Building an Enterprise-Class Electronic Commerce in Nigeria

R. Olufemi Akinyede
Department of Computer Science
The Federal University of Technology, Akure

ABSTRACT

Buying and selling on the Net (e-commerce) is no more new to both the developed and developing nations. The issue now lies with the effectiveness of the existing payment system and the ICT infrastructures in place. This research examined the problems of the existing payment system in Nigeria and proposed a new one that would take care some of the limitations of the existing ones. The architecture of the proposed payment system was designed and coded using HTML to design the interfaces, JAVA Scripts as the scripting language that connects the front-end with the back-end and MySQL as the database. Application software was developed to simulate the design model using NetBeans IDE 6.9, MySQL database system and Java ME programming language. The simulation runs were done and hosted on www.elexsoft.com/mobilepaymentsystem/ and implemented on mobile browsers using Samsung android GT-S5830D smartphone, 800 Mhz Intel processor mobile phone. The system uses the most common method of authentication which is user name and password.

Keywords

Internet, AES, payment system, goods and services

1. INTRODUCTION

Commerce, in the real sense of it started over two thousand years ago. The people that people have engaged in it have adopted tools and technologies that became available. According to [1], in ancient times, the advent of sailing ships actually paves ways of new trade to customers and merchants. In manner, innovations, such as the printing press, steam engine, and telephone, also changed the way in which people conduct buying and selling activities. Currently, the introduction of Internet has really changed the way people perform or organize business activities. The new technology has proved itself in many ways and more rapidly than any other technology so far in the history of business. At the tip of one's finger and comfort of one's home, transactions that worth millions of Naira can be performed. There are three (3) categories of e-commerce and they are:-

1.1 Consumer–to-Consumer (C2C)

C2C which can be treated as part of B2C is a situation where two or more parties can buy and sell goods to each or one another online.

This is a situation where business organizations sell products or services to individual persons known as consumers [2,3]. For example, First Bank Plc sells chairs to individual persons.

1.2 Business–to-Business (B2B)

This is a situation where business organizations sell products or services to another business organization. B2B has a longer sales cycle and a smaller, but more focused target audience [3]. For example, a commercial banks selling products to another other commercial banks.

2. THE DEVELOPMENT AND GROWTH OF ICT

It is no more gain-saying that the number of users of Internet has increased explosively as a result of the rapid growth in information technology (IT) industry. According to the International Telecommunication Union (ITU), [4], in 2000, the figure of the Internet users was 200,000 whereas in 2013 it was 67,319,186 which showed a percentage increase of 33,560% in Nigeria. Broadband satellite, *very small aperture terminal* (*VSAT*) [5] and wireless telephony technologies have provided wonderful opportunities for Nigeria to leapfrog in the information society age. These technologies have been exploited in order to accelerate information technology (IT) that leads to a cashless society development in Nigeria [6,7]. Many state governments have accorded ICT a priority. These states have information units directly under the control of and finance by the state governors. They work in hand with the National Information Technology Policies (NITP) and the National Information Technology Development Agency (NITDA). NITDA is the body responsible for facilitating ICT growth for development in Nigeria. Presently, the Internet users in Nigeria are approximated to 67,319,186 totalling to about 38.0% of her population [4]. In the same manner, Nigeria being Africa's largest mobile market with more than 125 million subscribers and a market penetration of around 75% in early 2014, has not been able to fully utilized the opportunities of mobile phones [8].

3. THE DEVELOPMENT AND GROWTH OF E-COMMERCE

The development and growth of e-commerce is a function of confidence that comes from trust that exists between the participants, business and government in the e-commerce environment. In Neilson's survey, it was revealed that the worries of consumers about doing web transactions were credit card transmission, privacy and authentication issues [9]. Online transaction suffers an array of electronic risks, which includes fraud, theft, and disruption of service and loss of consumer confidence. According to Gary's report [10] on the Statistical Abstract of the United States, 2008, Washington: U.S. Census Bureau, it was reported that in 1996 B2C Sales was less than 1$ Billion where as it was estimated to be more than 360$ Billions in 2011 in the U.S.. Likewise, in same 1996 B2B Sales including EDI was 460$ Billions and it was estimated to be 9500$ Billions in 2011. It was also reported that Intel accepts more than 98 percent of its orders (more than $38 billion per year) through the Internet. Intel also purchases billions of dollars' worth of supplies and raw

materials on the Web each year. The total volume of all worldwide business activities on the Web is expected to exceed $9.8 trillion by 2011 [1]. This also can be the case in Nigeria in few years to come if e-commerce can consider and take advantage of a payment system that can be anchored by the recent development and growth of ICT in Nigeria.

