DEVELOPMENT OF SECURED E-COMMERCE DIGITAL LEARNING (SEDL) FOR NIGERIA EDUCATIONAL SYSTEM

Owamoyo, N. & Sulaimon, H. A.
Computer Science Department, Federal College of Education, Zaria, Kaduna State, Nigeria.
E-mail: najolp@yahoo.com **Phone:** +2347039090222.

Abstract
The Website is a useful tool for teaching basics e-commerce, because students can actually list items for sale, receive payments, and fulfill orders. Therefore, for the purpose of this study, there is a need to develop and improve an e-commerce application called Secure E-commerce Digital Learning (SEDL) for Nigeria Educational System. This paper therefore looks into the necessary steps to develop an e-commerce application and implement security framework for online ordering system. It also investigates security threats and other problems that e-commerce customers and merchants face. The Secured Electronic Transaction (SET) protocol and cryptographic hash function are used to develop SEDL to encrypt all the information through the communication channel between client-server, to assure Confidentiality, Integrity, Authentication Content Assurance, Non-Repudiation and other security services. Thereafter the paper recommends among others that Government should as a matter of urgency formulate and implement policies that would enhance the development and deployment of a Secure E-commerce Digital Learning (SEDL) to demonstrate the use of secured web application for sustainable development of educational system.

Keywords: E-commerce, Digital Learning, Protocol, Cryptographic, Client-Server

Introduction

E-commerce is a new business activity pattern and one of the main driving forces of the knowledge economy (Yeh *et al.,* 2012). However, the industrial sector and educational sector have different perception on e-commerce management. Yazdanifard and Zargar (2012) argued that some companies emphasize business e-commerce marketing management functions, while other companies focus on e-commerce management information functions or network design and development. Nevertheless, e-commerce technology has played an increasingly important role. Therefore, integrating information technology and business operations to promote the development of e-commerce and help students to develop e-commerce technology literacy will rely on the continuing efforts of e-commerce education. It is therefore important to look at how to make full use of the school resources of information technology and thereby enhance students' information technology literacy to achieve the objective of digital learning e-commerce in Nigeria education system.

The study conducted by Diwakar and Marathe (2000) stated that over three quarters of 10,000 respondents from online questionnaires on purchased items, using the web for personal shopping was convenience (65%), followed by availability of vendor information (60%), no pressure from sales person (55%) and saving time (53%). Although the issue of security remains the primary reason why more people do not purchase items online, the Gross Value Added (GVA) survey also indicates that faith in the security of e-commerce is increasing. As more people gain confidence in current encryption technologies, more and more users can be expected to frequently purchase items online (Pathak and Manju, 2010). Optimally, these tools should be completely automated, robust, expressive, and easily usable, so that they can be integrated into the protocol development and standardization processes to improve the speed and quality of these processes.

The required security services for an e-commerce protocol include confidentiality, fair exchange, content assurance and non-repudiation (Ray, 2001). Non-repudiation protects parties against each other from falsely denying having sent or received an item during a transaction. While Fair exchange ensures that either all involved parties receive expected items or no party receives any valuable item. It guarantees that a merchant and students involved in a transaction receive the payment and the e-good respectively. The purpose of this study is to examine the existence and develop a new secured digital learning e-commerce application capable of providing ordering and delivering items, products to the students and the merchant.

Related Works

Electronic commerce, commonly known as e-commerce, consists of buying and selling products, Information and services over the Internet (Hanson and Kalyanam, 2006). E-commerce transactions allow the purchase of valuable electronic goods (e-goods) from online websites application. It provides customers with the flexibility of purchasing without leaving the houses with just few clicks, but as a result of vulnerability of communication channel through client-server in e-commerce. Some of the security threat that undermined the use of web includes; Man In The Browser attacks (MITB), Packet sniffers, DOS, and Identity claiming/theft.

Zhang (2010), presented e-commerce web application related issues. He compared several related technologies such as ASP.NET, Java 2 Enterprises Edition (J2EE) and Window Apache MYSQL and PHP (WAMP) and considered the advantages and disadvantages of performance based on several different benchmarks-iteration tests. Previous studies have shown that such models are opened to vulnerability and it is opened and did not address the issue of security in e-commerce application. Abdul *et al.,* (2011) presented hybrid model for securing e-commerce transaction. In their research work, protocol for securing e-commerce transaction by using hybrid encryption technique was designed. The idea was to improve the Diffie -Hellman key exchange by using truncated polynomial in Discrete Logarithm Problem (DLP) to increases the complexity of this method over unsecured channel.

