IMPLEMENTASI APLIKASI E-COMMERCE DENGAN MENGGUNAKAN PROTOKOL HTTPS SEBAGAI PENDUKUNG KEAMANAN JARINGAN (Studi Kasus di PD. Kharima Jaya Cimahi, Bandung)

Ajeng Anggraeni

[1]Henry Rossi Andrian, S.T., M.T. [2]Erwansyah Putra
henry.andrian@gmail.com

ABSTRAK

Pengimplementasian sebuah aplikasi *E-Commerce* merupakan salah satu cara dalam mempromosikan perusahaan ini karena akan berdampak postif dalam memajukan proses bisnisnya dan memperbesar nama dagang Kharima Jaya.

Perkembangan teknologi yang semakin maju mengakibatkan tingkat kebutuhan terhadap keamanan informasi menjadi penting. Seiring berkembangnya informasi munculah permasalahan baru mengenai keamanan jaringan, contoh ancaman keamanan jaringan yang sering terjadi adalah pengendusan aktivitas di jaringan atau biasa disebut *sniffing*, selain ancaman pengendusan juga terdapat ancaman lainnya seperti *MITM attack* (*man in the middle*) yang memungkinkan *attacker* berada di tengah komunikasi bebas mendengarkan atau mengubah percakapan antara dua pihak.

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.

Kata Kunci : *E-Commerce, Sniffing, MITM Attack, SSL, HTTPS*

ABSTACT

Implementing an E-Commece application is one way in promoting this company because it will be positive impact in advancing its business processes and increase the trade name Kharima Jaya.

The increasing development of advanced technologies has made security of information very essential. New problems on network security emerge as the growth of information itself. One of those threats is sniffing which tracks down user activities on networks. The other one is "man in the middle" (MITM) which illegally permit attacker to intercept in the middle of communication so they can freely listen or change the conversation between two parties.

HTTP over SSL, which is usually implemented with HTTPS, is an HTTP protocol that uses Secure Socket Layer (SSL) as a sub-layer under the HTTP so it can be much more secure.

Keyword : *E-Commerce, Sniffing, MITM Attack, SSL, HTTPS*

1. Pendahuluan

1.1 Latar Belakang

Dewasa ini, perkembangan teknologi dan informasi semakin pesat. Teknologi Internet merupakan salah satu media informasi yang saat ini paling banyak digunakan karena memiliki banyak keunggulan terutama dalam efesiensi waktu serta murah. Salah satu contoh dari pemanfaatan Internet adalah aplikasi *web*. Aplikasi *web* adalah suatu aplikasi yang diakses menggunakan penjelajah web melalui suatu jaringan seperti Internet atau Intranet (Wikipedia). Aplikasi *web* sangat bermanfaat dalam mempromosikan ataupun melakukan transaksi jual beli pada sebuah perusahaan melalui media Internet. Sebagai contoh, banyaknya perusahaan yang menjual produk dan promosi produk melalui *E-Commerce* dan *E-Bussiness*. Penjualan tersebut dilakukan secara elektronik. Oleh karena itu, PD. Kharima Jaya ingin mempromosikan perusahaannya dengan mengunakan aplikasi *E-Commerce* ini agar dapat tersebar secara cepat.

Di samping itu, keamanan jaringan adalah isu paling penting saat kita membangun sebuah situs web yang ditujukan untuk mendukung aktivitas *E-Commerce*. Namun demikian, banyak sekali pemilik bisnis yang tidak menyadari hal tersebut karena terbatasnya informasi dan seringkali karena terbenturnya oleh minimnya kapabilitas pihak pengembangnya. Padahal jika menginginkan adanya transaksi pemesanan dan pembelian dalam situs web *E-Commerce*, minimal harus dilengkapi fasilitas enkripsi data.

Fasilitas enkripsi data yang standar yang digunakan di Internet saat ini adalah SSL (*Secure Socket Layer*) yang diterbitkan oleh penerbit terpercaya berdasarkan CA (*Certificate Authority*) yang diakui. Dalam hal ini protokol HTTP (*Hypertext Transfer Protocol*) adalah protokol baku yang digunakan dalam *web*. Demi mendukung kemudahan komunikasi antar perangkat yang beragam maka protokol HTTP dirancang bersifat memiliki platform terbuka. Kemudahan rancangan ini ternyata dimanfaatkan oleh beberapa oknum untuk mencuri informasi yang dikirimkan oleh pengakses suatu situs *web*.

Untuk melindungi paket informasi yang dikirimkan melalui protokol terbuka HTTP maka dirancanglah sebuah protokol HTTPS (*Hypertext Transfer Protocol Secure*) dengan sistem enkripsi data yang dinamakan SSL. Dengan demikian, pada saat seorang pengakses

situs *web* mengirimkan data secara elektronik, SSL yang dikonfigurasi dalam situs *web* tersebut akan mengenkripsinya dan mendistribusikannya melalui lapisan khusus yang sulit diakses oleh pihak ketiga.