4. RELATED WORKS

In [11], a general purpose e-commerce store where products like books, CDs, computers, mobile phones, electronic items, and home appliances can be bought at the comfort of home through the Internet was implemented. However, the system could not handle multiple processing at the same time and credit card validation could not be achieved. Akinyede, [12] proposed a secured e-commerce payment system that can be used in a wireless (mobile) network. In his work, he developed a model that defined the relationship and interaction among engaging participants in any payment system. He also formulated performance indices such as protocols and cryptographic techniques that would increase transaction performances of the system. In his work, Liu's [13] protocol was adapted. However, the security of the client-side of the system was not properly handled. Sufyan [14] emphasized the importance of some basic security properties or requirements such as confidentiality, integrity, non-repudiation, replay protection and entity authentication in his report. Sufyan, in his work, tried to design and implement a three-tiered architecture; however, the work is limited in that it did not give adequate privacy to information flow. Alexander [15] developed an e-commerce security and payment systems. In the work, he tried to secure the communication channels using SSL, VPNs, and protected the networks by building firewalls. However, Alexandra added lots of securities that eventually slow down the operation of the system. Finally, Pradnya, [16], developed a transaction security for e-commerce application that reduces costs, attain greater market reach, and increased relationships among engaging participants. However, the system could not adequately prevent loss of privacy with respect to transactions being performed by an individual on the e-commerce site.

5. THE PROPOSED SYSTEM

Having gone through some related literatures on the subject matter, we developed the proposed system by dividing it into three parts (see figures 1 and 2)namely: the 1. merchant server-side 2. customer-side and 3. payment-side.
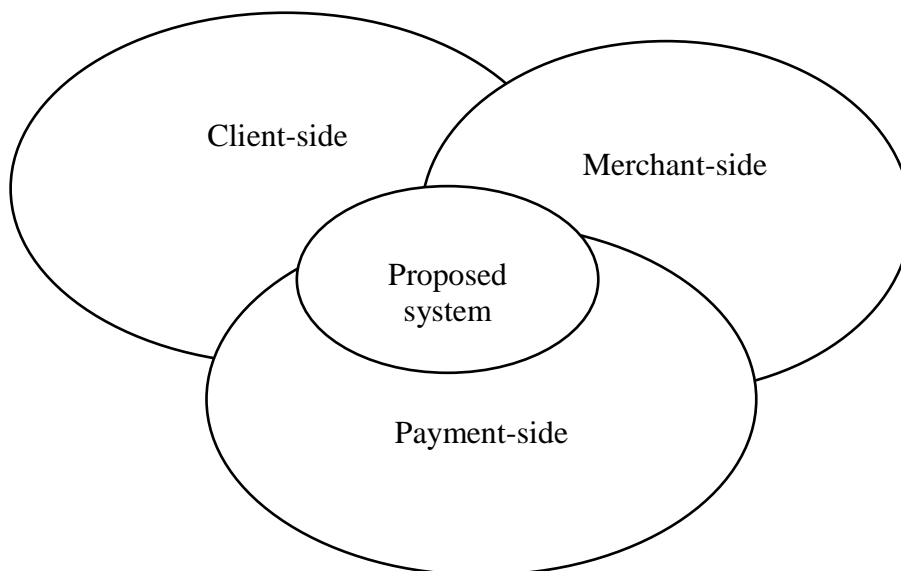

