

IMPLEMENTASI APLIKASI WEBSITE E-COMMERCE BATIK SUNDA DENGAN MENGGUNAKAN PROTOKOL SECURE SOCKET LAYER (SSL)

Dewi Rosmala^[1], M. Djalu Djatmiko^[2], Budiman Julianto^[3]

Jurusan Teknik Informatika

Jurusan Desain Produk

Intitut Teknologi Nasiona ITENAS Bandung

ABSTRAK

Berdasarkan riset yang dilakukan oleh MarkPlus Insight Jika di tahun 2010 lalu rata-rata penetrasi penggunaan Internet di kota urban Indonesia 30% - 35%, di tahun 2011 ini ditemukan bahwa angkanya sudah di kisaran 40% - 45%. Hasil riset, yang dirilis oleh Majalah Marketeers ini, dilakukan oleh MarkPlus Insight terhadap 2161 pengguna Internet di Indonesia memberikan gambaran jelas mengenai tren penggunaan Internet di Indonesia. Menurut MarkPlus Insight, jumlah pengguna Internet di Indonesia pada tahun 2011 ini sudah mencapai 55 juta orang, meningkat dari tahun sebelumnya di angka 42 juta. Dari hasil riset ini dapat dilihat bahwa pengguna internet yang cukup banyak berpotensi dalam penggunaan e-commerce seperti internet banking, penjualan online dan lain sebagainya. Batik merupakan komoditi yang mencirikan kebudayaan bangsa Indonesia. Batik Sunda banyak menyerap pengaruh dari lingkungan sekitarnya, terutama Jawa Tengah, serta negara lain, seperti Arab, India, dan China. Corak, ragam, dan motif batik provinsi ini berjumlah lebih dari 3.000 jenis. Ini merupakan potensi pasar yang menguntungkan. Namun timbul permasalahan mengenai keamanan jaringan dan kebutuhan akan keamanan informasi pada website e-commerce menjadi sangat penting untuk menjaga kerahasiaan data user maupun perusahaan. Pengimplementasian SSL pada Website E-Commerce merupakan salah satu cara mengamankan data yang ada pada setiap transaksi yang dilakukan user dan input data oleh admin. HTTP over SSL atau yang biasa diimplementasikan dengan HTTPS merupakan protokol HTTP yang menggunakan Secure Socket Layer (SSL) sebagai sublayer dibawah HTTP sehingga keamanan lebih terjamin. Pembuatan sertifikat ini menggunakan OpenSSL 1.0.1 yang merupakan software untuk menginstal sertifikat keamanan pada website.

Kata Kunci : SSL, E-Commerce, HTTPS, OpenSSL 1.0.1.

ABSTRACT

Based on research conducted by Insight MarkPlus, in 2010 the average penetration of internet usage in the urban city of Indonesia was 30% - 35%, in the year 2011 it was found that the score was in the range 40%-45%, Research results released by the magazine Marketeers, conducted by Mark Plus Insight of 2161 internet users in Indonesia, provided a clear picture of Internet usage trends in Indonesia. According Mark Plus Insight, the number of Internet users at Indonesia in the year 2011 has reached 55 million people, an increased from previous years which reached 42 million. From the results of this research could be seen Internet users that quite a lot of potential in the use of e-commerce such as Internet banking, online sales, etc. Batik is a commodity that characterizes the culture of Indonesia. Sundanese's Batik absorb influences from the surrounding environment, especially in Central

Java, as well as other countries, such as Saudi, India, and China. The style, variety, and the motif of the province amounted to more than 3,000 species. This is a potential lucrative market. However, problems occur regarded the need for network security and information security in e-commerce website to be very important for maintained the confidentiality of user data as well as companies. Implementing SSL on E-Commerce Website is one way of securing data on every transaction made by the user and input data by admin. HTTP over SSL or HTTPS that usually implemented with an HTTP protocol that uses the Secure (SSL) as a sub layer under HTTP so that safety is more assured. Preparation of this certificate used OpenSSL 1.0.1 which is the software to install a security certificate on the website.

