Sule Lamido University Journal of Science and Technology (SLUJST) Vol. 1 No. 2 [December, 2020], pp.68-78

Designing a conceptual Security Framework for Secure Online Ordering System (SOOS)

Owamoyo Najeem
Computer Science Department, Federal College of Education Zaria, Kaduna State.
najolp@yahoo.com

Abstract

The enhancement of internet technology has improved the security of online ordering system through the implementation of secure protocol in e-commerce application. ICT acquisition programmes enhance countries' ability to strengthen and involved in decision making which affect their live directly or indirectly and their entire wellbeing of her citizen. This paper therefore looks into the necessary steps to implement security framework for online ordering system (SOOS) in e-commerce application and also this paper investigates security threats and other problems that e-commerce customers and merchant's faces. Secure Online Ordering System (SOOS) was designed to show some area of security measure used to minimize the security threats encountered by both customers and merchants. The Secured Electronic Transaction (SET) protocol and cryptography are used in this research to prove clients detail to a server through an open connection. Advanced Encryption Standard (AES) and Message Digest (MD5) hash function are used for Password Based Encryption (PBE) for detecting data corruption and tampering and integrity of data message exchange between client and SET Protocol which are in turned encrypt the information through the interconnected channel in between client and server, to assure Confidentiality, Integrity, Authentication Content Assurance, Non-Repudiation and other security services. It is therefore recommended among others, that necessary attention should be accorded for designing good and secured shopping cart which must be connected with secure user-friendly shopping cart application.

Keywords*: E-commerce, Encryption, Cryptography, SET, SOOS*

1. Introduction

Electronic Commerce (e-commerce) involved buying and selling of goods, information and services via internet, with the help of just clicks on our computer system or smart phone many transactions could be achieved. It is an environment that provides a good network to users, merchant and people involved in this system (Hanson and Kalyanam, 2006). E-commerce provides opportunity to people to have sense of marketing through network, which make ecommerce transaction to be heterogeneous. The e-commerce application has become a usual place for online shopping. Security threat has been the major problem facing the application since inception; there is a need to address the issues. In order to attract more users and build robust system some of the following security threat most be resolved, Denial of service attacks, Confidentiality, Key recovery policy, Non repudiation, Padding attacks (Ashish *et al*., 2014).

The development of e-commerce has become a new driving force in many counties which include China. A good scenario is China's industry uplifting, economic and social improvement. Although the application has flourished greatly, many of the risks faced it, was caused due to information threat of online transaction that have not been greatly guaranteed in the aspect of legislation by the government or technology, as a result the customers' confidence to online shopping reduced gradually, which have hampered the growth of e-commerce in China (Qiaofen, 2018). The e-commerce has major role to play in china and other countries, has it provides some solution to the problem facing business transaction, because it has demonstrated effective and good results as the

major concern in IT technologies . The innovation has increased business, expand revenue and boost new jobs opportunity, it has about smart economy.

Akinyede, R. O. (2018) Proposed E-Commerce Framework, he gave an insight to how ecommerce services could be designed and customized by cloud services framework. He presented a cloud application layer in his framework that is available to end users. It was demonstrated that the layer provide consumers with web portal to access the services. The layer existed between the users and the cloud services which in turn provide various business services to the client. It was shown in his study that the clouds have good advantages over the ones that have yet to be introduced. The innovation of cloud services had brought about the necessary features to the ecommerce application. Certificate Duplicity, Authentication and remote access, Unsecure Database and Denial of Service Attacks were among the security issues raised in Tooba and Tauseef (2019) research work. A verification mechanism implemented in framework designed based on Service Oriented Architecture (SOA) was developed to assured the authentic customers are log in and perform necessary transaction in a secured environment.

The two major problems affecting e-commerce are; Privacy and security (Muneer *et al*, 2018). E-commerce has taken a stand in the worlds market in which people are willing to engage in it; despite the transaction on the system still portray a greater risk as a result of compromise of transactions which could result into non repudiation, financial loss and lack of confidence by the consumer. They ascertain that the growth of ecommerce rely on the security of the application; ecommerce security consist of five major categories; Integrity, Privacy, authentication, availability and non-repudiation (Kuruwitaarachchi *et al*, 2019).

Secure Online Ordering System (SOOS) framework is designed in this study, to show how some area of security measure could be used to stop the security threats encountered by both customers and merchants as it was mentioned by (Kuruwitaarachchi *et al*, 2019) work and related research work would be explored and necessary solution would be proffered. An improved Secured conceptual framework has been achieved in this research work through the encryption process; Encryption is the process of writing or encoding data in special format so that the content of the data would not be visible to the third party, in this paper encryption process has been employed to encrypt the data across the communication channel involving the combination of Secure Electronic Transaction (SET) protocol, Encryption Standard (AES) and Message Digest (MD5) hash function which are used for Password Based Encryption (PBE) for detecting data corruption, tampering and integrity of data message exchange between client and detail to a server through an open connection to assure the security services required.