The hybrid encryption method increases the performance of cryptographic algorithms, the Message Digest 5 (MD5) hash function provides the integrity and the modification of Diffie-Hellman to ensure the authentication, the experimental results showed that the model provide security service for e-commerce transactions to some extent, but failed to address non- repudiation, interacting performance, and high quality security service for desired e-commerce transactions.
Ho (2012) pointed out that the effectiveness of digital learning depends on technological support, institutional culture, staff development and students' receptivity and learning behaviors. He found that teachers and students have some obstacles to integrate information technology into teaching methods: (a) lack of sufficient time to learn or practice how to prepare teaching using the computer, (b) lack of time for students to use computers in the classroom, (c) lack of sufficient computers, (d) lack of good educational software, (e) lack of support in integrating internet technology and curriculum, and (f) lack of enough training opportunities.

The proposed security framework for the ecommerce digital learning will enhance secure environment to curtail the threats posed to confidentiality of information, fair exchange, content assurance, non-repudiation of information exchange, interacting performance, and high quality security service for desired e-commerce transactions among the students. In order to restore the trust and confidence that exists between the parties in digital learning e-commerce application, some issues are considered in the processes which are as follows;
i. A party fair exchange SET protocol will be introduced, a protocol that can be used as a building block to provide the ability to securely and fairly exchange e-goods among multiple parties in a digital rights management system. Cryptography will be introduced for authentication and also feedback mechanism will also be considered in the design of the application.
ii. How to increase school teachers' ability to integrate information technology into digital learning which is the key in promoting information technology in Nigeria education System.

Ching-San (2014) carried out researches on E-Commerce Digital Learning by Commercial Vocational Students in Taiwan where Learning Questionnaire was employed to gather student feedback on their learning with the 3D imaging technology system. The feedback collected was then analyzed using t-test and Analysis of Variance(ANOVA). Results indicated that integrating 3D imaging technology into e-Commerce promoted the e-Commerce technology literacy of students. His result shows that there was no gender difference in e-Commerce technology performance, but some differences did exist among students from different majors, failed to address how to develop e-commerce digital learning and its desired security service.

Methodology

The purpose of this section is to show the design process behind the website which consists of design process in the e-commerce system application and the implementation of security framework. A review of related studies of the existing research efforts on the problem domain were studied, which explore possibility of developing a secure e-commerce web application. It involves investigation of the current techniques used for designing and detecting the vulnerability of the existing system. Technically, a functional e-commerce website application was developed named Secure E-commerce Digital Learning (SEDL). The technologies used consist of Hypertext Preprocessor (PHP) and JavaScript. PHP was decided to be used within this study as it has very good compatibility with MySQL databases, and the query structures used in PHP are almost identical to those used in the MySQL command line therefore easy query testing can be achieved. PHP generally runs on a web server, taking PHP code as its input and creating Web pages as output.

The security measure was implemented in SEDL by using the designed security framework, cryptography and SET Protocol. The developed system will integrate web services together to ensure the free, flow and safe transmission of packets across the network for ordering, payment and delivering of product in digital learning e-commerce.

The stage is further divided as follows:

(a) Presentation and Testing of e-commerce data to carry out experiment to determine the weaknesses and strengths of the existing methods
(b) Demonstrating using the dataset collected and draw conclusion base on the experiment

Description of the System and Security Framework for SEDL

Secure E-commerce Digital Learning (SEDL) provides convenient environment for students to search and order many different kinds of products. The system is divided into front-end side (user side) and back-end side (Administrator side). There are modules such as registration, browse products, search products and order.

Front-end Side has the following modules: User Registration User Login / Logout User Center (my information, my order, my favorite, and my comments) Search Engine (use category or key word to search, advanced search). Shopping cart order query shop notice and articles friendly reminders email. This article category management comprises of add, delete, update. Also, view history, check out and add products to favorite.