Keywords : *SSL, E-Commerce, HTTPS, OpenSSL 1.0.1.*

PENDAHULUAN

Latar Belakang

Dunia bisnis telah memanfaatkan *website* sebagai tempat jual beli di internet dengan metode *e-commerce*. Namun kebutuhan terhadap keamanan informasi yang ada pada *website* menjadi penting dan timbul permasalahan mengenai keamanan jaringan.^[1]

Perkembangan teknologi yang semakin pesat mengakibatkan kebutuhan terhadap keamanan informasi yang ada pada *website* menjadi penting dan timbul permasalahan baru mengenai keamanan jaringan, contoh ancaman keamanan jaringan yang sering terjadi adalah pengendusan aktivitas di jaringan atau biasa disebut *sniffing*.^[4]

Pengimplementasian SSL pada *Website E-Commerce* merupakan salah satu cara mengamankan data yang ada di dalam setiap transaksi yang dilakukan user dan input data oleh admin. HTTP over SSL atau yang biasa diimplementasikan dengan HTTPS merupakan protokol HTTP yang menggunakan *Secure Socket Layer* (SSL) sebagai sublayer dibawah HTTP sehingga keamanan lebih terjamin. Pembuatan aplikasi ini menggunakan OpenSSL 1.0.1 yang merupakan software untuk menginstal sertifikat keamanan pada *website*.

Rumusan Masalah

Berdasarkan latar belakang yang telah dikemukakan, maka rumusan masalahnya adalah Bagaimana mengimplementasikan *Secure Socket*

Layer (SSL) pada aplikasi *e-commerce* batik sunda dan bagaimana melakukan pengamanan data pelanggan, data transaksi dan *e-commerce* batik sunda?

Tujuan

Tujuan dalam penelitian ini adalah mengimplementasikan *Secure Socket Layer* (SSL) pada aplikasi *website e-commerce* batik sunda agar data user dan data transaksi terjaga kerahasiaannya.

Batasan Masalah

Batasan permasalahan yang dirumuskan, antara lain :

- a. Pengamanan aplikasi ini menggunakan enkripsi SSL 1024 bits.
- b. Pengamanan informasi aplikasi *e-commerce* batik sunda : data login, data user, data produk, data transaksi.
- c. Pengujian aplikasi dilakukan pada server lokal.

Metodologi Penelitian

Metodologi penelitian yang digunakan penulis dalam penulisan tugas akhir ini adalah sebagai berikut :

1. Tahap pengumpulan data

Metode pengumpulan data yang digunakan dalam penelitian tugas akhir ini adalah sebagai berikut :

- a. Studi *literature*

Pengumpulan data dengan cara mengumpulkan *literature, paper* artikel, buku dan bacaan-bacaan yang ada kaitannya dengan judul penelitian.

- b. Observasi

Teknik pengumpulan data dengan mengadakan penelitian dan peninjauan

langsung terhadap permasalahan yang diambil.

c. Interview

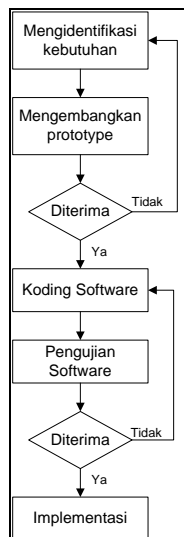
Teknik pengumpulan data dengan mengadakan tanya jawab secara langsung yang ada kaitannya dengan topik yang diambil.

2. Tahap pembuatan perangkat lunak

Metodologi pengembangan sistem yang digunakan adalah prototype. Metodologi prototype merupakan metode yang menyajikan gambaran yang lengkap tentang sistemnya, pemesan dapat melihat pemodelan sistem dari sisi tampilan maupun teknik procedural yang akan dibangun.

Tahap pertama adalah pembuatan prototype dari sistem yang akan dibuat. Lalu prototype tersebut akan diperlihatkan kepada user. Apabila prototype tersebut diterima user, maka prototype tersebut akan dikembangkan.

Tahap kedua adalah pembangunan sistem. Jika sebuah prototype telah diterima dan disetujui oleh user, maka prototype tersebut akan dikembangkan menjadi sebuah sistem sesungguhnya. Sebelum pembangunan sistem dilakukan, terlebih dahulu dilakukan proses perancangan.



Gambar 1. Metodologi Prototype

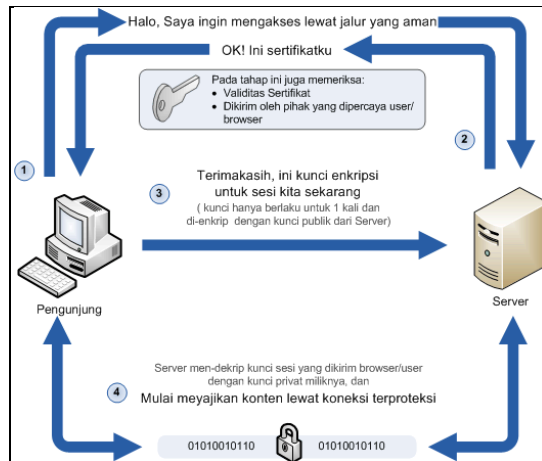
DASAR TEORI

Pengenalan E-Commerce^[1]