1.2 Perumusan Masalah

Berdasarkan latar belakang diatas maka rumusan masalah, yaitu:

1. Bagaimana sebuah *E-commerce* dapat diterapkan dalam proses jual beli pada PD. Kharima Jaya?
2. Bagaimana cara SSL diterapkan dalam aplikasi *E-commerce* ?

1.3 Tujuan

Tujuan dari Proyek Akhir ini adalah Sebagai berikut :

1. Menerapkan aplikasi sebuah *E-commerce* dalam proses jual beli pada PD. Kharima Jaya?
2. Menerapkan SSL dalam aplikasi *E-commerce*

1.4 Batasan Masalah

Untuk memfokuskan bahasan maka penulis memberikan batasan masalah dalam Proyek Akhir ini seperti berikut:

1. Informasi yang ditampilkan dalam web ini adalah informasi perusahaan, informasi produk, cara pembelian, dan cara pendaftaran menjadi anggota.
2. Proses transaksi dilakukakan hanya untuk pembayaran *offline*.
3. Aplikasi diimplementasi dengan menggunakan HTTPS sebagai protokol keamanannya dan OpenSSL sebagai *toolkit* kriptografi SSL.
4. Penyusunan proyek akhir ini hanya sampai pada tahap implementasi

2. Dasar Teori

2.1 Profil Perusahaan

PD. Kharima Jaya adalah perusahaan dagang yang berlokasi di kota Cimahi, Jawa Barat. Perusahaan ini didirikan oleh H. Erwansyah Putra , SE. pada tahun 1998 dan di resmikan sebagai perusahaan dagang pada 25 Juni 2007. Perusahaan ini bergerak pada bidang supplier knitting textile atau pemasok bahan dasar kain. Kharima Jaya memasok barang mulai dari partai kecil hingga partai besar dan juga telah mensupply barang ke beberapa kota besar di Indonesia.

Ruang Lingkup Kegiatan Perdagangan :

1. Kharima Jaya memasok barang yang langsung di ambil dari pabrik utama, dan menyusun ulang bahan dasar.
2. Bahan dasar yang telah siap di pasarkan di stok ke gudang dan saat ada customer yang membeli hanya melihat contoh bahan dasar.
3. Kesepakatan antara perusahaan dengan customer tentang harga dilakukan transaksi jual beli.
4. *Customer* atau pihak ke-3 menjual lagi bahan dasar dengan harga dan merek dagang yang berbeda, ataupun menggunakan untuk keperluan perusahaan lain.

2.2 Internet

"*Interconnection networking* atau yang lebih popular dengan sebutan Internet adalah sebuah sistem komunikasi global yang menghubungan komputer-komputer dan jaringan-jaringan komputer di seluruh dunia" (Purbo, 1998). Internet juga dapat diartikan hubungan berbagai komputer dan berbagai tipe komputer yang membentuk sistem jaringan yang mencakup seluruh dunia (jaringan global) dengan jalur telekomunikasi seperti *telepon, wirless* dan lainnya (Sutarman, 2003). Internet memungkinkan masyarakat untuk memperoleh informasi dan layanan dengan cepat.

2.3 Pengenalan E-Commerce

Electronic commerce (*e-commerce*) adalah suatu penjualan secara elektronis, yang bisa dilakukan dari jarak jauh (teknologi *marketing*) yang digunakan di luar toko. Untuk tempat yang jauh sekalipun tetap dilakukan perdagangan dengan memanfaatkan *e-commerce*. Perubahan cara dan bentuk perdagangan telah mengubah, menggeser dan menaklukkan cara bisnis global yang tidak mengenal jarak dan waktu. Kegiatan yang dilakukan juga menjadi tidak banyak lagi diwakili oleh tenaga manusia di saat terjadi peningkatan keterpaduan telekomunikasi dan komputasi secara integral. Berdagang lewat elektronik merupakan tantangan dan ancaman bagi perdagangan tradisional. (Tim Penelitian dan Pengembangan Wahana Komputer Yogyakarta, 2006).

2.4 Bahasa pemprograman dan teknik pemprograman Pembangun Sistem

2.4.1 Hypertext Modeling Language (HTML)

HTML adalah sebuah bahasa mark-up yang digunakan untuk membuat sebuah halaman web, menampilkan berbagai informasi di sebuah penjelajah web Internet dan *formating hypertext* sederhana yang di tulis ke dalam format ASCCI agar dapat menghasilkan tampilan wujud yang terintegrasi. Dengan kata lain, berkas yang di buat dalam perangkat lunak pengolahan kata dan di simpan dalam keadaan format ASCCI normal sehinga menjadi hompage dengan perintah perintah HTML.