2. Related Work

In this paper, review of related literature such as presented by Ashish *et al*. (2014) , Sibo *et al.* (2016), Sangeetha and Suchitra (2018) and Tooba and Tauseef (2019), were taken into consideration and reviewed accordingly, their framework gave a good background to this study; they implemented network security protocols in e-commerce applications but did not offer solution to the fair exchange and trust of security in e-commerce, SSL Protocol was used to ensure secure system; the SSL used has become vulnerable and it does not support a good security in client-server communication and encryption of messages to protect the confidentiality of exchanged information.

The introduction of security constraints has become a goal for many of today's systems. This study addresses the threat facing e-commerce by proposing a secure online communication framework, where remote parties, authenticate system has been developed to access the e-commerce system and to verify the functionality of the system works as expected behavior that is already specified. The online business usually occurred between consumers and sellers. This type of business activities includes the demands for quotation of prices, personal detail, payment, delivery of products, and the acceptance of services after the arrival of the product to consumers. The levels of confidence required from the system among others are confidentiality, authenticity and delivery of goods and services involved in the transactions. In respect with the initiatives established by e-commerce application to strengthen a web user identity, a proposed framework is designed as it is shown in Figure 1

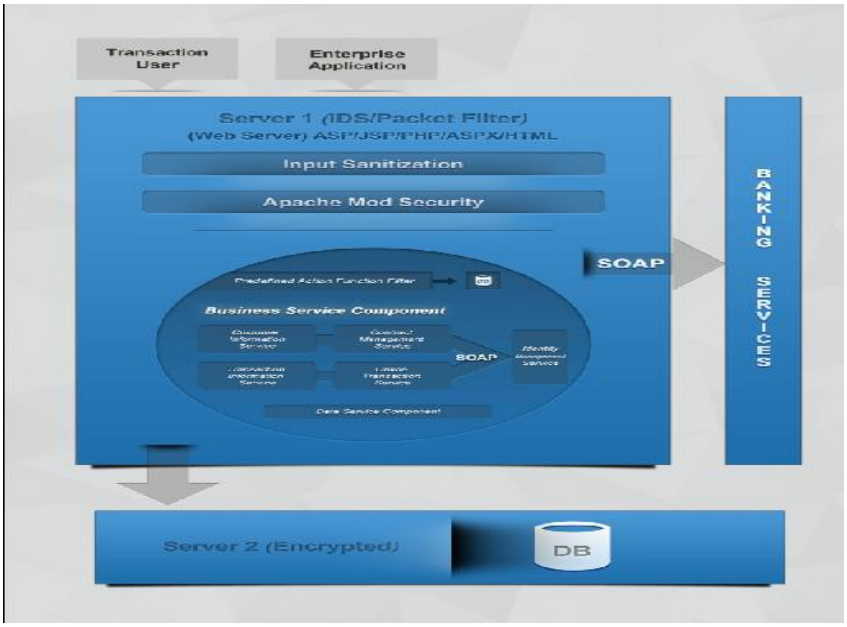

Figure 1. SOA Security Framework for E-commerce System (Source: Ashish *et al*., 2014)

Figure1 shows (Ashish *et al.,* 2014) framework system, they developed a framework with an authorization, authentication, verification and Session for Secure login mechanism using Service Oriented Architecture (SOA) to provide security for e-commerce. The architecture is designed with transaction as the user and enterprises as the application. The web server is ensured to preserve two tier securities; authentication and validation which could be submitted by the user and cannot be duplicated or forged. The security level was able to achieve through; sanitization of input, plug- in based on Rule and Intrusion detection system to provide security to online business. The database is kept in server that serves as the host; the database is encrypted with identical key. In order for customer to be sure of their transaction is secured the system was able to provide authentication, Integrity, and confidentiality. Hence, their framework was able to preserve message to some extend but fail to address non repudiation, key recovery policy and padding attack.

Sibo *et al.* (2016) implemented security framework as it is shown In figure 2, the framework depicted how first users are mandated to register their User ID and input their password for login into the system as part of security measured provided by (Sibo *et al*., 2016). The major security implemented in their research work, used a remote invocation technology over SSL, which provides a method to authenticate the provider that sells a particular resource as it is illustrated in figure 2 Before the e-purchase takes place, the requester (client) checks the validity (the expiration date). The security was able to establish between the buyers to the product received to customer over secure socket layer.

The research works gave a good background for this study but did not offer solution to the fair exchange and trust of security in e-commerce, the SSL protocol used has become vulnerable and it does not support non-repudiation, services are established by various enterprises, controlled or preserved by different section within the capability, that produce online ordering system a service aligned with diversified system; This would give rise to different types of security problems and element of security danger which are: service denial, network failure, duplication of certificate and , restricted time requirement attacks.