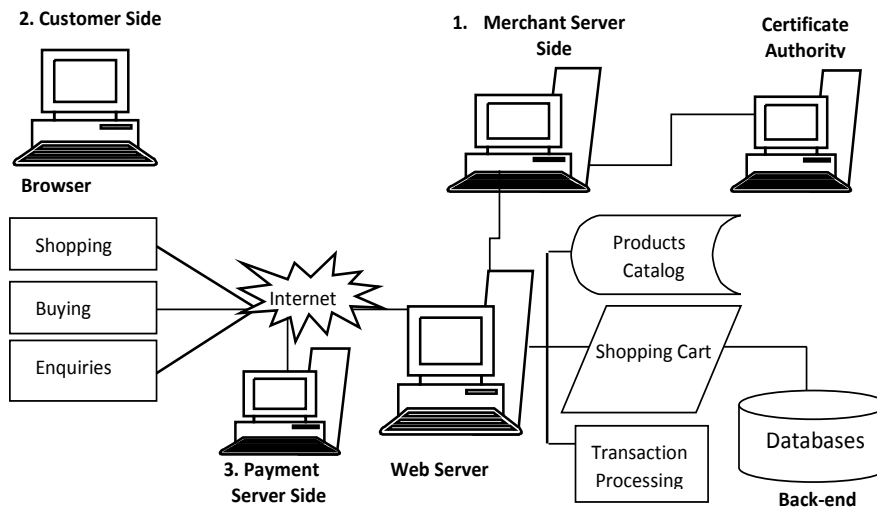**Figure 1: A Secure client-side E-Commerce Payment System Methodology**

Fig 2: Architectural design showing the merchant server-side, customer-side and payment-side of the proposed new payment system for an enterprise-class e-commerce in Nigeria

5.1 Merchant server-side

The merchant-side was developed using Java scripting and MYSQL. Here, adequate attention is given to customer's requests by running a script directly on the merchant web server to generate dynamic web pages. Interactive web sites that interface to databases and other data stores are also provided.

5.2 Customer-side

The customer-side was developed using HTML. It has a shopping cart where goods are stored temporarily and allows scripts to run by viewing web browser and performs the following functions:

5.3 Registration of New Users

Allowing registration of new users/ signing in of existing ones.

5.4 Customer's Request

Passing request made by customer to web/merchant server.

5.5 Storing of Information

Storing all transaction information in a set of data files.

5.6 Transaction Processing

Processing transactions and transfers fund appropriately.

5.7 Payment server-side

The key functions of e-commerce are products catalog, shopping cart and transaction processing. It deals with fund transfer. The payment-side uses payment gateway system (wallet). The back-end database will allow storage of users and product catalog and the web will be the means for users to interact or retrieve information from the database. The payment gateway will process the information of the ATM cards as provided by the customers.

Finally, figure 2 is secured for e-commerce transactions because security was considered at the design stage for the needs of the network.

5.8 The basic functions of an e-commerce

A good e-commerce application must provide the following:

5.8.1 Product Catalog

It organizes the goods and services being sold. It lists goods and services so that interested customers can select items to be purchased. With it in place, the merchant can make additions, deletions and edition of items in store.

5.8.2 Shopping cart

It allows customers select items they wanted to purchase by displaying an interface that asks for selections. To order for desired items, the customer simply clicks on the items and when this is done, all of the details about the items, including their prices, products numbers, and other identifying information, such as billing and shipping information, will be stored in the cart. The cart will keep a running total of each type of item. It will calculate the total as well as sales tax and shipping costs.

5.8.3 Transaction processing

It allows the e-commerce system to perform the required calculations, such as volume discounts, VAT, and shipping costs.

6. SYSTEM IMPLEMENTATION PHASES

We made use of MySQL relational database management system (RDBMS) program to serve as a tool for storing and maintenance of data. This will enable users who want to input large amount of information and perform calculations at the same time [16, 18]. However, in e-payment system, server stores records of every transaction.

6.1 Customer-Merchant registration

The proposed system allows a preliminary registration process for both the customer and merchant. This is important because it will prevent eavesdropping and protects customers' sensitive data. This is the first step for customer registration. The customer clicks on register new user and supplies his details including the information on the credit card that he wants to use with Certificate Authority (*CA*).

6.2 User interface

The merchant and customer interfaces are the two (2) interfaces that were considered. The merchant interface is for

uploading and displaying of items for shopping. The customer interface links the customers to the server. It takes all inputs from the customers, and passes them to the server's database system. The customer use the interface to determine what goes into the server. A Click will request the customer to enter his user name and passwords (see figures 3 and 4 for welcome and login pages). The login authentication is hereby presented
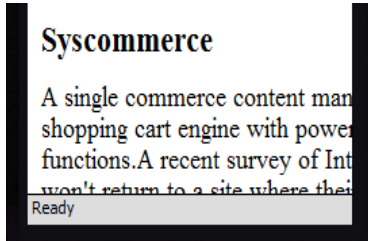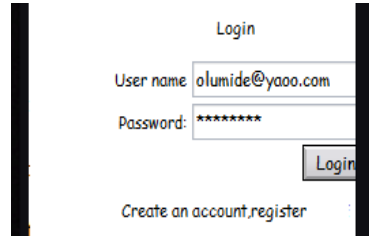

Fig. 3: Welcome page

Fig 4: Login page screen

Let *U* represent either merchant or customer. When *U* wants to access the certificate authority (*CA*), the following steps will be carried out:

U submits the computed *ID, yId* and *Id* and generates random number *a*, such that $a \in [1, n-1]$.