Management Side has the following modules: Products Category Management: add, delete, update, query Products Management: add, delete, update, query Member Management and check order manifest, product delivery status. In summary the description of the system captures the following activities:

a. Collection of idea among group of students on item that could be sell or buy via online.
b. Choose an item to sell on SEDL.
c. Photograph the item with a digital camera.
d. Search SEDL for a completed listing for a similar item. Use other seller listings to make comparison and get ideas for the item category, price, item description, and terms.
e. Description of the item, and include payment and shipping terms.
f. Create web listing (with photo) and list the item for sale on SEDL.
g. Send an invoice to the respective buyer.
h. Receive payment.
f. Fulfill the order by packing and shipping the item

SET and E-Commerce Application

Security framework will be used to present the system, the system will be developed and validated using e-commerce network data set The Cryptography and secured protocol will be implemented and tested with the developed web applications that have proven to uphold the integrity and authenticity of information exchange and which will increase students' confidence.

SET employs a client /server architecture and provides user-to-server authentication rather than host-to-host authentication. SET is a protocol that provides encryption, decryption and security specification designed to protect the users and merchant in their transaction in the e-commerce

model. Security and authentication will be based on secret key technology where every host on the network has its own secret key. SET protocol provides the following features:

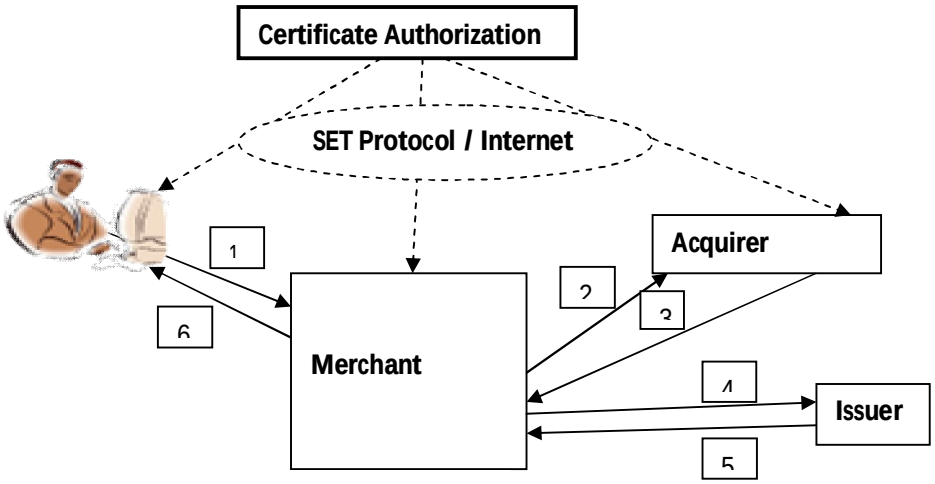
(a) Provides a secure communications channel among all parties involved in transaction
(b) Provides privacy because the information is only available to parties in transaction when and where necessary
(c) Provides trust and fair exchange by the use digital certificates

SET Messages Exchange in E-commerce Application

SET message components that are implemented for this E-Commerce application and their relevance and impact on the system is performed as presented in Figure 1.

Figure 1 presents a diagrammatic overview of SET, with the message exchanges presented in a SET protocol.

Security Framework in SEDL



KEYS

Message Exchange

Trusted infrastructure secured communication channel

Figure 1: Data Flow Diagram for SET Messages Exchange in SEDL

Consumer (Cardholder): In the electronic environment, consumers and corporate purchasers interact with merchants from personal computers over the Internet. A cardholder is an authorized holder of a payment card that has been issued by an issuer.

Merchant: A merchant is a person or organization that has goods and services to sell to the consumer. Typically, these goods and services are offered via a Web site or by electronic mail. A merchant that accepts payment cards must have a relationship with an acquirer.

Issuer: This is a financial institution, such as a bank, that provides the cardholder with the payment card.

Acquirer: This is a financial institution that establishes an account with a merchant and processes payment card authorizations and payments. Merchants will usually accept more than one credit card brand but do not want to deal with multiple bankcard associations or with multiple individual issuers. The acquirer also provides electronic transfer of payments to the merchant's account.