Their paper explained the threat against e-commerce and suggests a secure system that used secure oriented architecture. The proposed secured framework presents e-commerce system that demonstrates issues and threats involved in ecommerce. The framework is firstly designed on unsecured e-commerce system and shows that the necessary features. The system implemented the secure features of SOAP with total way of amalgamated security

which protects the ecommerce platform. The system provide security solution to the threat raised, the system also provide authentication and remote access, which assured the authenticity of users and log out uncertified users. The implemented IP multimedia subsystem is meant for identification of customers involved in the transaction. The system proposed three security access namely; Input sanitization, Rule based protection and action filter. With the system, the issues of certificate duplication is solved, the layer is provided for preventing threat and protect the available database implemented in the system, indirect access to application and prevention against denial of services threat.

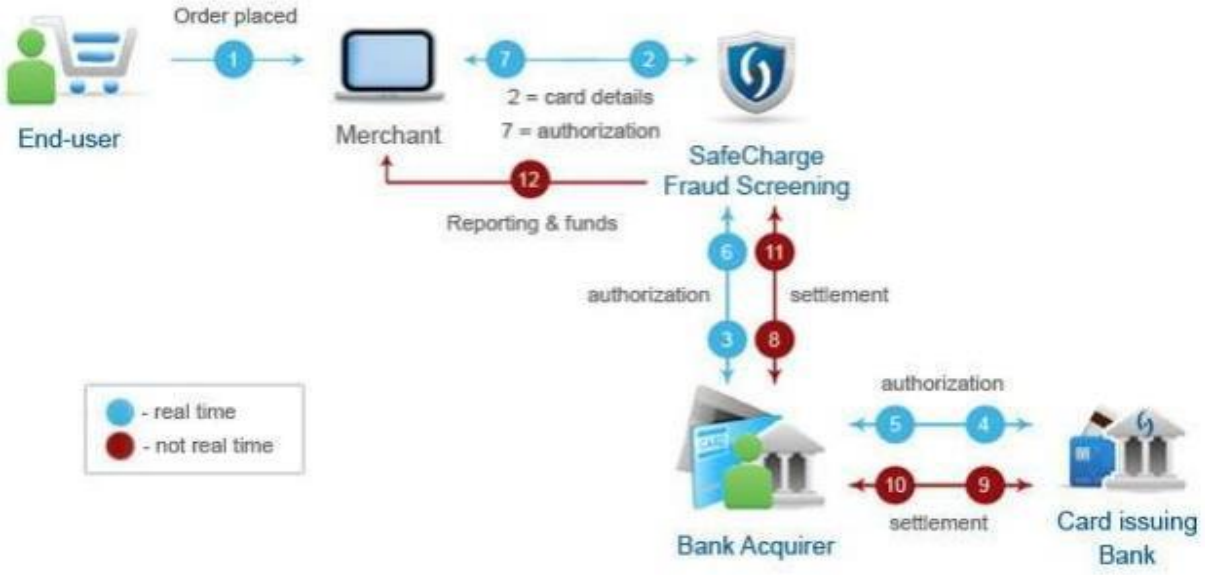

Figure 2. Steps for ordering and Digital Payment in E-Commerce (Source: Sibo *et al*., 2016)

Sangeetha and Suchitra (2018). Worked on, the Study of E-Commerce Security Issues and Solutions. In their research they came out with idea of how to protect e-commerce from unauthorized users and ensured some of security service required; Alteration, Integrity, data modification among others. They identified the activities of fraudsters in online shopping that is not secure and how mistakes from users could lead to users vulnerable. In their work they provided five security threats that affect ecommerce and also proffers solutions; Confidentiality of personal detail, Identification and Authentication, problems with access control, Integrity of data and non-repudiation of data. The study address the problem facing ecommerce to some extent and also proffer solution on how to tackle some of the problems, the paper did not come out with good and well-structured framework.

Tooba and Tauseef (2019). Presented Designing of secure framework for ecommerce using Simple Object Access Protocol (SOAP). The authors designed a well-structured architecture illustrating the flow of transaction from the users been connected to the web server and with the aid of SOAP the channel connected with access protocol to the main ecommerce environment and used database at the backend, while the enterprises follow same channel. With the aid of SOAP, the framework provided a secure ecommerce platform for good transaction. The framework is designed as it is illustrated in figure 3. The research work gave a good background for this study but did not offer solution to the fair exchange and trust of security in e-commerce, websites survey, attacks due to truncation. The SOAP protocol used has become vulnerable and it does not support non-repudiation and The system could be termed heterogeneous because the service provided are originated by vendors, the service are stored, managed, by different section, the heterogeneous would confront several categories security threat such as denial of services, duplicity of detail and restricted time of information channel, key recovery policy and padding attack and feedback mechanism not implemented.

