ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 2, February 2014

Different Techniques for the Implementation of Electronic Shopping Cart

Ninad Sanjay Puranik[1], Zuber Shaikh[2], Radha Dhekane[3]

Sinhgad Academy of Engineering, University of Pune, Pune, India[1,2,3]

Abstract: Considering the rapid development and domestic use of electronic shopping cards, solutions are given by different methods. All the survey methods are given with their pros and cons so that by considering all these conditions a new robust method for implementation of Electronic shopping cart could be proposed. In the already implemented techniques market risk is considered and handled in efficient manner but still the techniques are not 100% secure. Factors like security, reliability and session management are considered and the facts are given in effective manner. Objective of this survey is the need for development of new robust techniques for shopping cart application which covers previously mentioned factors. While developing new techniques all the facts and figures of the existing techniques and technologies are to be considered. Major importance is given to privacy, security and application development factors.

Index Terms: Electronic Shopping cart, e-commerce, Credit card, Third Party Payment, Parametric documents

I. INTRODUCTION

Recently, World Wide Web (The web) is the mainstream of base system on which client server systems are developed. The major reason for the wide spreading use of web is the low maintenance cost of the software. The distribution cost is almost zero. All the clients can therefore use newest application software easily. Thus web-based client server system is widely use architecture not only for internet based application but also for intra-net systems.[1]

There are several problems which occur in this approach, problems which did not occur in the conventional client server application. These problems should be analyzed to find the optimal way of solving the problems. This paper considers shopping cart system to be developed on the web. Shopping cart has a simple functionalities but it contains essential problems for construction of client-server system on web.

HTTP is a stateless protocol. Hence it is not possible to maintain user data in between two states, thus the major problem here is "session management". Several methods have been implemented for realizing and implement session management. Though several methods have been proposed to realize session management, they are not sufficient form the point of view of reliability and safety. We then compare all the methods implemented before to check if all the difficulties mentioned above are solved and if they attained efficient communication between client and Web server.

This paper also puts forward TPP (Third Party Payment for short) conception and payment model. This makes sure that there is no cheating and makes sure that money is received on time. Personal credit mechanism is discussed to help the customer choose a reputable seller.[2]

II. WORKING OF ELECTRONIC SHOPPING CART

In this section we define the shopping cart system on the Web. This includes essential features that are possessed by most client-server applications. The customers can do the following four actions:

- Browse the item
- Select the item
- Remove item form cart
- Send their cart to the accounting server.

Actually, the shopping site consists of many web pages linked to one another. For each item price is assigned. Then a customer can use electronic shopping cart to hold items that customer has selected to buy. Customers are allowed to take three behaviors: Browse freely listed items for sale on web, Put the items in cart, Discard the items if the customer changes his mind finally send the shopping cart to the server and pay an account.[1]

There are several problems faced in implementation of Web based shopping cart application. HTTP being a 'session-less' or 'state-less' it is difficult to maintain the content in among successive user session. When the customer moves form one page to another the content has to be maintained. However, the HTTP protocol cannot maintain it even if the user is on the same website. First is the problem of reliability. If the web server crashes the content in the cart may disappear.

The content in the cart should be maintained till the server recovers. The second important problem is security. The content in the cart should not be viewed by other users. There is a case of the content changed by the customer (for example, the price of product). Thus it is important to implement security functions.

III. EXISTING TECHNIQUES

There are 4 implemented methods for realizing session management and the factors such as reliability and safety and session management.

a. Parametric Documents

In this, the context data is passed in the form of arguments for a program that generates the dynamic HTML document. Thus it is quite obvious for the observer to

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 2, February 2014

understand the session management in online shopping system.[1]
Also the context data is easily available in the source of html file, the context of the shopping kart are easily available and thus can be changed by the user. Thus this result in a serious threat to the safety of this architecture.

b. Client Side Cookie

Cookies are small *data structures* delivered by a Web site to a Web client which store the context data. Cookies are stored in text files generally known as cookie files. The web server can read and write these files. For this parametric document to be processed the browser must have the cookie functionality. The cookie can be processed and then destroyed according to their expiry time. Using cookies one can regenerate the situation same as the previous visit.[1]

There exit a problem of safety as the document is in the form of text and the content of a shopping kart can be easily modified by the users.

c. Server Side Cookie

The working of server-side cookie is similar to the client-side cookie. The cookie data is stored in the main memory of the web server rather that the client computer. On the client-side cookie small information i.e. session id is stored. [1]

In this method the user cannot read the context data, thus the server-side cookie have high security of the context data.

d. Context Data Storing Mechanism:

In this method we introduce document-view architecture. Here we separate the data management part(documentation) and graphical user interface part(view).[1] Hence the main functions for the web shopping cart system can be constructed efficiently by assigning the context data and the web browser to the document and the view, respectively.