Electronic Commerce (*e-Commerce*) adalah proses pembelian, penjualan atau pertukaran produk, jasa dan informasi melalui jaringan komputer. *e-Commerce* merupakan bagian dari *e-business*, ruang lingkup *e-business* lebih luas, tidak sebatas perniagaan tetapi mencakup juga pengkolaborasian mitra bisnis, pelayanan nasabah, lowongan pekerjaan dan lain-lain. Selain teknologi jaringan *www*, *e-Commerce* juga memerlukan teknologi basis data atau pangkalan data (*database*), *e-surat* atau surat elektronik (*e-mail*), dan bentuk teknologi non komputer yang lain seperti halnya sistem pengiriman barang, dan alat pembayaran untuk *e-Commerce* ini.

Secure Socket Layer (SSL)^[6]

Secure Socket Layer adalah protokol khusus atau jalur khusus yang lebih aman pada website dimana semua transaksi data yang menggunakan protokol tersebut akan di enkripsi. Teknologi SSL menggunakan konsep teknologi kriptografi kunci publik untuk bisa mencapai komunikasi yang aman ini antara server dan pengunjungnya. Kedua pihak yang berkomunikasi ini (server dan pengunjungnya) saling mengirimkan data yang disamarkan dan untuk membacanya digunakan sandi dan kunci yang hanya dimiliki kedua pihak yang berkomunikasi tersebut, sehingga pihak lain yang mencoba menyadap data yang dikirim tersebut tidak akan bisa membacanya karena sandi dan kunci yang dibutuhkan tersebut hanya dimiliki oleh kedua pihak yang berkomunikasi.



Gambar 2. Cara Kerja SSL

Jenis SSL yang paling aman dapat dilihat dari tingkat keamanan SSL, yang terletak pada kekuatan enkripsi yang didukungnya (misalnya 256 bit). Semakin besar tingkat enkripsi semakin susah untuk dibobol. Secara teknis, semua SSL dengan tingkat enkripsi yang sama, mempunyai tingkat keamanan yang sama.

Komponen Secure Socket Layer (SSL)^[3]

Komponen SSL disusun oleh dua sub-protokol :

1. SSL handshaking, yaitu sub-protokol untuk membangun koneksi yang aman untuk berkomunikasi.
2. SSL record, yaitu sub-protokol yang menggunakan koneksi yang sudah aman. SSL record membungkus seluruh data yang dikirim selama koneksi.

ANALISIS DAN PERANCANGAN

Identifikasi Kebutuhan

Metode pengembangan aplikasi *e-commerce* menggunakan metodologi *prototype*. Proses awal *prototype* dimulai dengan mengidentifikasi kebutuhan apa saja yang diperlukan aplikasi *e-commerce* tersebut. Melakukan identifikasi masalah yang ada dilapangan, hal apa saja yang dibutuhkan dalam membangun sebuah aplikasi *e-commerce* :

a. Manajemen User

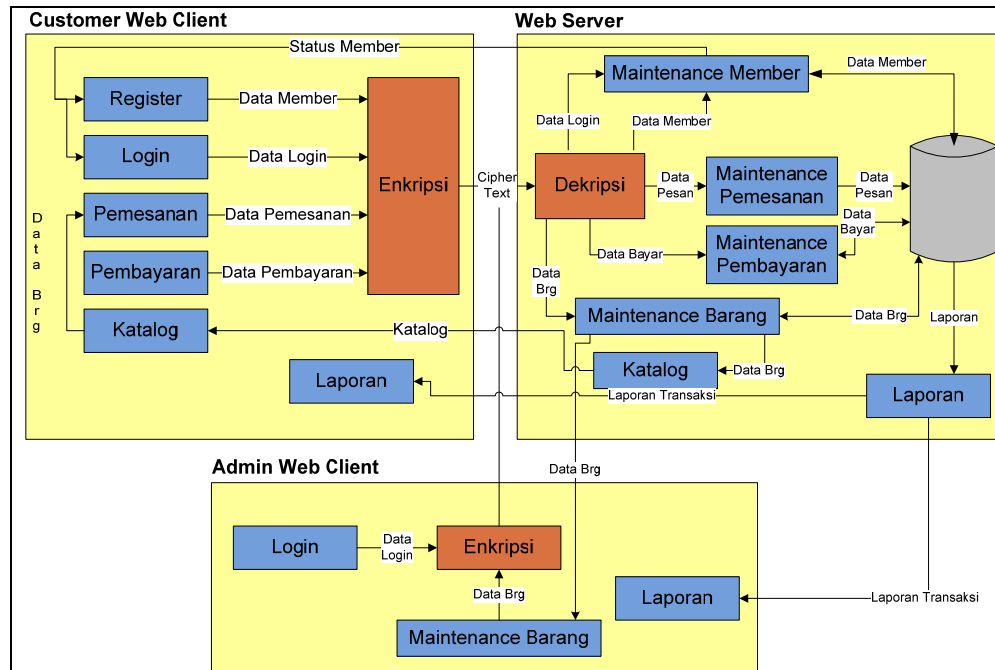
- b. Manajemen Produk
- c. Manajemen Orders
- d. Manajemen Pembayaran
- e. Manajemen Pengiriman
- f. Manajemen Kategori
- g. Manajemen Website