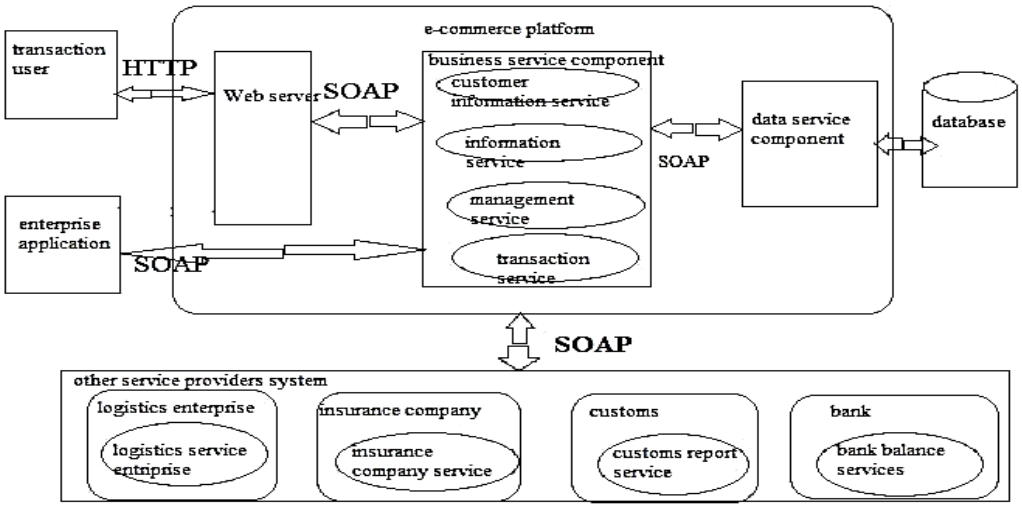

Figure 3. Designing of secure framework for ecommerce using SOAP (Source: Tooba and Tauseef, 2019)

3. Design Process of proposed e-commerce

ASP.NET has good features that enable the users to apply; the large pool of database functionality, speedy online application, recovery from loss of storage capability and loss of secure environment. The objective is to design online products storage framework. Anytime the consumer login to the system; each product has address location in the browser area. Web server is called to fetch the sought information. Internet Information Service (IIS) is positioned as web server in Dot NET framework environment. The major function of a web server is to receive entering HTTP request and supply the sought resources in an HTTP feedback. Whenever a request is being established IIS would determine firstly how to tackle the request.

The requested file is accepted by ASP.NET and request from database through ADO.NET for the needed file and the information is returned to user's browsers. IIS confirms if entering request is actually entering through IP address which is permitted to gain entrance to the domain. Otherwise, the request not granted.IIS has its own feature that responsible for user authentication, if it is instructed. Upon a request in IIS web server the extension is checked depending on the required extension, IIS would now tackled the request directly or diverted to ISAPI extension. The ISAPI extension is an installed extension which is a compiled in a manner of class in web server and is major work is to deliver the markup language for the requested document category. The features of this document comprises of images of the product, CSS file, JavaScript etc these are used in designing SOOS Project in the study. Whenever a request is being established through that has dot.html extension, the main contents of the requested HTML file would be returned by IIS.

3.1 MySQL Database

In this SOOS project, MySQL is used as the backend database. MySQL is an open source database management system. MySQL database is connected to ASP.NET using an ODBC driver. Open Database Connectivity (ODBC). The ODBC driver is a library that implements the functions supported by ODBC API. It processes ODBC function calls, submits SQL requests to MySQL server, and returns results back to the application. In this SOOS Research, the database management system is designed using MYSQL. ODBC driver is used as a connector between the database and ASP.NET. The Open Database Connectivity (ODBC) uses its driver and library to implement function with the aid of ODB. It therefore perform operation on ODBC function calls, delivers SQL requests to the server that holds MySQL , and deliver the output to the application.

3.1.1 Database Connectivity

It is necessary for web server to seek the database in order to acquire necessary information from database when necessary or anytime is being requested. In this study, database connectivity in an online ordering system is established by ASP.NET using its feature termed Data Objects.NET which can also be called ADO.NET to link to the database for fetching any requested information**.**

3.2 The Description of SOOS Framework in E-commerce

This section shall give a pictorial presentation of the architecture of the intended system. The entire architecture can be decomposed into three major components. The component is illustrated as shown in Figure 4. These components are;

(a) Client Layer User: User information encoded in the database and the system application. The computer system that falls into this layer is called Client computer, it works on software application which can be regarded as a client program, it allows the customer to make a request for series of information from the server, by first login to the system.

(b) Security Layer: The security implemented in this study involves encryption process, which is achieved by Secured Electronic Transaction (SET) protocol. In this, Advanced Encryption Standard (AES) protocol was used for encryption process and Message Digest (MD5) hash function are used for Password Based Encryption (PBE) for detecting data corruption and tampering and integrity of data message exchange between clients.