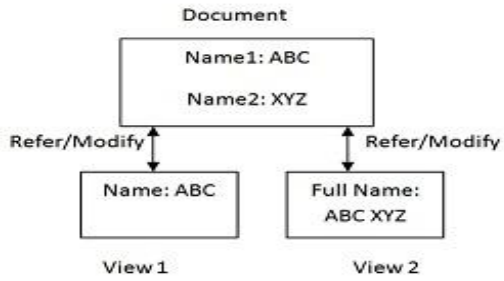

Fig1[1]. Document View Architecture

An advantage of this method is that users can form their own views by defining the views. Thus the usability of the application is also improved.

If several views exist in the same system, updating of data from one view must be informed to all related views. As shown in the next figure suppose the data named "Name" on the View -1 is modified. Then the corresponding data "Name1" on the document must be updated and its change must be informed to the view-2. In order to implement the document-view architecture, we used to kind of communications, server and client.

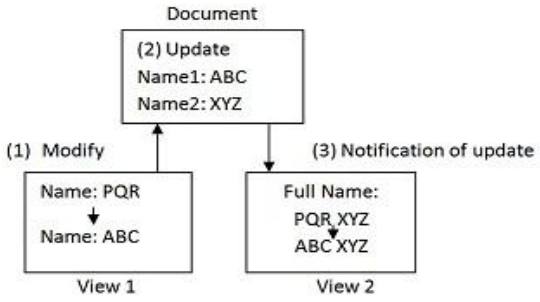

Fig2[1]. Updating of data in a view

e. Difficulties in implementing previous methods

An implementation of the web shopping cart system using client side cookie method is shown in the figure given below. The figure shows an activity flow which selects item 1, item 2 and item 3 and puts them in the cart and finally pays an account.[1] Using the client side cookie, a cookie file is generated by the web's server program to store the context data for each item. Thus the communication between the client and web server occur frequently. At time t_i (i=1,2 and 3), item list is browsed, and item i is selected and put in the cart. Finally at time t_4, the cart is sent to the accounting server. For each selection of new item, communication is done between server and client computer via the web. If we apply parametric document and server-side cookie, then the server and client do the handshake.

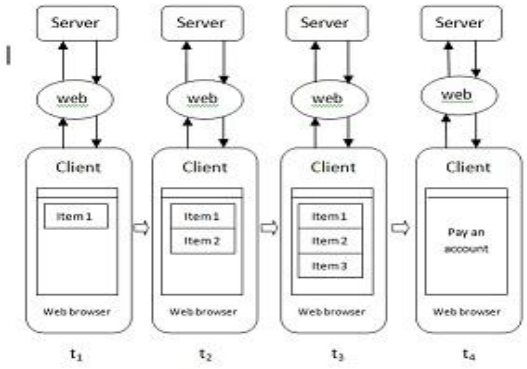

Fig3[1]. Implementation of client-side cookie

More over there still exist several other problems. If the web server crashes or is down, then all the context data on the server disappear suddenly. One solution would be several web server should be introduced. However the reliability problem still remains. Next consider parametrical document. Here the document is again available directly without encryption which again reduces the security.

IV. TPP PLATFORM

Third party platforms are supplied by third party independent institutions which have already signed contracts with big banks.[2] These organizations are can be classified as agent organization with clear payment responsibility. After the customer has selected the product

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 2, February 2014

the customer is supposed to make the payment using TPP platform and the third party is responsible for notifying the sellers to deliver the commodities.

a. Advantages of TPP platform

- Reduces the risk of bad payment.
- It promotes the interaction between merchant and bank and increases the business of banks
- It provides increment service and helps the sellers' website

b. Framework of TPP

TPP consist of three major components Buyers, Seller, Finance Institute. [2] It connects buyers, sellers and finance institutes. The foreground trade components are responsible for dealing with buyers' online transaction, while background management components are responsible for dealing with banks managing and querying online components. The framework is given in the figure.

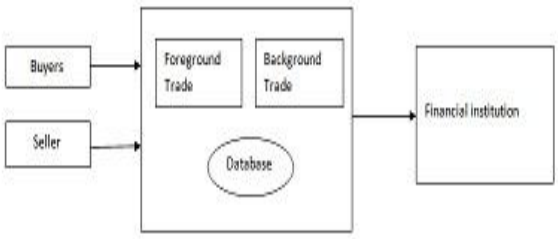

Fig4. Third party system payment [2]

Buyers and sellers register themselves with the TPP system. This enables them to obtain virtual account. These virtual accounts are connected to real accounts. This is used to transfer the money is real account to virtual currency in virtual account which is used in online trasaction.TPP achieves this by building a connection between platform and banks. Functions related virtual money and credit card account are also provided by TPP. During the money transfer the money is money is kept by the third party temporarily. If anything goes wrong with the transaction, the third party is responsible for negotiation with both sellers and buyers to decide what to do.

c. Problems associated with TPP

- The system cannot prevent customers' vicious cheating:

If a customer claims that they haven't received the product which they actually did then one cannot do anything. The problem is that there are lots of possible logistic can be chosen by the seller but it is impossible to check the flow of goods. Even if the system has a function the cost will be too much.