Ja

2.4.2 Java Script

Java Script adalah bahasa skrip yang populer di Internet dan dapat bekerja di sebagian besar penjelajah web seperti Safari, *Mozila Firefox, Internet Explorer*. Kode *java script* dapat disisipkan dalam halaman *web* mengunakan tag *script* / <*script*>.

2.4.3 Hypertext Prepocessor (PHP)

Hypertext Prepocessor (PHP) adalah bahasa skrip yang dapat ditanamkan atau disisipkan ke dalam HTML. PHP banyak dipakai untuk memprigram situs *web* dinasmis.

2.4.4 Cascading Style Sheet (CSS)

Cascading Style Sheet (CSS) merupakan salah satu bahasa pemprograman *web* yang mengendalikan beberapa komponen dalam sebuah *web* sehinga akan lebih terstuktur dan seragam.

Pada umumnya CSS untuk memformat tampilan halaman *web* yang dibuat dengan bahasa HTML dan XHTML. CSS dapat mengendalikan ukuran, warna, gambar bagian tubuh pada teks warna table ukuran *border*, warna border, warna *hyperlink*, warna *mouse over*, spasi antar paragraf, spasi antar *text*, *margin* (kiri, kanan, atas, dan bawah), dan parameter lainya.

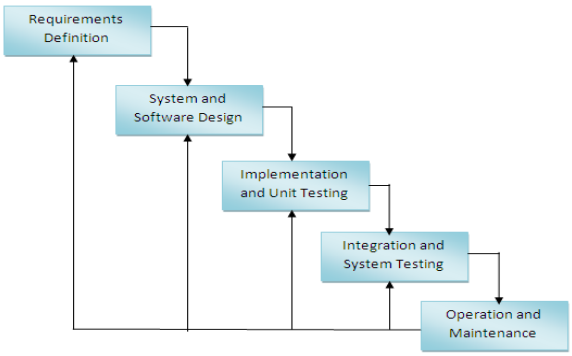
2.4.5 Web Server

Web Server dapat merujuk baik pada perangkat keras ataupun perangkat lunak yang menyediakan layanan akses kepada pengguna melalui protokol komunikasi HTTP atau HTTPS atas berkas-berkas yang terdapat pada suatu situs *web* dalam layanan ke pengguna dengan menggunakan aplikasi tertentu seperti peramban *web*.

Fungsi utama sebuah *server web* adalah untuk mentransfer berkas atas permintaan pengguna melalui protokol komunikasi yang telah ditentukan. Disebabkan sebuah halaman web dapat terdiri atas berkas teks, gambar, video, dan lainnya pemanfaatan *server web* berfungsi pula untuk mentransfer seluruh aspek pemberkasan dalam sebuah halaman web yang terkait; termasuk di dalamnya teks, gambar, video, atau lainnya.

2.5 Software Development Life Cycle

Metode yang digunakan untuk mengerjakan proyek akhir adalah *Software Development Life Cycle* (SDLC) dengan menggunakan model *Waterfall*.



Gambar Error! No text of specified style in document..**1** Tahapan SDLC

SDLC adalah proses pembuatan dan pengubahan sistem serta model dan metodologi yang digunakan untuk mengembangkan sistem-sistem tersebut. Sedangkan model *Waterfall* adalah sebuah metode pengembangan software yang bersifat sekuensial dan terdiri dari 5 tahap yang saling terkait dan mempengaruhi, antara lain :

a. Analisis Kebutuhan
b. Desain Sistem
c. Penulisan Kode Program
d. Pengujian Program
e. Penerapan Program

2.6 Flowchart

Drs. Suarga (2006:6) mengemukakan bahwa "Flowchart adalah suatu teknik untuk menyusun rencana program yang telah diperkenalkan dan dipergunakan oleh kalangan programer komputer sebelum algoritma menjadi popular."

Flowchart adalah representasi grafik dari langkah-langkah yang harus diikuti dalam menyelesaikan suatu permasalahan yang terdiri atas sekumpulan simbol, dimana masing-masing symbol merepresentasikan suatu kegiatan tertentu. Flowchart diawali dengan penerimaan input, pemrosesan input, dan diakhiri dengan penampilan output.

2.7 Data Flow Diagram (DFD)

Nugroho dkk., (2009:61) mengemukakan bahwa "*Data Flow Diagram* (DFD) adalah diagram untuk menggambarkan aliran data dalam sistem, sumber dan tujuan data, proses yang mengolah data tersebut, dan tempat penyimpanan datanya."

Diagram ini diperkenalkan oleh Tom DeMarco (1978) dan Chris Gane dan Trish Sarson (1977) berdasarkan notasi *Structure Analysis and Design Technique* (SADT).