(c) Server Layer: Comprises of the various tools, datasets, Java scripts, Web server, MSQL DB server and other relevant smaller components that makes it functional, ActiveX Data Objects .NET (ADO.NET) and ASP.NET.

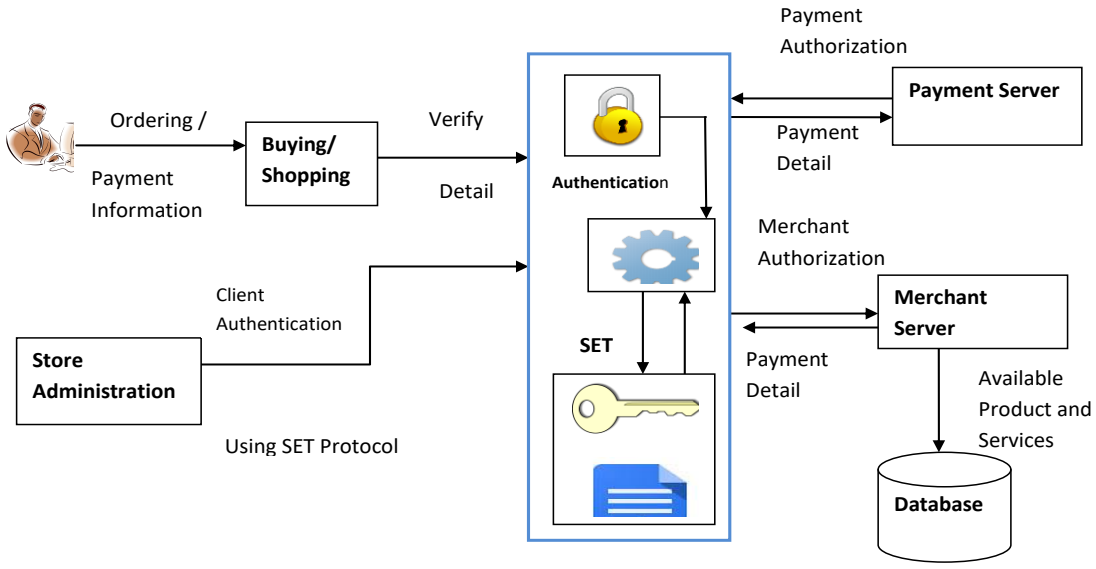

Figure 4. Secure Online Ordering System (SOOS) framework

Figure 4, depicted a Secure Online Ordering System framework in e-commerce which provides robust and conducive application for consumers to place an order on many types of products. The application is categories to

User side also known as front –end and Management side known as back-end. It has modules that consist of Registration, Search items and placing of order.

Front –end consist of the following modules: User Login and User Registration/ Logout User Center (My: Information, favorite and comment) Search Engine (key word to Search, use of Category and More search). The cart order query notice and messages as reminders to the email. The messages are classified as view, delete, add, update, add items to favorites also View History. Back–end consists of: Product management category; which include Product, update, add, delete and check order manifest, product delivery status.

3.2.1 Encryption process and client-server communication in SOOS

The proposed SOOS framework; will provide secure communication over a distributed environment by achieving; authentication, integrity, confidentiality, authorization and non- repudiation. The security implemented in this study involves encryption process, which is achieved by the combination of SET protocol, in this protocol AES was used for encryption process and MD5 hash function are used for PBE for detecting data corruption and tampering and integrity of data message exchange between clients.

The multi-agent system used combined the concept of technology and a secure authentication procedure to facilitate information exchange between agents, while the optimized access to the method used, the messages sent across the client to server would be encoded, also the encoded messages is signed to form digital signature. For security reasons authentication between communicating server can be proven using cryptography, the SET protocol helps the client to authenticate its personal detail to server (vice versa) through an open network, after connecting client/server to a SET protocol to verify their personal detail, also assured the encryption of all the communication channel to enable data integrity and protection of data. The communication between Client and server is illustrated in figure 4.1.

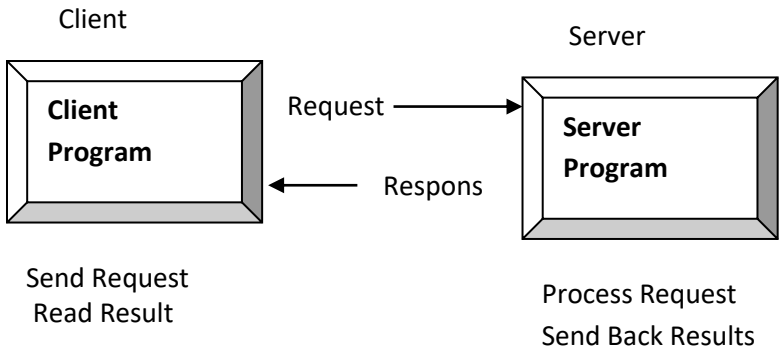

Figure 4.1. Client/Server Communication in SOOS Framework

Figure 4.1, shows the client/server communication model which allows the customer to fetch information in an easy way; the relationship is built on several ordering and getting responses from the system. The model is based on ordering by client for information about a particular product from the server and respond from is established to the client.