Pengembangan *Prototype* (Perancangan)

Dari identifikasi masalah diperoleh suatu model untuk melakukan pengembangan aplikasi *e-commerce*. kemudian *prototype* tersebut akan diperlihatkan kepada user. Pembangunan sistem pada metodologi jika sebuah *prototype* telah diterima dan disetujui oleh user, maka *prototype* tersebut akan dikembangkan menjadi sebuah sistem sesungguhnya. Sebelum pembangunan sistem dilakukan, terlebih dahulu dilakukan proses perancangan. Dalam proses ini juga dilakukan presentasi kepada user mengenai sistem yang telah dibuat. Jika sistem telah memenuhi kebutuhan dan disetujui user.

Blok Diagram Arsitektur Sistem

Sistem website *e-commerce* ini dapat diakses oleh user yaitu admin dan member. Untuk admin ia harus login terlebih dahulu, Setelah login maka dapat melakukan proses maintenance barang dan menerima laporan. Semua data yang masuk ke web server akan di enkripsi terlebih dahulu di enkripsi sebelum dikirim ke web server dan setelah tiba di server akan di dekripsi agar diproses, sehingga aliran data yang diproses oleh webserver akan aman dan terjamin kerahasiaannya. Web server akan melakukan maintenance semua aktifitas data yang keluar masuk pada *database*. Dengan menggunakan sertifikat SSL diharapkan data yang diproses oleh *database* tidak dapat di manipulasi maupun diganggu gugat oleh pihak lain yang tidak bertanggungjawab.



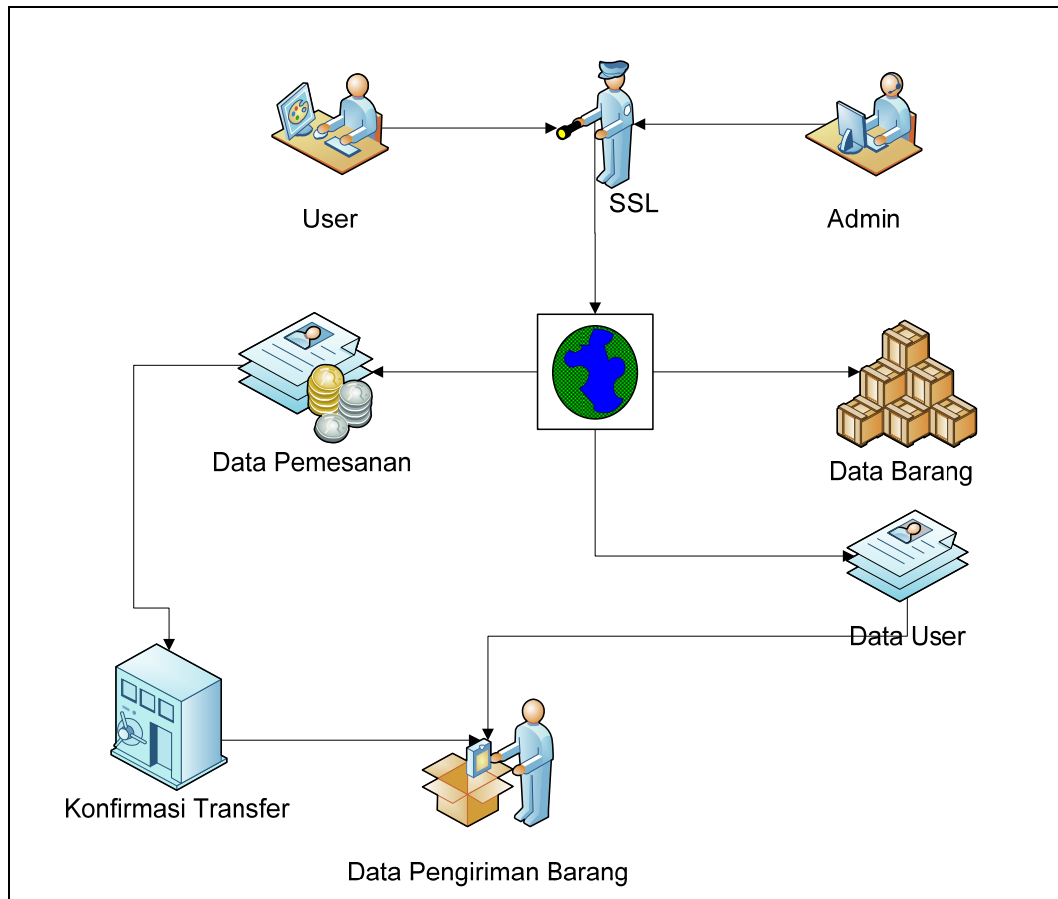
Gambar 3. Blok Diagram Arsitektur Sistem