Calculates $Q_i = q_iP$ and then $p_i = h(Q_i)$, $X = q_iK_{pub\_ib}$ and $g = h(ID\|Id\|p_i\|T_i)$

Select random number *a*, calculates $Q_i = q_iP$ and then $p_i = h(Q_i)$, $X = q_iK_{pub\_ib}$ *and* $g = h(ID\|Id\|p_i\|T_i)$.

U computes the hashed password $Y = yId$, dynamic identity $dID = p_iH(ID_i)$ encrypted and sends message to *CA server*
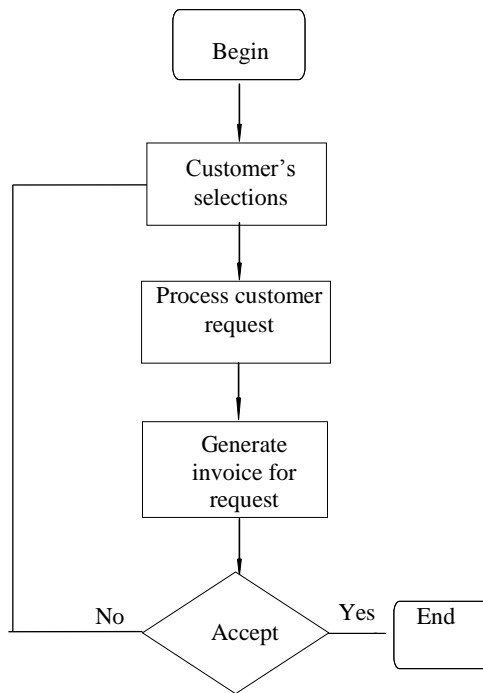

Fig 5: Data Flow Diagram for Viewing Purchase Details at the Customer's side

Decrypt $p_iH(ID_i)$

Verify both certificate & signature

If the entry is *successful*, customer will gain access to the system. Customer though the interface will choose a desired merchant and select items from the items' list (e.g the system displays item ID, item price, and the required quantity and total amount of the purchased goods) and add them to the cart. He can make other purchases also (Figure 5). At the end of his selection, the system will begin payment initialization as follows:

6.3 Payment Initialization

Verify *PIN*

IF PIN is *correct* THEN

$\{mp \ \ A: [[\text{PI, signed}], C\ ID]\}$

ELSE *terminate*

$\text{C} \rightarrow \text{M}: \{\{Ordered\ Items, Transaction.ID\ \ , M_{ID}\}K^{-1}\}K^{secret}$

$\text{M} \rightarrow \text{C}: \{Item, M_{ID}, Transaction.ID\ \ , ID_{\text{CA}}\}K^{secret}$

$$\text{C} \rightarrow \text{M}: \{\{PaymentOrder, Transaction.ID\ \ , M_{ID}\}K^{-1}\}K^{secret}$$

6.4 Payment Subtraction Request

$C \rightarrow C's CA: \{M_{ID}, Transaction.ID\ \ , ID_{\text{CA}}, AMOUNT,$

$$DATE, H(M_{ID}, Transaction.ID\ \ , ID_{CA}, AMOUNT, DATE),$$

$\{\text{R, DESC}\}\ K_2\}\ X_i, \text{i}, C_{ID}$

$$C's\ CA \rightarrow TC: H[\{M_{ID}, Transaction.ID\ \ , R, ID_{CA}, \quad AMOUNT,$$

$$DATE, H(M_{ID}, Transaction.ID\ \ , ID_{CA}, AMOUNT, DATE),$$

$\{\text{R, DESC}\}\ K_2\}\ X_i, \text{i}, C_{ID}]$

$M \rightarrow TH: \{\{\{PaymentOrder\}K^{-1}, K^{secret}\}K^{-1}\}K^{secret}$

$TH \rightarrow M: \{\{\{Result, K^{secret}\}K^{-1}\}K^{secret}$

$$M \rightarrow C: \{\{Result, K^{secret}\}K^{-1}\}K^{secret}$$

6.5 Payment Authorization Request

$C's\ CA \rightarrow M'sCA: \{R, M_{ID}, Transaction.ID\ \ , \ \ AMOUNT, DATE, \{\text{R, DESC}\}\}K^{secret}$

In steps (D) - (E), the customer pays for the ordered items and obtains the decryption key.