3.2.2 SET protocol and SOOS Framework

In this study, an improved SET protocol has been designed to form a layer in the framework by combining with other advanced encryption process while increasing the complexity of its method over unsecured channel It gives rise to more secure e-commerce application as shown in figure 4.2. The digital signature obtained from SET protocol which uses AES and MD5 in an encryption process which act as security layer as it is illustrated in figure 4.2. the layer forms better security framework measure put in place to secure the channel communication in e-

commerce, to ensure the security service required confidentiality, Authentication, Integrity, Certificate Duplicity, Failure of point, Restricted time requirement, Service attacks denial and Non-Repudiation.

Figure 4.2, shows a sub component layer in figure 4 where an improved SET protocol is implemented in a client /server framework, it enables the user-server authentication rather than host-to-host authentication. An improved SET protocol is a protocol that provides encryption, decryption and security specification designed to protect the users and merchant in their transaction in the SOOS framework. The encryption process is meant for the protection of card digit, CVV number, tracing data PIN , expiry date and some other personal data upon subjected on the system during the time of transaction etc . The approach used includes secret key technology where each of the host is expected to have its personal key. An improved SET protocol sign and prove clients personal data to server. AES and MD5 hash function used in the SET protocol are used for PBE for monitoring data corruption and altering and integrity of data messages trading between client and the system, the message is encrypted through the interconnected channel in between client and server before passing it on to the processor, the data remains intact till it reaches processor for onward processing to ensure the security that exist in communications process in between all users involved in SOOS framework designed.

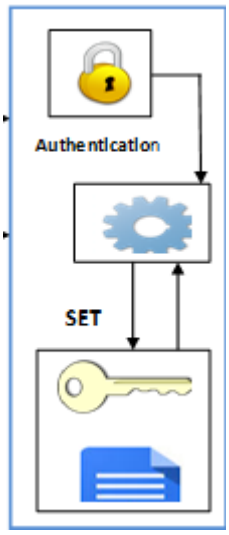

Figure 4.2. An Improved SET Protocol Layer in SOOS Framework

4. Results and Discussion

4.1 Shopping Cart Process and Checkout Process

An ideal cart is designed majorly for a place where each product is kept for selection of preferred products and places an order using credit card. After successful opening the SOOS project, the customer login; username and password are entered through Password Based Encryption (PBE) process, in this study, the customer order green shirt from the items available with specific price attached to it, as it is shown in figure 5. The product ordering page has peculiar features; the items made available, the calculator for displaying total items bought, price of items bought, payment method and delivery method; the delivery method show how the shirt is being conveyed as regard to the shipping method is selected at the moment of ordering the product as it is illustrated in figure 5. The login detail and all the transaction occurred in the system are subjected through the PBE in an improved SET protocol as explain in section 2.4.1.

Figure 5. Product Ordering Page

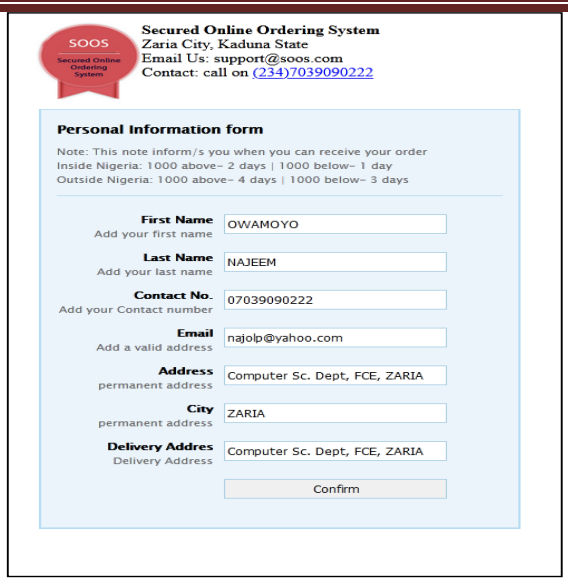

Figure 6. Personal Information and Payment Detail Form

The cart product designed in this research easy to understand and has database to house the various resources on the product cart. The logging has session for user displaying the resources available based on the authorization set up. In this study, to protect between ordering of product, a cookie and session is established which permit verification of the items that are meant for a particular users. 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 or Shipping to Nigeria or Shipping out of Nigeria. After successful ordering and Payment, users could now proceed to checkout process; where it would be requested to fill their personal details; such as Customer- Name, Telephone, Address, Electronic-Mail and Delivery area as shown in Figure 6 and Figure 6.1 respectively.

