lainnya. Jika ada permintaan dari browser, maka *web server* akan memproses permintaan itu kemudian memberikan hasil prosesnya berupa data yang diinginkan kembali ke *browser*. Data ini mempunyai format yang standar, disebut dengan format SGML (*standar general markup language*). Data yang berupa format ini kemudian akan ditampilkan oleh browser sesuai dengan kemampuan browser tersebut. Contohnya, bila data yang dikirim berupa gambar, browser yang hanya mampu menampilkan teks (misalnya *lynx*) tidak akan mampu menampilkan gambar tersebut, dan jika ada akan menampilkan alternatifnya saja. Web server, untuk berkomunikasi dengan client-nya (*web browser*) mempunyai protokol sendiri, yaitu HTTP (*hypertext transfer protocol*).

Dengan protokol ini, komunikasi antar *web server* dengan client-nya dapat saling dimengerti dan lebih mudah. Seperti telah dijelaskan diatas, format data pada *world wide web* adalah SGML. Tapi para pengguna internet saat ini lebih banyak menggunakan format HTML (*hypertext markup language*) karena penggunaannya lebih sederhana dan mudah dipelajari. Kata *HyperText* mempunyai arti bahwa seorang pengguna internet dengan *web browser*nya dapat membuka dan membaca dokumen-dokumen yang ada dalam komputernya atau bahkan jauh tempatnya sekalipun. Secara garis besarnya *web server* hanya memproses semua masukan yang diperolehnya dari *web client*nya. *(http://www.*ittelkom*.ac.id/library/index.php?view=article&catid=10%3Ajaringan&id=406%3A-web-server-&option=com_content&Itemid=15, 2010)*

2.2 Dasar Teori

A. SSL *(Secure Socket Layer).*

Salah satu cara untuk meningkatkan keamanan web server adalah dengan menggunakan enkripsi pada komunikasi terhadap tingkat socket. Dengan menggunakan enkripsi, orang tidak bisa menyadap data-data (transaksi) yang dikirimkan dari client ke web server. Dengan kata lain SSL *(Secure Socket Layer).* SSL adalah mekanisme pembungkusan data yang berlalu-lalangantara klien dan serverdengan suatu enkripsi data.

SSL menyediakan keamanan, dan yang lebih penting adalah ketenangan. Dengan menggunakan SSL, kita dapat memastikan bahwa data kita aman dari pihak-pahak yang tidak berhak mengakses. (Dian Rakyat, *Membuat dan Mengelola Web Hosting*, Jakarta 2004)

B. Open SSL

Open SSL adalah sebuah toolkit kriptografi yang mengimplementasikan protokol jaringan Secure Sockets Layer (SSL v2/v3) dan Transport Layer Security (TLS v1).

Termasuk berbagai standar kriptografi lainnya yang di butuhkan. Openssl sendiri adalah program di Linux yang sifatnya command line tidak menggunakan grafik user interface (GUI). (*muchammad.sholeh@gmail.com/sholeh@depkominfo.go.id*)

C. Cara Kerja SSL

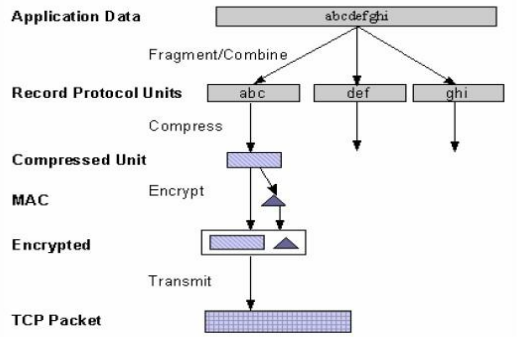
SSL membangun hubungan (connection) yang aman antara dua socket, sehingga pengiriman pesan antara dua entitas dapat dijamin keamanannya. public dengan menggunakan algoritma RSA dan sertifikat digital untuk mengotentikasi server di dalam transaksi san untuk melindungi informasi rahasia yang dikirim antara dua buah socket. Server selalu diotentikasi, sedangkan client tidak harus diotentikasi oleh server.

Server diotentikasi agar client yakin bahwa ia mengakses situs web yang sah (dan bukan situs web palsu yang menyamar seolah-olah benar ia adalah server yang asli.

Client tidak harus diotentikasi oleh server karena kebanyakan server menganggap nomor kartu kredit sudah cukup untuk mengotentikasi client. Perlu dicatat bahwa SSL adalah protokol client-server, yang dalam hal ini web browser adalah client dan website adalah server. Client yang memulai komunikasi, sedangkan server memberi respon terhadap permintaan client.

Protokol SSL tidak bekerja kalau tidak diaktifkan terlebih dahulu (biasanya dengan meng-klik tombol yang disediakan di dalam web server yang diakses oleh client. (http://www.ssl.com. Desember 2006.)