Pada Gambar 3 merupakan gambaran secara umum data yang diamankan oleh sertifikat SSL, pada saat penginputan data yang dilakukan oleh user dan admin terlebih dahulu harus melewati sertifikat SSL, sehingga setiap aliran *database* tidak dapat di *sniffing* oleh pihak lain maupun user dan admin karena telah di enkripsi terlebih dahulu. Data yang diamankan pada user adalah register, login, pemesanan dan pembayaran. Setiap data akan diproses pada aplikasi *e-commerce* melalui login yang sah dilakukan oleh admin maupun kustomer. Data user akan memproses data kustomer yang akan melakukan pemesanan dan pembelian. Data produk akan memproses informasi produk yang tersedia pada aplikasi *e-commerce*. Data pemesanan akan memproses pemesanan yang dilakukan oleh kustomer. Data pembayaran akan memproses konfirmasi pembayaran yang telah dilakukan kustomer pada saat melakukan pemesanan. Data pengiriman akan memproses alamat pengiriman kustomer setelah kustomer melakukan konfirmasi pembayaran. Dengan menggunakan sertifikat SSL diharapkan data yang diproses oleh *database* tidak

dapat di manipulasi maupun diganggu gugat oleh pihak lain yang tidak bertanggungjawab karena data tersebut telah di enkripsi.

Pengamanan Data Dengan SSL Pada Aplikasi E-Commerce

Setiap interaksi yang di lakukan oleh admin dan user akan di enkripsi terlebih dahulu oleh *Secure Socket Layer* (SSL). Data yang di amankan oleh SSL 1024 bits ini adalah : data user, data barang, data order, dan data pengiriman. Setelah menggunakan setifikat SSL maka data yang akan di proser oleh web server akan terjaga kerahasiaannya.



Gambar 4. Pengamanan Data SSL pada Aplikasi E-Commerce

Pada Gambar 7 merupakan gambaran secara umum data yang diamankan oleh sertifikat SSL, pada saat penginputan data yang dilakukan oleh user dan admin terlebih dahulu harus melewati sertifikat SSL, sehingga setiap aliran *database* tidak dapat di *sniffing* oleh pihak lain maupun user dan admin. Data yang diamankan adalah data user, data produk, data pemesanan, data pembayaran dan data pengiriman. Setiap data akan diproses pada aplikasi *e-commerce* melalui login yang sah dilakukan oleh admin maupun kustomer. Data user akan memproses data kustomer yang akan melakukan pemesanan dan pembelian. Data produk akan memproses informasi produk yang tersedia pada aplikasi *e-*

commerce. Data pemesanan akan memproses pemesanan yang dilakukan oleh kustomer. Data pembayaran akan memproses konfirmasi pembayaran yang telah dilakukan kustomer pada saat melakukan pemesanan. Data pengiriman akan memproses alamat pengiriman kustomer setelah kustomer melakukan konfirmasi pembayaran.