Certification Authority (CA): This is an entity that is trusted to issue public-key digital certificates for customers, merchants, and payment gateways. The success of SET will depend on the existence of a CA infrastructure available for this purpose

Exchange of SET Messages

The exchange of SET message to establish a secure communication; the context is summarized in the following six phases;

i. Customer browses website of the merchant, decides what to purchase and adds them to the shopping cart and determine the price. The customer then sends a list of the items to be purchased to the merchant, who returns an order from containing the list of items, their price, a total price, and an order number.
ii. Merchants have their own certificates to issue**;** A merchant who accepts a certain order from the user have two certificates in possession to issue for two public keys owned by the merchant: one for signing messages, and one for key exchange. The merchant also needs a copy of the payment gateway's public-key certificate.
iii. SET sends both order and payment information to the merchant, along with the customer's certificate. The order confirms the purchase of the items in the order form. The payment contains credit card details. The payment information is encrypted in such a way that it cannot be read by the merchant.
iv. Merchant's bank contacts the issuer and checks with the issuer for payment authorization.
v. Issuer authorizes the purchase and sends authorization to Merchant's bank server
vi. Merchant completes the order and sends confirmation to the Customer, and provides the goods or service. The merchant ships the goods or provides the service to the customer.

Shopping Cart application

The objective of this application is to provide the user an online website where they can order any product from the comfort of their home. A shopping cart is used for the purpose. The user can select the desired products, place them in the shopping cart and purchase them using a Credit Card. The user's order will be shipped according to the type of shipping selected at the time of placing the order. The shopping cart application being used in this paper is very simple and involves the use of a database table to store the contents of the shopping cart. Sessions support the logging in of a user and showing content according to their authorization level or personal preferences. In this research, to prevent the confusion between orders a cookie and session is set-up that allows easy identification of the products that relate to a particular customer using the site.

The sessionID is a key that allows registration of particular variables, often called session variables, the contents of these variables are stored at the server. The sessionID is the only information visible at the client-side. If, at the time of a particular connection to the website, the sessionID is visible either through a cookie or the URL, the session variables stored on the server for that session can be accessed. Session variables are used in this study, to carry out the details of the user, on the site and then allow the cart contents to be specific and the delivery details extracted from the database for the user.

Checkout Process

In the checkout application the cart contents and delivery details specifically for the customer logged in to the system based on session variables. The second page of the checkout process as the credit card details form that is validated using JavaScript, when these details are submitted, they are encrypted then transferred to the next page for display in the order summary and decrypted but in a real e-commerce application they would be transmitted to bank for processing. On this page, there are two buttons on this page, one allows the user to proceed with the checkout process and the other cancels the order and logs them out of the system.

It is essentially an order summary that displays the order details, the delivery details and payment details. This page is designed for the user to print out and keep for their records. To finalize the process, the user is requested to push the logout button that terminates the session and empties the cart, as well as storing the relevant details in a database.

Result and Discussion

This section discusses the process of implementation of Secure E-ecommerce Digital learning and evaluation that has been conducted. To start the Secure E-ecommerce Digital learning, open the project name in SEDL then select the lunch button. After opening the project, enter the user's login name and password, these are stored in user details in the Database as shown in figure 2.