6.6 Delivery Request

After payment has been made, *M* will send confirmation to *C* and delivery process will begin.

6.7 Payment Confirmation Request

$M's\ CA\ \rightarrow M: \{R, Transaction.ID\ \ , \ \ AMOUNT,$

$DATE, \{\text{R, DESC}\}\ K^{\text{secret}}$

$$H(R, Transaction.ID\ \ , AMOUNT, DATE, \{\text{R, DESC}\}K^{\text{secret}}), H\}\ Y_i, \text{i}$$

6.8 Payment Confirmation Response

$M \rightarrow M's\ CA: \{Yes\ or\ No,\ H(K_{p-p}),$

$$H(R, Transaction.ID\ \ , AMOUNT, DATE, \{R, DESC\}, K^{\text{secret}}),$$
$$\{Yes\ or\ No, Transaction.ID\ \ , AMOUNT, DATE\}, K^{\text{secret}}\}Y\}K_{i+1}$$

6.9 Payment Authorization Response

$M's\ CA \rightarrow TC: H[\{Yes\ or\ No, \quad H(K_{p-p}), \quad H(R, Transaction.ID\ \ , AMOUNT, DATE, \{R, DESC\}, K^{\text{secret}}),$

$$\{Yes\ or\ No, Transaction.ID\ \ , AMOUNT, DATE\}K^{\text{secret}}\}Y_{I+1}$$

$$TC\ \rightarrow M'sCA : TC2$$

$$M's\ CA \rightarrow C's\ CA: Yes\ or\ No, Transaction.ID\ \ , \ \ AMOUNT, DATE,$$

$$(Yes\ or\ No, Transaction.ID\ \ , AMOUNT, DATE\}K^{\text{secret}}$$

$$\text{M} \rightarrow \text{C}: \{\{CONFIRM, \text{mname, amout}\}K^{-1}\}K^{secret}$$

6.10   Payment Subtraction Response

$C's\ CA \rightarrow C's\ \{Yes\ or\ No, H(K_{p-p}),$

$$H(M_{ID}, ID_{\ CA}, \text{R}, Transaction.ID\ \ , AMOUNT, DATE),$$

$\{Yes\ or\ No, Transaction.ID\ \ , AMOUNT, DATE\}K^{secret}\}X_{i+1} \rightarrow \text{M}: \{\text{Received},$

$$H(K_{p-p}), H(R, \; Tansaction.ID \;,$$

$$AMOUNT, DATE\} \, K^{secret}\} X_{i+1}$$

Upon transferring the amount from *I* to *A*, *A* sends the credit information to *C through I*. The important issue of sending payment confirmation note is completed under the banking private network.

I sends message to *C* that contains the payment *CONF*irmation.

I → C: Confirmation *ACK*nowledged

Since customer has a registration number and password, he can always check the status of his purchased up till the time of delivery. When the goods finally arrive, the shipping agent can easily call the customer in case the customer is not found in the delivery address to notify him of the arrival of his goods.

6.11   Delivery of Goods Update

M shipped ordered goods to *C*'s address

$$M \rightarrow C: \{\{Ordered \; Items, \quad ACKnowledgment, Transaction.ID \;, C_{ID}\} K^{-1}\} K^{secret}$$

C→M: Goods delivery CONFirmation/ACKnowlegment

The network operator makes sure the generated keys have not been used before committing payment and if peradventure any of the keys has been used, such keys will be discarded to prevent re-use or replay attack

7. CONCLUSION

Literatures have shown that enterprise-class e-commerce applications usually require several dedicated computers in addition to the Web server system because large organizations can use them to run their online businesses. Though lots of researches have been conducted in this area, but unfortunately, many of them are practicable or implementable. As a result, this paper has tried to showcase a modeled new payment system for an enterprise-class electronic commerce in Nigeria.