Merupakan salah satu teknik yang cukup penting dalam menganalisis sistem karena :

a. Dapat mendefinisikan batasan sistem dan proses-proses pengolahan data yang ada didalamnya.
b. Membantu memeriksa kebenaran dan kelengkapan aliran informasi.

c. Merupakan dasar perancangan dengan memunculkan proses-proses pengolahan data.
d. Dapat digunakan untuk menggambarkan aktivitas proses secara paralel (beberapa aliran data dapat terjadi secara simultan).

2.7 Entity Rational Diagram

Janner Simarmata (2006:59) mengemukakan bahwa **"***Entity Relationship* (ER) data model didasarkan pada persepsi terhadap dunia nyata yang tersusun atas

Kegunaan model ER dalam perancangan tersebut adalah :

a. Mampu memetakan model relasional dengan baik. Pembangunan yang digunakan di dalam model ER dengan mudah diubah ke dalam tabel relasional.
b. Sederhana dan mudah dipahami hanya dengan sedikit pelatihan. Oleh karena itu, model bisa digunakan oleh perancang basis data untuk mengomunikasikan perancangan kepada pengguna akhir.
c. Model bisa digunakan sebagai suatu rencana perancangan oleh pengembang basis data untuk menerapkan suatu model data dalam perangkat lunak manajemen basis data spesifik.

2.8 Keamanan Jaringan

Keamanan Jaringan adalah menjaga agar resource digunakan sebagaimana mestinya oleh pemakai yang berhak.

Tujuan keamanan jaringan adalah sebagai berikut :

- *Availability* / Ketersediaan
- *Reliability* / Kehandalan
- *Confidentiality* / Kerahasiaan

Keamanan Jaringan juga memiliki Faktor-faktor yang membuat suatu jaringan beresiko untuk kehilangan data. Beberapa faktor Penyebab Resiko Dalam Jaringan Komputer adalah sebagai berikut :

- Kelemahan manusia (*human error*)
- Kelemahan perangkat keras komputer
- Kelemahan sistem operasi jaringan
- Kelemahan sistem jaringan komunikasi

Berikut adalah contoh dari serangan keamanan jaringan :

1. *Sniffing*

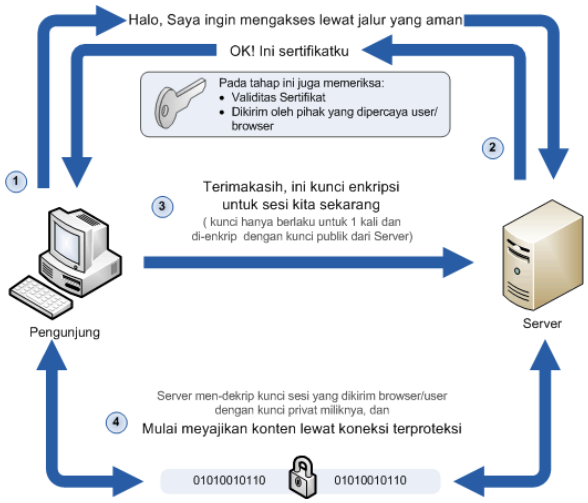
   Sniffing disebut juga mengendus, yakni seseorang di luar sana yang ingin mengambil *username* dan *password* yang kita miliki. Biasanya terjadi pada saat login. Orang asing tersebut akan melakukan *sniffing* atau pengendusan dengan menggunakan tools keamanan.

2. MITM

   MITM *attack* adalah serangan dimana *attacker* berada di tengah bebas mendengarkan dan mengubah percakapan antara dua pihak. Jadi dengan serangan MITM ini *attacker* tidak hanya pasif mendengarkan, tetapi juga aktif mengubah komunikasi yang terjadi. Sebagai contoh, pada percakapan antara Alice dan Bob, Charlie menjadi pihak yang ditengah melakukan MITM *attack*. Charlie tidak hanya bisa mendengarkan percakapan itu, namun juga bisa mengubah percakapannya. Ketika Alice berkata "Besok makan siang jam 7″, Charlie bisa mengubahnya menjadi "Besok makan siang dibatalkan" sehingga Bob mengira makan siang dengan Alice tidak jadi. *[6].*

2.9 Pengenalan Hyper Text Transfer Protocol Secure (HTTPS)

HTTPS yang berarti sisi aman dari pada HTTP. Kelebihan HTTPS dibandingkan dengan HTTP adalah jika *user* mengakses *web* server dengan jalur HTTPS maka orang lain yang tidak berkepentingan tidak akan dapat membajak atau *sniffer* packet-packet data yang dimiliki *user*, serta melindungi username dan password *user* itu sendiri yang ingin mengakses *web server*.