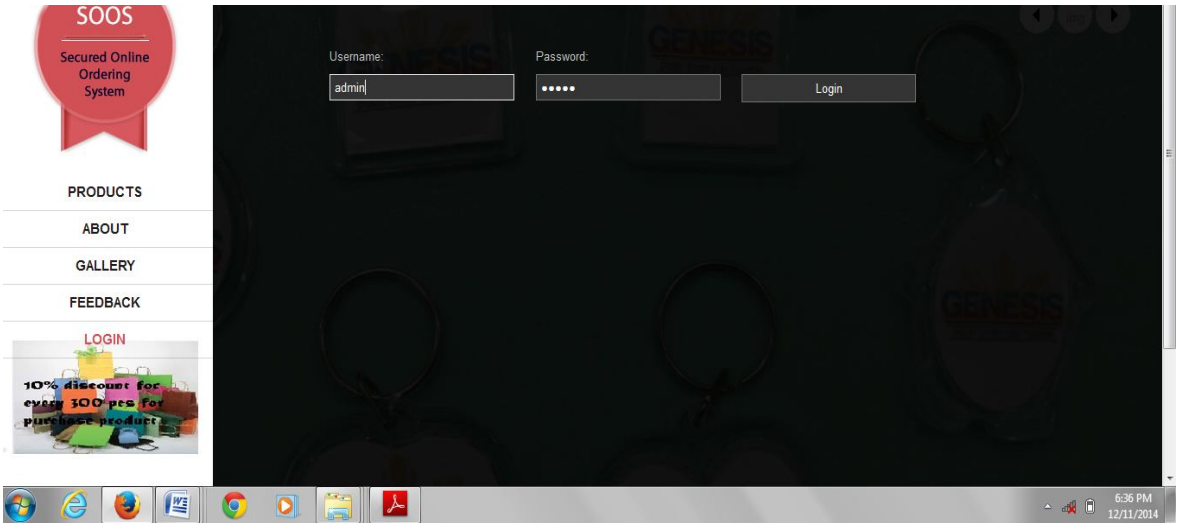


Figure 2: User Login and Password.

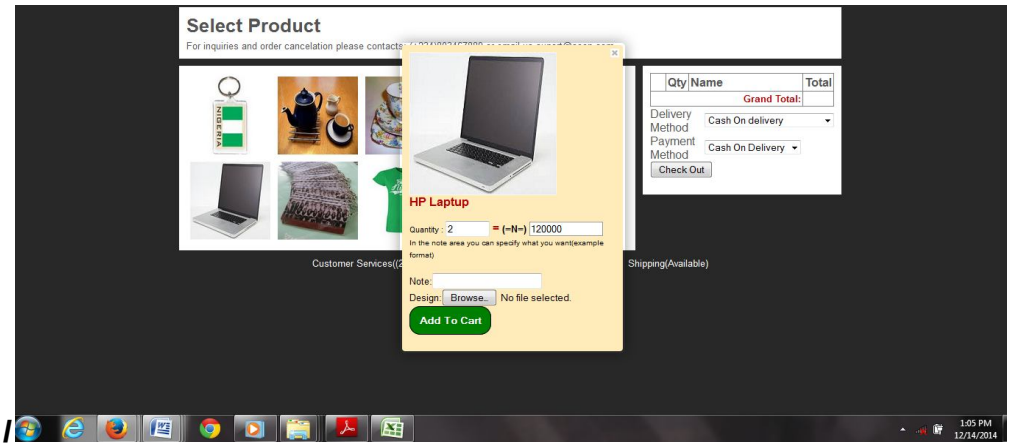


Figure 3: Display Selected Ordering Product with details of the Transaction

Figure 3 shows the “Selected Product”, enter the quantity needed and add to the chart then press the launch button. The total amount to be paid will automatically display. Also, the delivery method, which gives account for whether the product is based on cash on delivery, shipping to Nigeria and Shipping out of Nigeria. Payment, and Check Out allows the user to proceed with the checkout process to Figure 4.

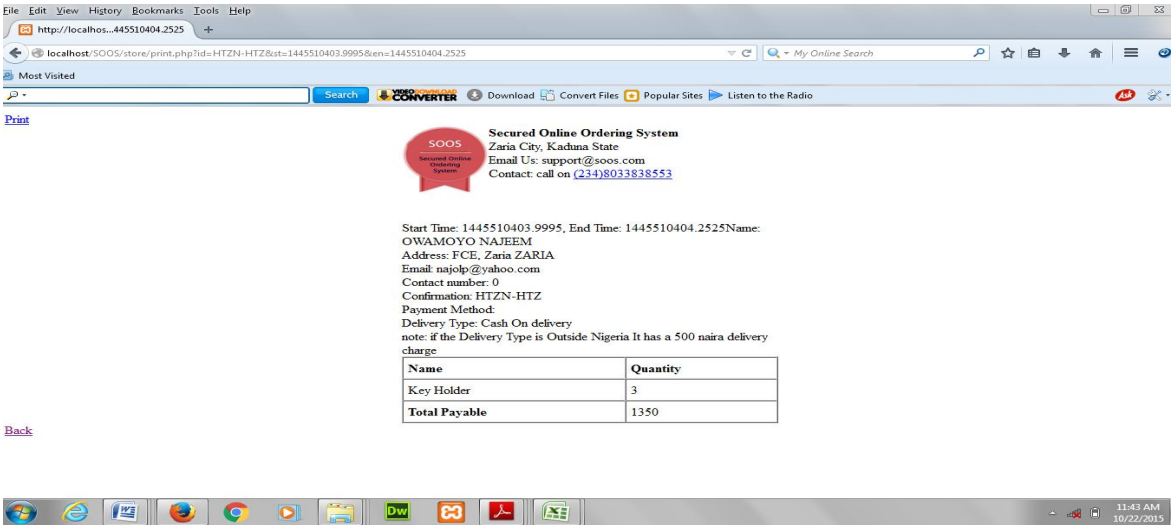


Figure 4: The Receipt of completed Transaction

Figure 4 shows the Receipt of completed Transaction which is designed for the final page in the checkout process. It is essentially an order summary that displays the order details, the delivery details and payment details. This page is designed for the user to print out and keep for their records.