D. Pembungkusan Pesan SSL



Gambar 2.1 Pembungkusan Pesan oleh SSL

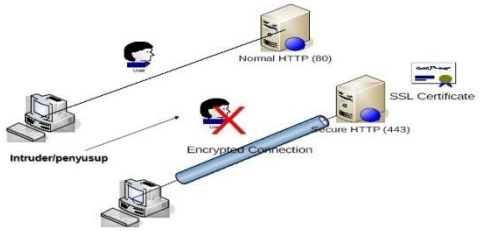
Setelah kanal yang aman terbentuk, client dan server menggunakannya untuk menjalankan sub-protokol kedua (SSL Record) untuk saling berkirim pesan. Misalnya client mengirim HTTP request ke server, dan server menjawab dengan mengirim HTTP response.

Pesan dari client ke server (dan sebaliknya) dikirim dalam bentuk terenkripsi (pesan dienkripsi dengan menggunakan session key). Tetapi, sebelum pesan dikirim dengan TCP/IP, protokol SSL melakukan proses pembungkusan data sebagai berikut:

a. Pesan dipecah menjadi sejumlah blok (fragment) yang masing-masing panjangnya 16KB; setiap blok diberi nomor urut sekuensial.
b. Setiap blok kemudian dikompres,lalu hasil kompresi disambung.
c. kemudian, hasil dari langkah 2 di atas di-hash dengan algoritma MD5.Setelah itu ditambahkan ke setiap blok sebagai MAC (Message Authentication Code).
d. Hasil dari langkah 3 kemudian dienkripsi dengan SSL *(source socket layer).*
e. Terakhir, hasil dari langkah 4 diberi header (2 atau 3 byte), baru kemudian dikirim melalui koneksi TCP/IP aman yang terbentuk sebelumnya.(htpp//informatika/rinaldi.com/ecommerce.pdf)

E. Fungsi SSL

a. Menjamin kerahasiaan dan keutuhan pesan, sehingga tidak bisa dibaca atau di ubah di tengah jalan oleh pihak yang tidak diinginkan.
b. Menjamin keabsahan/keaslian, sehingga meyakinkan pihak-pihak yang berkomunikasi antara client dan server.
c. Meminimalisasi serangan sniffing data.



Gambar 2.2 Ilustrasi Sniffing Data

F. Enkripsi MD5

MD5 adalah salah satu dari serangkaian algortima *message digest* yang didesain oleh Profesor Ronald Rivest dari MIT (Rivest, 1994). Saat kerja analitik menunjukkan bahwa pendahulu MD4 mulai tidak aman,kemudian MD5 didesain pada tahun 1991 sebagai pengganti dari MD4 (kelemahan MD4 ditemukan oleh Hans Dobbertin).

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.

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 digunakan untuk melakukan pengujian integritas sebuah file.(http://kriptografi.multiply.com)

3. METODE PENELITIAN.

Metode yang digunakan dalam penulisan laporan ini adalah sebagai berikut :

a. Pengamatan di Lapangan (*Observasi*)
   Dengan mempelajari secara langsung permasalahan yang terjadi pada JANIS'S FOOTWEAR .
b. Wawancara Langsung (*Interview*)
   Dilakukan untuk mendapatkan informasi mengenai barang- barang yang ada JANIS'S FOOTWEAR dan pelayananya.
c. Studi Pustaka
   Yaitu pengumpulan data dan melakukan studi kepustakaan di Internet untuk mendapatkan

bahan-bahan yang berkaitan dengan laporan ini.

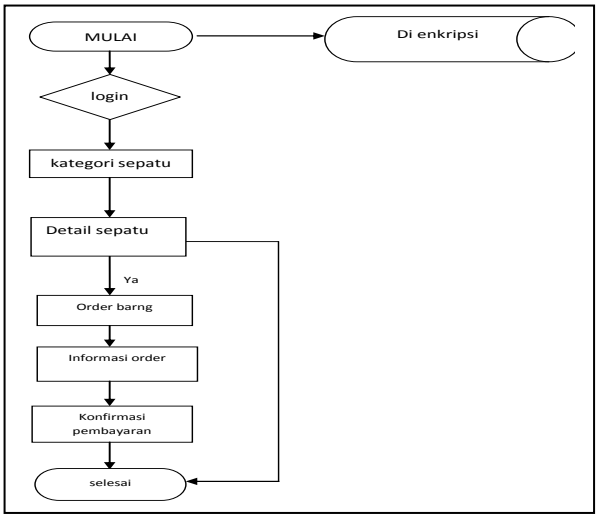
4. HASIL PENELITIAN DAN PEMBAHASAN

4.1 *Hasil Penelitian*

Hasil penelitian yang telah dilakukan untuk pengembangan sistem informasi e-commerce dengan security SSL menerapkan analisis kebutuhan, Tujuannya dari analisa kebutuhan tersebut adalah proses perancangan sistem yang mudah dimengerti sehingga memungkinkan komunikasi antara *developer* dengan pihak-pihak lain yang terlibat dengan pengembangan sistem *user* sehingga dapat dengan mudah berintraksi *(user friendly)*.