8. REFERENCES

[1] P. S. Gary, "Electronic Commerce". Ninth Edition© 2011 Course Technology, Cengage Learning.

[2] D. Murphy, "Marketing for B2B vs. B2C – Similar but Different". Published in 2007. http://masterful-marketing.com/marketing-b2b-vs-b2c/

[3] W. Teri, "Content Marketing Examiner". Published in 2013. http://cmexaminer.cadence9.com/strategy/creating-b2c-buyer-personas-for-effective-content-marketing/

[4] ITU, "Local NICs and other local sources". Internetworldstats.com. Copyright © 2014, Miniwatts Marketing Group. All rights reserved. http://www.internetworldstats.com/stats1.htm#africa

[5] L. Fabio, "The Rise of Wireless Broadband. Fixed Wireless Systems, Radio-communication Bureau", ITU. Published in 2004. www.intercomms.net/…EB04/docs/wirelessbroadband.php

[6] G. O. Ajayi, "African Response to the Information Communication Technology Revolution. A case study of the ICT Development in Nigeria". Published in 2002 (ATPS Special Paper Series No 8). p.1. http://www.amazon.com/response-information-communication-technology-revolution/dp/9966916288

[7] R. O. Akinyede, O. S., Adewale, and O. K. Boyinbode, "Towards a Sustainable Agricultural Development in Nigeria: Taking Advantage of Distance Education and eLearning, Anchored on Computer Technology", in proceedings of International Conference on e-Learning, e-Business, Enterprise Information Systems, and e-Government (EEE'08) - at the 2008 World Congress in Computer Science, Computer Engineering, and Applied Computing (WORLDCOMP'08), July 14 - 17, 2008 in Las Vegas, Nevada, USA, 519-525.

[8] Paul Budde, "The largest telecommunications research site on the internet". http://www.budde.com.au/Research/Nigeria-Mobile-Market-Insights-Statistics-and-Forecasts.html?r=51

[9] R. O. Akinyede, "Development of a Payment System for e-Commerce and banking industry in Nigeria". A Thesis Submitted for Fulfillment of the Requirements for the Degree of Masters of Technology, Computer Science, The Federal University of Technology, Akure, Nigeria. Published in 2005.

[10] U.S. Census Bureau, Forrester Research and the Statistical Abstract of the United States, Washington. U. S, Adapted from reports by ClickZ Network Published in 2008 (http://www.clickz.com/stats/stats_toolbox/); eMarketer (http://www.emarketer.com/); and Forrester Research (http://www.forrester.com).

[11] Swapna "The design and implementation of an E-Commerce site for online book sales". Published in 2007 https://www.iusb.edu/math-compsci/_prior-thesis/SKhodali_thesis.pdf

[12] R. O. Akinyede, "Modelling a Secure e-Commerce Payment System for Wireless (Mobile) Network in Nigeria": Ph.D Project Report, Department of Computer Science, The Federal University of Technology, Akure, Nigeria. Published in 2012.

[13] Y. Liu, G. Wen, Y. Hongxun, and Y. Xinghua, "Elliptic Curve Cryptography Based Wireless Authentication Protocol". International Journal of Network Security, Vol.5, No.3, PP.327–337, Published in 2007. https://www.academia.edu/4989125/Elliptic_Curve_Cryptography_Based_Wireless_Authentication_Protocol

[14] T. F. Sufyan, "Development of a Secure SET-Based E-Commerce System". Published in 2008. *icit.zuj.edu.jo/icit07/PaperList/Papers/384faraj.pdf*

[15] Alexander "Development of an E-Commerce Security and Payment Systems". Published in 2002

[16] B. R. Pradnya, "Transaction Security for E-Commerce Application". Published in 2012. *www.ijecse.org/wp.../2012/08/Volume-1Number-3PP-1720-1726.pd*

[17] D.J. Date, "An introduction to Database System", ISBN 0-201-824582, Seventh Edition, the System Programming Series, Addison-Wesley Publishing Company, Published in 1994. http://avaxsearch.org/?q=An%20introduction%20to%20database%20system

[18] P. P. Hun, "Design and Implementation of Secure Electronic Payment System (Client)". World Academy of Science, Engineering and Technology, Published in 2008. http://waset.org/publications/7025/design-and-implementation-of-secure-electronic-payment-system-client-.