Conclusion

In conclusion, it has been demonstrated that the proposed SET designed are more intuitive than the existing ones. On the same note, it was observed that satisfying security requirement is one of the most important goals for e-commerce system designers; in this study, SET protocol was used for securing transaction by using encryption process techniques. The encryption techniques surely will increase the performance of cryptographic algorithms. This protocol will ensure the confidentiality, integrity, authentication, non-repudiation and fair exchange, while providing high quality of securing services for desired e-commerce transaction. Lastly, a Secured Online Ordering System (SOOS) was developed to demonstrate the use of secured web application.

Recommendations

Government should as a matter of urgency formulate and implement policies that would enhance the development and deployment of a Secured Online Ordering System (SOOS) to demonstrate the use of secured web application for sustainable development. This work could then be enhanced to allow a search agent to purchase and pay for the goods and services based on the need of the user especially students. E-commerce merchants usually face the modification of data as it is transferred between the client and server which resulted in packet sniffing. This study recommends that data could be encrypted and a signature could also be applied so as to detect any modification that occurred as the signature would be different at the recipients' end from where it was originally sent.

References

Abdul M., Rahma D., Rabah N., and Hussam J. (2011). Hybrid Model for Securing E-Commerce Transaction. *International Journal of Advances in Engineering and Technology*, IJAET 1(5): 14-20.

Diwakar, H., Marathe, M. (2000). The architecture of a one-stop web-window shop. *ACM SIGecom Exchanges*, 2(1): 1-7.

Hanson, W. and Kalyanam, K.(2006). Internet Marketing and e-Commerce. Retrieved on July 20, 2013 from: https://lib.ugent .be/catolog/rugo1:00089/papers/P11.pdf.

Harrison, K**.** and Xu, S., (2007)." Protecting Cryptographic Keys From Memory Disclosure

Attacks," in *37th Annual IEEE/IFIP International Conference on Dependable Systems Networks.* 7(35): 25-40.

Ho, R. (2012). Educational technology: A brief retrospect and prospect in Taiwan. *Taiwan Education Review, 674*, 41-47.

Houmani, H., Mejri, M. (2012). Formal Analysis of SET and NSL Protocols Using the Interpretation Functions-based Method, *Journal of Computer Networks and Communications.* 20(12), 18-19.

Huang, T. (2013). Problem-solving approach to the analysis of development principals for information technology integrated with teaching. *Journal of Education Research, 236*, 57-71.

Nenadic A. (2005). A security solution for fair exchange and non-repudiation in e-Commerce. *Proceeding of IEEE international conference on circuit, Power and Computing Technologies.*University of Manchester, 4(4):12-27.

Pathak, H. K., Manju, S. (2010). Public key cryptosystem and a key exchange protocol using tools of non-abelian group. (IJCSE) *International Journal on Computer Science and Engineering*. 2(4): 27- 35.

Ray, I., (2001). Fair Exchange in E-commerce. Information in *ACM SIG proceeding in Ecommerce Exchange,* 4(1):16–19*.*

Yazdanifard R. and Zargar A. (2012). Today need of e- commerce management to e skill trainings *International Journal of, e- education e-business, e-management and e-learning, 2*(1), 52.

Yeh R, Chen Y., Kuo S, and Chung P. (2012). The trend of research topic classification of Electroniccommerce in Taiwan *Journal of Meiho University*, 31 (2), 41 – 62.

Zhang J. (2010). Development of E-commerce Web application using WAMP. A Thesis Presented to the Faculty of San Diego State University. Retrieved on July 11, 2013 from: *https://sdsu dspace.calstate.edu/ bitstream/handle/Zhang Jie.pdf.*