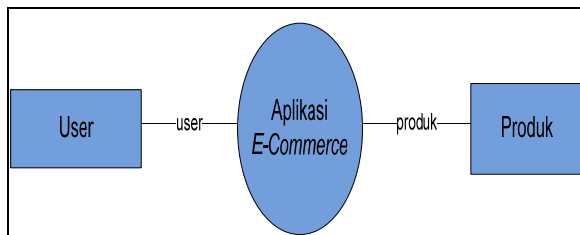
Workflow Sistem

Pada sistem informasi pemesanan barang berbasis web ini terbagi menjadi 2 bagian yaitu staff atau sebagai admin dan customer sebagai pelanggan Batik. Maka dari kedua bagian ini memiliki peran masing-masing sebagai berikut :

1. Staff/admin : pada aplikasi ini staff harus melakukan login terlebih dahulu untuk menjaga keamanan data-data customer. Jika staff berhasil login sebagai admin maka staff hanya dapat melakukan insert, update, dan delete data customer dan data pemesanan yang dilakukan pelanggan.
2. Customer/Pelanggan : di aplikasi ini customer dapat melakukan pemesanan barang maupun jasa. Dan dapat melihat info-info baru seputar produk-produk yang ditawarkan oleh pemilik batik.

Data Flow Diagram (DFD)

Pada aplikasi ini Pelanggan akan memasukkan data diri sebagai pelanggan tetap pada sistem kemudian sistem akan memberikan informasi seputar produk yang dipesan oleh pelanggan. Setiap proses dapat di turunkan sebagai berikut, Pertama admin dapat melakukan input data produk yaitu insert, update, dan delete dan diproses oleh sistem pengolahan data produk dan tagihan yang nantinya akan tersimpan kedalam database. Dan untuk Pelanggan dapat melakukan input data sebagian yang diperlukan di form untuk melihat laporan tagihan produk.



Gambar 5. Diagram Konteks

Desain Sistem Informasi *E-commerce* berbasis Web

Secara keseluruhan aplikasi *e-commerce* terdiri dari 15 form. Dari ke-15 form dikelompokkan berdasarkan kesamaan desain, yaitu form utama, form user, dan form login. Berikut adalah desain layout dari aplikasi *e-commerce* :

a. Form Login

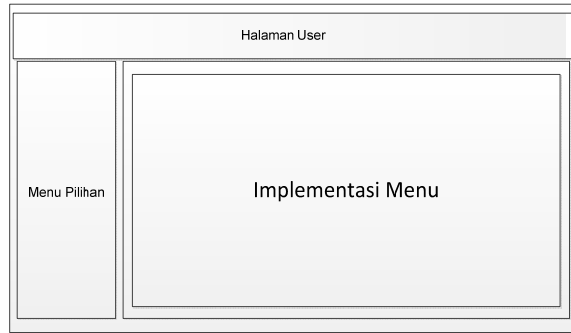
Gambar 6. Desain Layout Form Login

b. Form Utama

Gambar 7. Desain Layout Form Utama

Desain form utama pada bagian menu terdapat tombol untuk mengakses form-form yang tersedia. Di bagian kiri terdapat form login, kategori dan produk favorit. Di bagian tengah

c. Form User

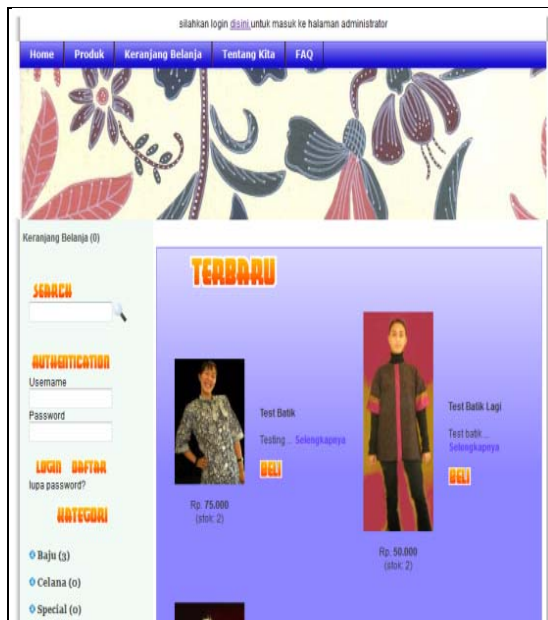


Gambar 8. Desain Layout Form User

Form user memiliki fasilitas untuk admin mengedit data yang ada pada website. Pada user pelanggan akan menampilkan data pemesanan yang telah dilakukan sehingga lebih *user friendly*. Di bagian kiri terdapat berbagai fitur *insert*, *update*, *delete* pada admin dan untuk user untuk melihat status pemesanan.