ASP.NET using cookie-based session state allocates storage for session items also allow registration until the session object is used. As a result, a new session ID is generated for each product request Till session transport is established, this occur at the time the application request a stagnant session ID for the whole session start_procedure is also established in the system's Global.sax document and save the item in session transport to initiate the ID. This code is also added to the file Global.asax which add each entry to the session object. The session ID stores variables and the resources of the identifiers are kept in server**.** Content of the session ID display its content as information at the client-side.

4.1.1 Feedback Mechanism in Checkout Process

Another implementation in this study is feedback mechanism that has been implemented. The client side and server side are displayed in Figures 8 and 8.1, respectively. The user enter the necessary information; which include Name, E-mail-address, Subject and the actual information in the command buttons as shown in Figure 8, after pressing the lunch button, it displays all the transaction and the comments made by the user in Administrative dashboard. As shown in Figure 8.1. This encryption procedure would improve the function of cryptographic. The protocol used would provide the authentication data integrity and data confidentiality. The AES provides confidentiality; the MD5 provides the integrity and SET protocol ensure the authentication, verification and signing by the Digital Signature (DS) as a result produced after the encryption process as shown in Figure 7. The digital signature obtained, the message and the private key is encrypted with symmetric key encryption method of AES, the output is formed as special code. The result obtained can now be sent to the receiver; on getting to the receiver end, it could now be decrypted by own secret key.