Gambar Error! No text of specified style in document..**3** Simulasi cara kerja HTTPS

Kelebihan server yang menggunakan HTTPS diantaranya adalah :

1. Jalur yang digunakan untuk transfer data sangat aman karena terenkripsi.
2. Sertifikat yang didapatkan dari beda pemberi sertifikat dijamin keamanannya oleh badan tersebut.
3. Dapat menangkal serangan *sniffer* maupun *middle attack.*

2.9.1 Secure Socket Layer (SSL)

Secure Socket Layer (SSL) adalah protokol yang digunakan untuk *browsing web* secara aman. SSL bertindak sebagai protokol yang mengamankan komunikasi antara client dan server. Protokol ini memfasilitasi penggunaan enkripsi untuk data yang rahasia dan membantu menjamin integritas informasi yang dipertukarkan antara website dan web browser.

SSL hanya mengenkripsikan data yang dikirim lewat http. Bagaimana SSL berjalan dapat digambarkan sebagai berikut :

- Pada saat koneksi mulai berjalan, klien dan server membuat dan mempertukarkan kunci rahasia, yang dipergunakan untuk mengenkripsi data yang akan dikomunikasikan. Meskipun sesi antara klien dan server diintip pihak lain, namun data yang terlihat sulit untuk dibaca karena sudah dienkripsi.
- SSL mendukung kriptografi *public key*, sehingga server dapat melakukan autentikasi dengan metode yang sudah dikenal umum seperti *RSA* dan *Digital Signature Standard (DSS)*.
- SSL dapat melakukan verifikasi integritas sesi yang sedang berjalan dengan menggunakan algoritma *digest* seperti MD5 dan SHA. Hal ini menghindarkan pembajakan suatu sesi.

2.9.2 Port 443

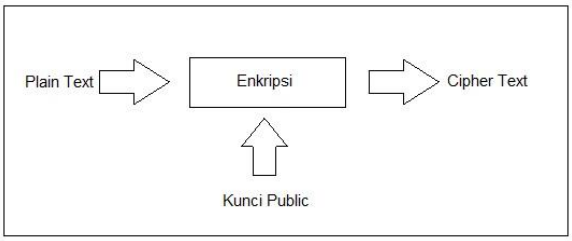
Port ini berfungsi pada *Secure Socket Layer* (SSL) ketika kita menjalankan *server* makan SSL client meminta untuk terhubung ke *server* ini kemudian *server* akan terhubung ke port 443 ini. Port ini dibuka untuk menjalankan keamanan *server*.

2.9.3 Open SSL

Open SLL adalah layanan yang digunakan utuk membuat sertifikat SSL.

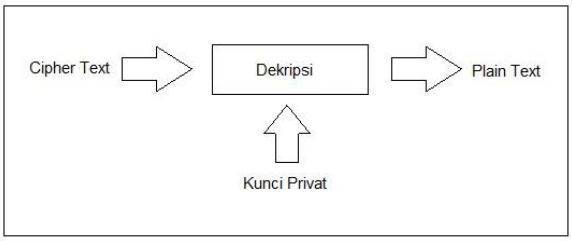
2.9.4 Kriptografi

Kriptografi adalah ilmu dan seni penyimpanan pesan, data, atau informasi secara aman. Algoritma kriptografi terbagi menjadi 2, yaitu : **enkripsi dan dekripsi**. **Enkripsi** adalah proses pengubahan data jelas (*plain text*) menjadi data sandi (*cipher text*).



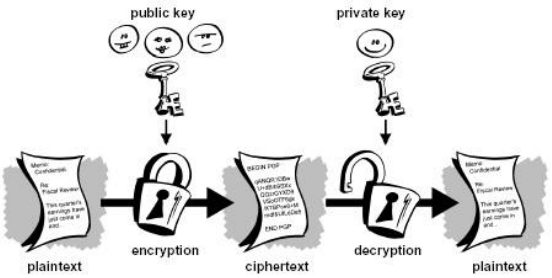
Gambar Error! No text of specified style in document.**.4**
Proses Enkripsi Data

sedangkan **dekripsi** adalah proses pengubahan data sandi (*cipher text*) menjadi data jelas (*plain text*).



Gambar Error! No text of specified style in document.**.5**
Proses Dekripsi Data

Proses pengiriman data jelas (*plain text*) yang dienkripsi dengan *public key* kemudian menghasilkan data berupa sandi (*cipher text*) yang kemudian akan didekripsi oleh penerima dengan menggunakan *private key* miliknya sehingga saat diterima data tersebut kembali dalam bentuk (*plain text*).