IMPLEMENTASI DAN PENGUJIAN Halaman Utama

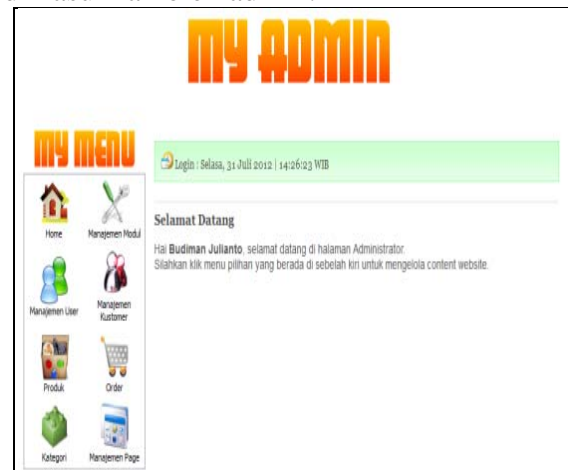
Pada Gambar 8 merupakan gambaran tampilan awal pada saat user memasuki aplikasi *e-commerce*. Pada halaman tersebut terdapat beberapa fitur seperti *search*, login, menu, kategori, produk terbaru. Sehingga mudah dipahami oleh pengguna.



Gambar 9. Tampilan Home

Tampilan Halaman Admin

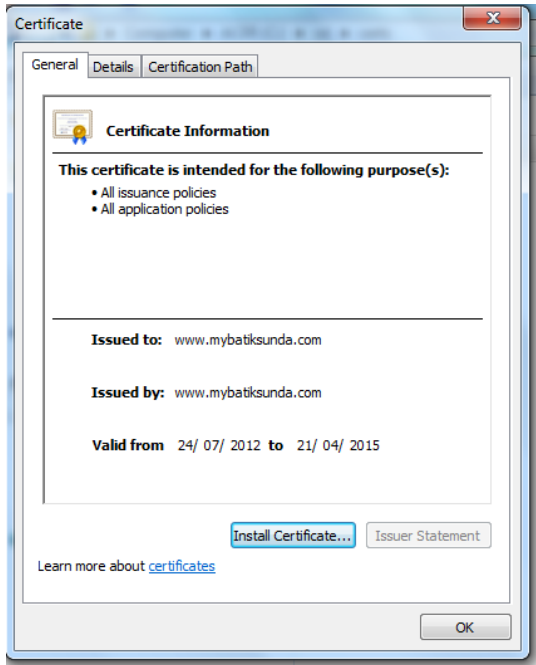
Pada Gambar 9 merupakan tampilan pemesanan yang dilakukan oleh user untuk melakukan transaksi pada aplikasi *e-commerce*. Terdapat beberapa pilihan : manajemen modul, manajemen user, manajemen kustomer, produk, order, kategori, manajemen page. Semua fitur tersebut dapat mempermudah kerja admin dalam mengelola data yang ada di website dan penggunaanya yang *user friendly* dapat mengurangi kesalahan data yang dimasukkan oleh admin.



Gambar 10. Tampilan Menu Admin

Implementasi SSL

Pada Gambar 21 merupakan hasil sertifikat SSL yang telah berhasil dibuat untuk diimplementasikan ke aplikasi *e-commerce* untuk mengamankan data yang ada dalam aplikasi tersebut.