- Sellers may not receive money in time

In TPP model once the buyer gets the right commodity, they can login to the system and confirm the payment. If the system doesn't received in specific time the payment TPP transfers the money to the sellers. The problem is that the confirmation sometimes is not given due to consumer negligence and the given time is too long in some circumstances.

V. SECURITY PROTOCOLS

a. Security Socket layer Protocol

The Secure Sockets Layer (SSL) is a commonly-used protocol for managing the security of a message transmission on the Internet.[3] SSL has recently been succeeded by Transport Layer Security (TLS) which is based on SSL. SSL uses a program layer located between the Internet's Hypertext Transfer Protocol (HTTP) and Transport Control Protocol (TCP) layers. SSL is included as part of both the Microsoft and Netscape browsers and most Web server products. Developed by Netscape, SSL also gained the support of Microsoft and other Internet client/server developers as well and became the de facto standard until evolving into Transport Layer Security.[4] The "sockets" part of the term refers to the sockets method of passing data back and forth between a client and a server program in a network or between program layers in the same computer. SSL uses the public-and-private key encryption system from RSA, which also includes the use of a digital certificate.

TLS and SSL are an integral part of most Web browsers (clients) and Web servers. If a Web site is on a server that supports SSL, SSL can be enabled and specific Web pages can be identified as requiring SSL access. Any Web server can be enabled by using Netscape's SSL Reference program library which can be downloaded for noncommercial use or licensed for commercial use.

In the TCP/IP model view, TLS and SSL encrypt the data of network connections at a lower sub layer of its application layer. In OSI model equivalences, TLS/SSL is initialized at layer 5 (the session layer) then works at layer 6 (the presentation layer): first the session layer has a handshake using an asymmetric cipher in order to establish cipher settings and a shared key for that session; then the presentation layer encrypts the rest of the communication using a symmetric cipher and that session key. In both models, TLS and SSL work on behalf of the underlying transport layer whose segments carry encrypted data

b. Secure electronic socket (SET):

Secure electronic transaction was developed by SET co, led by VISA and MasterCard (and involving other companies such as GTE, IBM, Microsoft, Netscape, RSA, Safe layer — formerly SET Projects — and VeriSign. VeriFone - who built one of the earliest Internet Payment gateways used by several leading banks, was also closely involved.)[3] Starting in 1996.It supports electronic commerce based on Certificate Authority. SET protocol includes payment section which is able to deal with different credit cards and it applies an acquirer payment gateway which is able to authorize the usage of existing bankcard network. In the authorization request sent by the merchant to the acquirer,

the purchase instruction of the customer enables the acquirer to verify that the merchant and the buyer agree as to what is purchased and how much is authorized. [4]

To meet the business requirements, SET incorporates the following features:

- Confidentiality of information
- Integrity of data
- Cardholder account authentication
- Merchant authentication
- Dual signature

SET made possible the work of information integration, verification of all financing data and coding of sensitive data. It realized financing payment safety work of assisting cardholders, supplier, payment request, payment authorization and records of payment by use of advanced technology like data coding and digital signature.

VI. CONCLUSION

In this paper, we defined the Web shopping cart system as a typical client-server application on the Web. We then mentioned the different methods which are used for the implementation of the shopping cart. We discussed the problems and difficulties related to each method and the different factors that are considered while implementing.
The platform of Third Party Payment was taken into consideration while the essential security protocols needed while the implementation was discussed.

From the above analysis we can conclude that there is a need for robust method for implementation of shopping cart or online shopping application in the future with security and safety of the stake-holder as the most important factor.

FUTURE WORK

There is always a need of development in this area of security as anything less than 100% secure is not acceptable.. There is always the case of increase in the kind of security threats so this factor should always have higher priority and continuous evolution is required.

ACKNOWLEDGEMENT

“Authors would like to thank Mr. Santosh Shelke for his guidance and cooperation”.

REFERENCES

[1] Satoru Uehera, Osamu Mizuno, Tohru Kikuno “An implementation of Electronic shopping cart on the Web system using Component-Object Technology”, IEEE Transaction 0-7695-1068-WO1 2001.
[2] Chuanjin Jiang Shanghai, Wenguan Song “An online Third Party Payment Framework in E-Commerce” 978-1-4244-5848-6/10 ©2010 IEEE
[3] Daud Khan,Praveen Varshney, Mohammed A Oadeer “E-Commerce: From Shopping Carts to Credit Cards” 978-1-61284-486-2/111 ©2011 IEEE
[4] http://en.wikipedia.org/wiki/Transport_Layer_Security
[5] http://en.wikipedia.org/wiki/Secure_Electronic_Transaction
[6] Ying Yin, Liang-rong Song “The Issue and Risk Analysis of the Credit Card” 978-0-7695-4527-1/11 © 2011 IEEE
[7] Shafiq ur Rehman, Jane Coughlan “Building Trust for Online Shopping and their Adoption of e-Commerce” 978-1-908320-05/6/©2012 IEEE