Gambar Error! No text of specified style in document.**.6**
Proses Enkripsi dan Deskripsi

3 Analisa Kebutuhan Dan Perancangan

3.1 Analisis kebutuhan sistem

3.1.1 Spesifikasi Perangkat Lunak

Berikut adalah spesifikasi kebutuhan perangkat Lunak yang dibutuhkan dalam membangun Aplikasi *E-Commerce* dengan menggunakan protokol HTTPS pada PD. Kharima Jaya.

Tabel Error! No text of specified style in document.**..1**
Spesifikasi Perangkat Lunak

No.	Spesifikasi
1	*Notebook*
2	Processor Intel Core 2 Duo
3	Harddisk 120 Gb
4	RAM 1,5 Gb

3.1.2 Spesifikasi Perangkat Keras

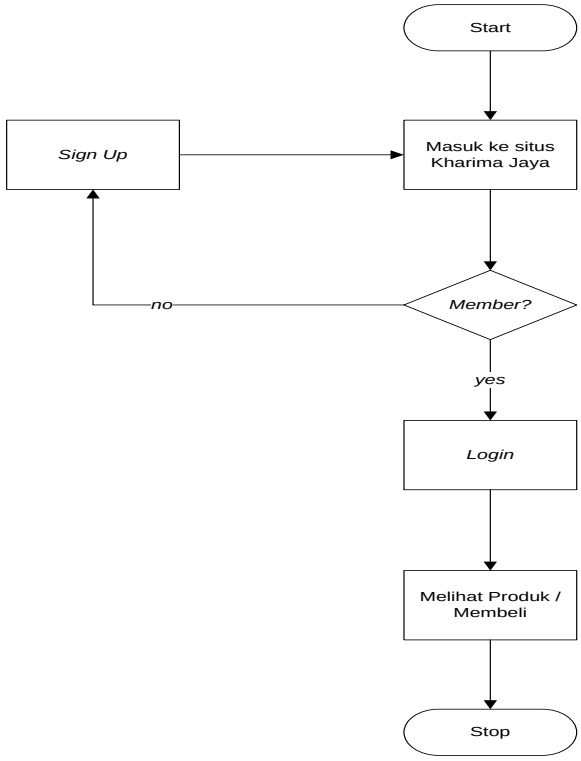
Berikut adalah spesifikasi kebutuhan perangkat Keras yang dibutuhkan dalam membangun Aplikasi *E-Commerce* dengan menggunakan protokol HTTPS pada PD. Kharima Jaya.

Tabel Error! No text of specified style in document.**-2**
Spesifikasi Perangkat Keras

No.	Jenis Software	Nama Software
1.	Sistem Operasi	Ubuntu 10.4
2.	Web Server	Apache2
3.	Bahasa Program	PHP5
4.	Database	My SQL Server
5.	Browser	Mozilla FireFox
6.	Testing	Wireshark

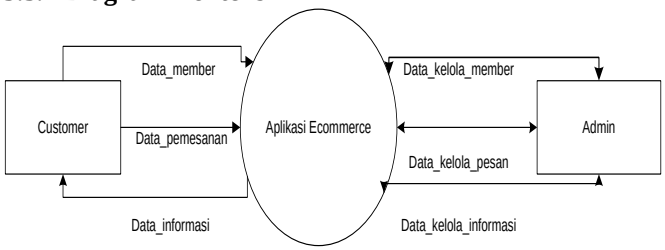
3.3 Perancangan Sistem

3.3.1 Flowchart (Alur Sistem Website)



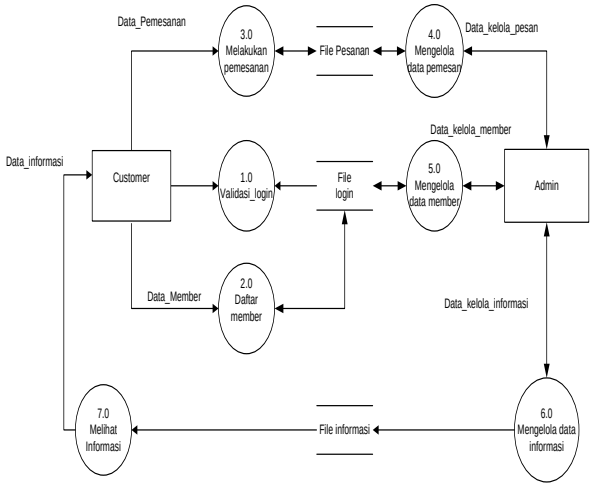
Error! No text of specified style in document.**..1 Flowchart (Alur Sistem Website)**

3.3.2 Diagram Konteks



Gambar Error! No text of specified style in document.**..2**
Diagram Konteks

3.3.4 Diagram DFD Level 0



Gambar Error! No text of specified style in document.**.3** *Data Flow Diagram Level 0*