Setelah melakukan riset bagaimana sistem transaksi yang telah dijalankan oleh pihak JANIS'S FOOTWEAR, maka penulis melakukan pendekatan secara umum untuk memenuhi kebutuhan tersebut. Penulis mempunyai ide atau solusi yang akan diterapkan untuk sistem ini dengan tujuan memberikan gambaran secara umum melalui suatu relasional basis data sehingga mempermudah dalam perancangan dan implementasi

4.1.1 Flow Chart Transaksi yang Di Ekripsi Oleh SSL



Gambar 4.1 Flow Chart Transaksi yang di Enkripsi dengan SSL

Dari Flow Chart Pembeli diatas maka dapat dijelaskan sistem alur kerja dari toko sepatu online tersebut, sebagai berikut :

1. Pertama member membuka browser,kemudian melakukan login, dan data login itu telah di enkripsi oleh SSL.
2. Pembeli akan dihadapkan pada halam index yang berisi: kategori sepatu.
3. Jika pembeli mengklik sepatu terbaru, maka akan muncul detail sepatu disertai tombol pemesanan yang bila diklik akan menuju ke halaman pemesanan.
4. Pada halaman keranjang belanja daftar belanja akan ditampilkan kembali.Setelah pembeli menyelesaikan semua proses pemesanan.
5. Setelah pembeli menyelesaikan semua proses pemesanan, maka sebuah e-mail yang isinya daftar belanjaan akan dikirim secara otomatis ke alamat pembeli sebagai bukti pemesanan.
6. Setelah pembeli melakukan transfer uang ke bank, maka pembeli harus mengisi konfirmasi pembayaran sebagai bukti bahwa pembeli sudah membayar.

4.2 Pembahasan

Implementasi sistem yang akan dibahas adalah mengenai gambaran desain halaman (*user interface*) dan form-form yang terdapat dalam sistem informasi ini dengan tujuan agar mudah dimengerti dan dipelajari oleh pengguna,Data flow diargram tersebut menggambarkan tentang alur perpindahan dan proses yang melibatkan data-data yang dibutuhkan oleh sistem, proses tersebut adalah:

1. *Proses insert member*, proses ini dilakukan oleh administrator, data yang diinputkan adalah data detail member yang kemudian disimpan dalam file, file ini akan digunakan member untuk login sebagai member.
2. *Login Member*, sebagai upaya otientikasi dan keamanan, proses ini berperan penting untuk memberikan izin kepada member, member adalah pelanggan yang terdaftar. Apabila data pengguna ditemukan dan sesuai dengan file, maka akan dilanjutkan melihat kategori sepatu.
3. *Proses Input* sepatu, seluruh data-data yang berkaitan dengan sepatu. Proses ini dilakukan oleh administrator, kemudian data sepatu akan digunakan pada proses lihat detail sepatu oleh member.
4. *Proses order*, dilakukan oleh member yang telah login dengan benar, proses ini menggunakan data-data sepatu sebagai sumber informasi utama. Informasi yang diberikan berdasarkan kategori sepatu.
5. *Order* sepatu, apabila ada sepatu yang dikehendaki oleh member, maka member melakukan order sepatu itu.
6. *Konfirmasi Order*, proses ini digunakan untuk mengakhiri proses order. Dalam proses ini akan ditampilkan jumlah sepatu dan harga yang telah di order.

5. KESIMPULAN

Berdasarkan penelitian dan pembahasan mengenai pemecahan masalah di JANIS'S FOOTWEAR, maka penulis dapat menyimpulkan sebagai berikut: E-COMMERCE pada JANIS'FOOTWEAR di Madiun dapat di dibuat/dirancang dengan menggunakan bahasa pemrograman PHP, database MySQL dan desain editor

Macromedia Dreamwever cs3 dengan security SSL dengan harapan bisa lebih memberi kenyamanan dan keamanan transtraksi jual beli.

Daftar Pustaka

Dian Rakyat, *Membuat dan Mengelola Web Hosting*, Jakarta 2004)

Jeffery L, dkk. 2004. *Metode Desain dan Analisis Sistem.* Edisi 6. Yogyakarta: Penerbit Andi.

Lukmanul Hakim,*2009. Transaksi jual Beli berbasis E-Commerce dalam sistem Hukum Indonesia, Jakarta*

Puspitosari, *Heni.2011.Pemrograman Web Database dengan PHP dan MySQL, Yogyakarta: Skripta Media Creative muchammad.sholeh@gmail.com/sholeh@depkiimfo.go.id*

*http://www.*ittelkom.*ac.id/library/index.php?view=article&catid=10%3Ajaringan&id=406%3Aweb-server-&option=com_content&Itemid=15, 2010)*
file.(http://kriptografi.multiply.com)