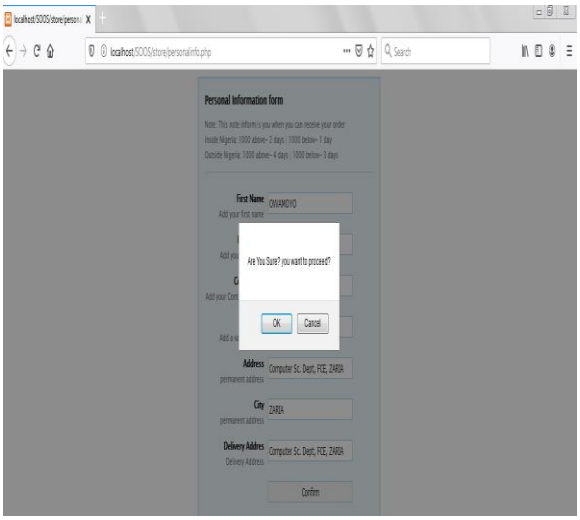

Figure 6.1. Personal Information, Payment Detail and Checkout form

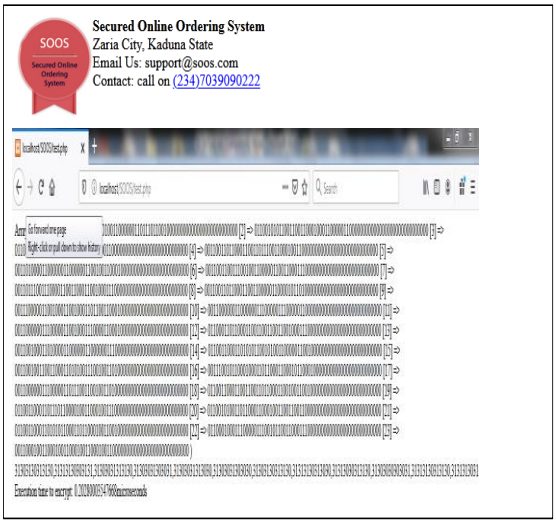

Figure 7. Digital Signature

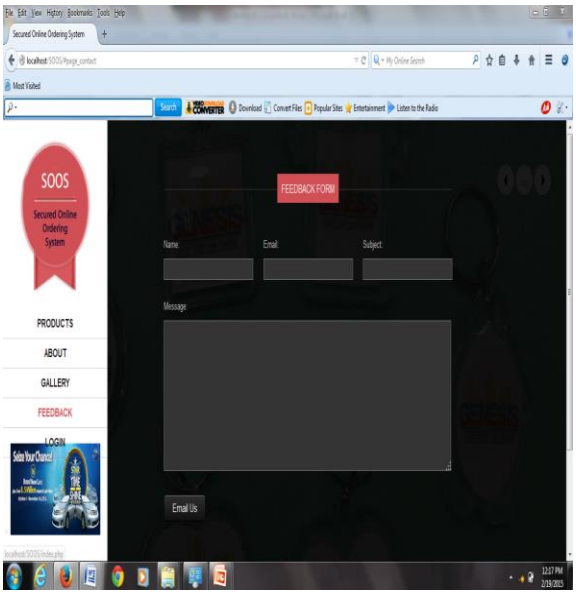

Figure 8. User Feedback Form

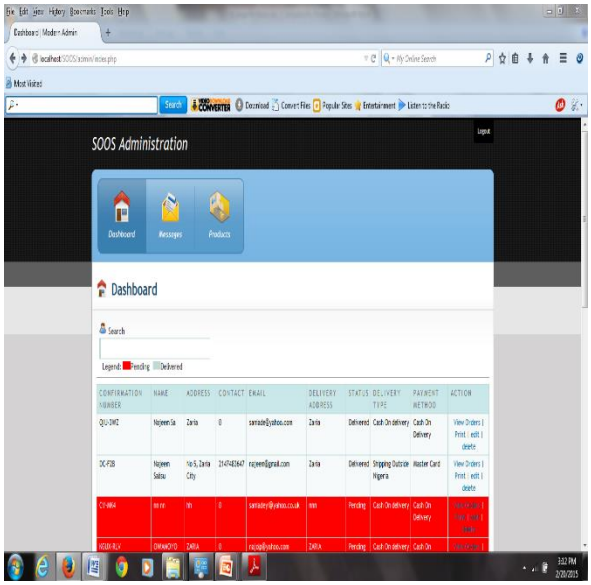

Figure 8.1. User Feedback Form and SOOS Administrative Dashboard

Checkout process has variety of product in the cart and the customer information with the help of session identification. The other page of the checkout act as the card information form which is proved by JavaScript, the data is encoded on entering the data and channel to the other page in the checkbox order and decrypted, which could later be forwarded to bank for onward processing. On this page, two buttons are situated; there is proceed button together with checkout process, the other one cancels and exit the transaction.

5. Conclusion

The research work is concerned with the development of secure framework for carry out online buying and selling. It has been demonstrated in this study that the proposed security measure are more expressive and intuitive than that of existing ones. On the same note, it was observed that ensuring security service is very crucial for e-commerce developers; an improved SET protocol was used for securing transaction by using encryption process techniques. The encryption techniques used in this study have increased the effectiveness of protocol in cryptographic function. The protocol used in the framework assured confidentiality, authentication, integrity, fair exchange, non-repudiation while ensuring the free flow of transaction, high level security services for d e-commerce transaction and feedback mechanism was intr. Lastly, a Secured Online Ordering System (SOOS) was developed to demonstrate the use of secured web application, the evaluated results obtained showed that improvement on the required security service and better relationship between the parties involved in the transaction have been established in the framework.

6. Recommendations

Necessary attention should be accorded for developing a suitable product cart that is flexible and embedded with logic. A robust system that provide convenient environment for the users to navigates through available product in the cart where items could be a add or remove. Country stakeholders should rise up and formulate necessary policy that will allow the development and deployment of secure of e-commerce related technology and policies that would regulate the use of e-commerce for sustainable development. The government or relevant agency should carry out a public awareness to people as regard to how e-commerce can be used effectively, benefits of e-commerce to the society and how it will eventually minimize their expenses compare to another means of buying and selling of products

Reference

Akinyede, R. O. (2018). Proposed E-Commerce Framework Using Cloud Computing Technology". *International Journal of Computer Science Trends and Technology (IJCST),* 6(3), pp. 48-51

Ashish, K. L., Sanjay, K. D.,and Jha, C. K. (2014). Designing a logical security framework For e-commerce system based on SOA. *International journal on soft computing (IJSC)* 5(2):6-8.

Hanson, W. and Kalyanam, K.(2006). Internet Marketing and e-Commerce. Retrieved July 20, 2019 from:https://lib.ugentbe/catolog/rugo1:00089/papers/P11.pdf 2-10.

Muneer, A., Razzaq, S. and Farooq, Z. (2018). Data Privacy Issues and Possible Solutions in E-commerce. *Journal of Accounting & Marketing, Department of CS & IT, University of Sargodha Sub-Campus Mianwali, Pakistan*. Pp 2-4.

Qiaofen, J. (2018).Study on Information Security Issues of E-Commerce. IOP Conference Series: Materials Science and Engineering Qiaofen Ji 2018 IOP Conf. Ser.: Mater. Sci. Eng. 452 032050

Sangeetha, M. K. and Suchitra R. (2018). The Study of E-Commerce Security Issues and Solutions. *International Journal Of Engineering Research & Technology (IJERT). 4(27) pp 4-7*

Sibo, P. P., Neelamadhab, P. and Rasmita, P. (2016). International Journal of Advanced Research in Computer and Communication Engineering IJARCCE ISO 3297:2007. Certified 5(12):82-84

Tamara, A. and Yousef, Kh. (2018). Cloud Computing of E-commerce. Modern Applied Science; Published by Canadian Center of Science and Education 13(1), pp.

Tooba, A. and Tauseef, R. (2019). Secure Architecture for E-commerce Websites. *Sir Syed University Research Journal Of Engineering And Technology*, 9 (1,) , pp 13-15.

Kuruwitaarachchi, N., Abeygunawardena, P.K.W, Rupasingha L., and Udara, S.W.I (2019). A Systematic Review of Security in Electronic CommerceThreats and Frameworks. *Global Journal of Computer Science and Technology: E Network, Web & Security 19(1), pp.3-6*