4 Implementasi dan Pengujian

4.1 Implementasi

4.4.2 Login ke root

Gambar 5.1 menjelaskan ketika user akan memulai konfigurasi. User akan melakukan di root.

```
ajeng@ajeng-laptop:~$ sudo su
[sudo] password for ajeng:
```

Gambar Error! No text of specified style in document.**.2 Login ke root**

Melihat dpkg apache2

```
root@ajeng-laptop:/home/ajeng# dpkg -l | grep apache

ii apache2                2.2.14-5ubuntu8.4          Apache HTTP Server
metapackage
ii apache2-mpm-worker     2.2.14-5ubuntu8.4          Apache HTTP
Server - high speed threaded mod
ii apache2-utils          2.2.14-5ubuntu8.4          utility programs for
webservers
ii apache2.2-bin          2.2.14-5ubuntu8.4          Apache HTTP
Server common binary files
ii apache2.2-common       2.2.14-5ubuntu8.4          Apache HTTP
Server common files
```

Gambar Error! No text of specified style in document.**.3 Melihat dpkg apache2**

Install Apache2

```
root@ajeng-laptop:/home/ajeng# apt-get install
apache2
```

Konfigurasi openSSL

root@ajeng-laptop:/home/ajeng# mkdir /etc/ssl/CA

root@ajeng-laptop:/hoxme/ajeng# cd /etc/ssl/CA

root@ajeng-laptop:/etc/ssl/CA# openssl genrsa -des3 -out server.key 1024

Generating RSA private key, 1024 bit long modulus

.....++++++

.....++++++

e is 65537 (0x10001)

Enter pass phrase for server.key:

Verifying - Enter pass phrase for server.key:

root@ajeng-laptop:/etc/ssl/CA# openssl rsa -in server.key -out server.key

Enter pass phrase for server.key:

writing RSA key

root@ajeng-laptop:/etc/ssl/CA# openssl req -new -days 3650 -key server.key -out server.csr

You are about to be asked to enter information that will be incorporated

into your certificate request.

What you are about to enter is what is called a Distinguished Name or a DN.

There are quite a few fields but you can leave some blank

For some fields there will be a default value,

If you enter '.', the field will be left blank.

Country Name (2 letter code) [AU]:id

State or Province Name (full name) [Some-State]:west java

Locality Name (eg, city) []:bandung

Organization Name (eg, company) [Internet Widgits Pty Ltd]:Kharima Jaya

Organizational Unit Name (eg, section) []:Kharima Jaya

Common Name (eg, YOUR name) []:Ajeng

Email Address []:jengaah.chubby@gmail.com

Please enter the following 'extra' attributes

to be sent with your certificate request

A challenge password []:

An optional company name []:

root@ajeng-laptop:/etc/ssl/CA# openssl x509 -in server.csr -out server.crt -req -signkey server.key -days 3650

Signature ok

root@ajeng-laptop: sudo /etc/init.d/apache2 restart

subject=/C=id/ST=west java/L=bandung/O=Kharima Jaya/OU=Kharima Jaya/CN=Ajeng/emailAddress=jengaah.chubby@gmail.com

Getting Private key

root@ajeng-laptop:/etc/ssl/CA# chmod 400 server.*

root@ajeng-laptop:/etc/ssl/CA# nano /etc/apache2/sites-available/default

default default-ssl

root@ajeng-laptop:/etc/ssl/CA# nano /etc/apache2/sites-available/default-ssl

root@ajeng-laptop:/etc/ssl/CA# nano /etc/apache2/sites-available/default-ssl

root@ajeng-laptop:/etc/ssl/CA# vi /etc/apache2/sites-available/default-ssl

root@ajeng-laptop:/etc/ssl/CA# gedit /etc/apache2/sites-available/default-ssl
root@ajeng-laptop:/etc/ssl/CA# ls
server.crt server.csr server.key
root@ajeng-laptop:/etc/ssl/CA# gedit /etc/apache2/sites-available/default-ssl
root@ajeng-laptop:/etc/ssl/CA# ls /etc/apache2/sites-available/
default default-ssl
root@ajeng-laptop:/etc/ssl/CA# ls /etc/apache2/sites-enabled/
root@ajeng-laptop:/etc/ssl/CA# a2ensite default-ssl
Enabling site default-ssl.
Run '/etc/init.d/apache2 reload' to activate new configuration!
root@ajeng-laptop:/etc/ssl/CA# /etc/init.d/apache2 reload
* Reloading web server config apache2
apache2: Could not reliably determine the server's fully qualified domain name, using 127.0.1.1 for ServerName[OK]