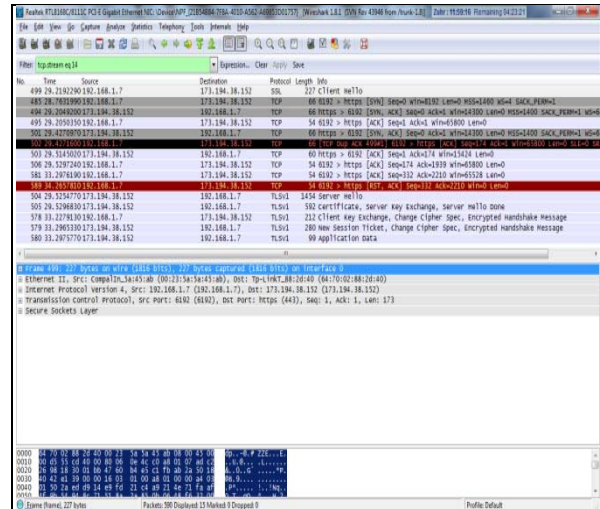


Gambar 11. Sertifikat SSL

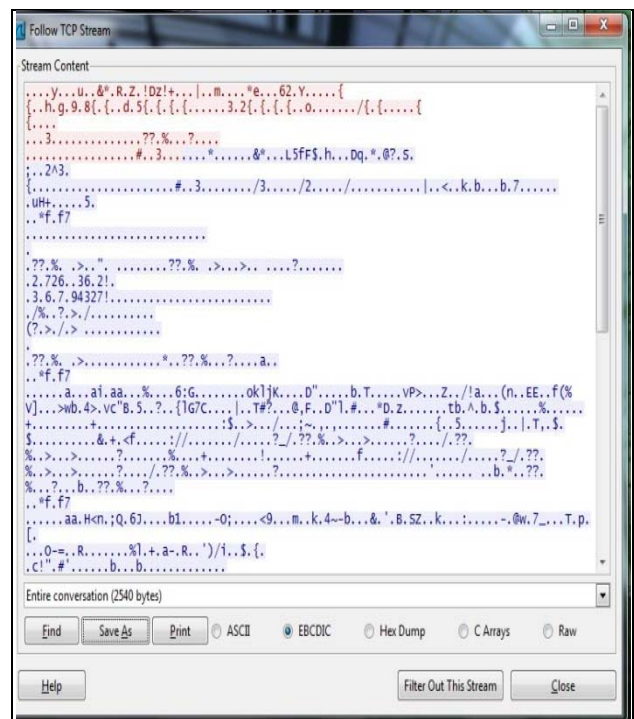
Pengujian Aplikasi Menggunakan Wireshark^[1]

Wireshark merupakan software untuk melakukan analisa lalu-lintas jaringan komputer, yang memiliki fungsi-fungsi yang berguna bagi profesional jaringan, administrator jaringan, peneliti, hingga pengembang piranti lunak jaringan. Program ini juga sering digunakan oleh *sniffer* untuk mengetahui ip victimnya maupun data berupa username dan password pada suatu website.

Pada saat customer mengatakan bahwa jaringan nya pelan, atau jaringan nya tidak responsive, atau jaringan nya kadang cepat kadang tidak bisa connect, dsb., maka cara paling mudah adalah ‘mengendus’ jaringan dengan langsung melihat isi-isi paket yang lewat di jaringan tersebut.



Gambar 12. Hasil Pengujian SSL menggunakan Wireshark 1.8.1



Gambar 13. Hasil Enkripsi

Dari hasil pengujian menunjukkan bahwa data yang ada pada aplikasi *e-commerce* tidak dapat di sniffing atau dilihat karna sudah diubah secara acak oleh sertifikat SSL. Sehingga data yang terdapat pada aplikasi *e-commerce* batik sunda terjaga kerahasiaannya.

P E N U T U P

Kesimpulan

Berdasarkan hasil pengujian dengan menggunakan Wireshark menunjukkan bahwa data yang ada pada aplikasi e-commerce tidak dapat di *sniffing* atau dilihat karna sudah diubah secara acak oleh sertifikat SSL. Sehingga data yang terdapat pada aplikasi *e-commerce* batik sunda terjaga kerahasiaannya.

Dengan pengimplementasian SSL pada aplikasi e-commerce, data user dan data admin akan terjaga kerahasiaannya. Secara umum aplikasi ini merupakan aplikasi yang dapat mempermudah proses transaksi barang dan memberikan rasa aman pada user pada saat berbelanja di toko online Batik Sunda ini serta mencegah pemanfaatan data yang ada pada website oleh orang yang tidak memiliki wewenang dan tidak bertanggung jawab.

Informasi Penjualan Furniture pada PT. First Homeware Berbasis Web, Skripsi, Jurusan Sistem Informasi, STIKOM, Surabaya.

6. Oppliger, Rofl, 2009, *SSL and TLS : Theory and Practice*, Artech House, Norwood.

DAFTAR PUSTAKA

1. Julianto, Budiman. Rosmala, Dewi. 2012. *Referensi Data dan Informasi melalui Internet*. Teknik Informatika, ITENAS, Bandung.
2. Laksana, Fajar, 2008, *Manajemen Pemasaran Pendekatan Praktis*, Graha Ilmu, Yogyakarta
3. Adhiguna, Ary Tirta, 2010. Dalam Tugas Akhir, *Rancang Bangun Website Penjualan Tupperware dengan Sistem Shopping Cart*, Skripsi, Jurusan Sistem Informasi, STIKOM, Surabaya.
4. Anggraini, Ajeng, 2010. Dalam Tugas Akhir, *Implementasi Aplikasi E-Commerce Dengan Menggunakan Protokol Https Sebagai Pendukung Keamanan Jaringan*, Skripsi, Politektik Telkom, Bandung.
5. Dinata, Praya, IMade, 2010. Dalam Tugas Akhir, *Rancang Bangun Sistem*