Instalasi PHP MyAdmin, php5, MySQL Server
Instalasi PHP MyAdmin

1. Login terdahulu ke root kemudian Install

```
ajeng@ajeng-laptop:~$ sudo su
[sudo] password for ajeng:
```

2. Install PHP 5

3. Agar PHP dan Apache berjalan sejalan, maka restart apache2

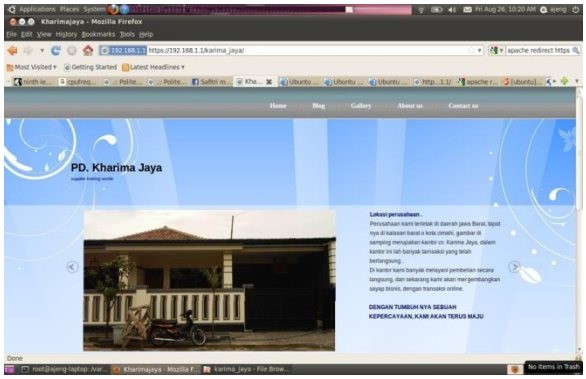
4. Instalasi My SQL Server

```
root@ajeng-laptop: sudo apt-get install mysql-server
```

Agar PHP dan Apache berjalan sejalan, maka restart apache2

```
root@ajeng-laptop: sudo /etc/init.d/apache2 restart
```

4.2 Pengujian
4.2.1 Hasil

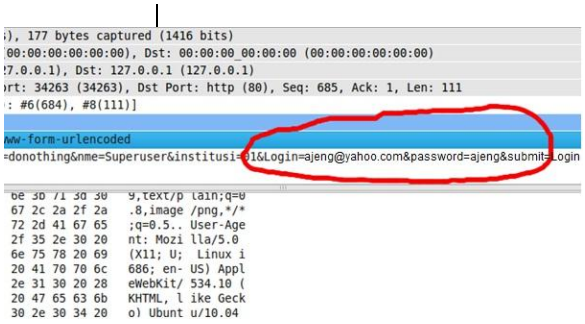


Gambar 4.1 Hasil Pengujian 1

Gambar 4.2 Hasil Pengujian 2

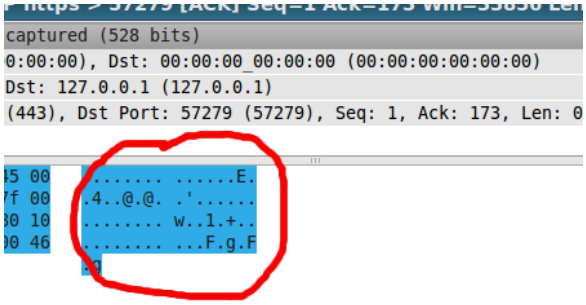
4.2.3 Perbandingan dengan HTTP
a. Dengan HTTP

```
root@ajeng-laptop:/var/www# apt-get install phpmyadmin
root@ajeng-laptop: sudo apt-get install php5 libapache2-mod-php5
Reading package lists... Done
Building dependency tree
Reading state information... Done
```



Gambar 4.3 Hasil Capture HTTP

b. Dengan HTTPS



Gambar 4.4 Hasil Capture HTTPS

5. Kesimpulan dan Saran

5.1 Kesimpulan

Berdasarkan hasil pengujian dan analisis dari implementasi proyek akhir ini dapat diambil beberapa kesimpulan yaitu :

1. Aplikasi *E-Commerce* diimplementasikan di PD. Kharima Jaya guna mengembangkan informasi penjualan kain dan membuat proses jual-beli menjadi efisien dan murah.
2. Penerapan SSL pada aplikasi *E-Commerce* ini merupakan salah satu cara mengamankan komunikasi data antara *client* dan *server*.

5.2 Saran

Untuk konfigurasi selanjutnya, sebaiknya menggunakan *Certificate Autority* yang di dapat dari perusahaan yang resmi mengeluarkan *Certificate Autority* tersebut.

6. Referensi

[1] Bambang, W., Renaldy, B., & Ashari, A. (2010). *Linux System Administrator.* Bandung: Informatika.
[2]Hendro. (2005, Desember 26). Sniffing vs Spoofing . p. 1.
[3]Jayan. (2010). *CSS untuk orang awam.* Palembang: Maxikom.
[4]Kadir, A. (2009). *From Zero to a Pro membuat aplikasi web dengan php ++ database My SQL .* Yogyakarta: Andi.
[5]Komputer, W. (2010). *Menguasai Pemprograman Web dengan Java Script.* Yogyakarta: Andi.
[6]Nugroho, A. (2006). *Ecommerce, memahami perdagangan modern di dunia nyata.* Bandung: Informatika.
[7]Nugroho, B. (2004). *Aplikasi Pemprograman Web Dinamis dengan PHP dan My SQL.* Yogyakarta: Gava Media.
[8]Nugroho, B. (2005). *Instalasi dan Konfigurasi Jaringan Windows dan Linux.* Yogyakarta: Andi.