International Journal of Cyber-Security and Digital Forensics (IJCSDF) 6(2): 92-100
The Society of Digital Information and Wireless Communications (SDIWC), 2017 ISSN: 2305-0012

A Novel Framework for Secure E-Commerce Transactions

[1]Kenneth L. Mlelwa* and [1]Eng. Dr. Zaipuna O. Yonah+
[1]School of Computation and Communication Science and Engineering,
Nelson Mandela African Institution of Science & Technology
P.O. Box 447, Arusha, TANZANIA.
mlelwak@nm-aist.ac.tz*, zaipuna.yonah@nm-aist.ac.tz+

ABSTRACT

E-commerce is now a trend and a must in many business sectors. In line with this eCommerce trend, many businesses use the internet to transact their business and to share information among trading partners. It is for this reason a proper and clear security has to be defined to guarantee secure eCommerce transactions. This paper proposes a novel framework that integrates secure technical, Business/organization, Operation security parameters, policy, customers and merchants as stakeholders in business for proper and secure information exchange. The framework points out the relationship among different parameters. With this framework, secure eCommerce transactions can be achieved.

KEYWORDS

Pretty Good Privacy (PGP), Secure Electronic Transaction (SET), Security Protocols, Secure Socket Layer (SSL), trusted third party.

1. INTRODUCTION

Security and privacy are two key concerns to be addressed when deploying information and communication technologies (ICT). Coincidentally eCommerce shares security concerns with other technologies in information security frameworks. Fortunately, privacy concerns have been found, revealing a lack of trust in a variety of frameworks, including those for electronic health records, social networking and e-recruitment technologies; and this has directly influenced users [1].

An information security framework is a synchronized system of behaviors and tools for monitoring transactions and data that are extended to where data utilization occurs, thereby providing end-to-end security [2].
Ecommerce Security framework is a subset of the Information Security framework and is particularly applied to the components that influence eCommerce that include Data Security, Computer security and communication channel of the Information Security framework. Security in eCommerce has its own particular nuances and is one of the maximum visible security components that influence the end user during their daily transactions and interactions with businesses that are conducted on the global network (Internet), which is un-trusted.

Thus, confidentiality is needed throughout the transmission of transaction information and the information should be kept protected (Secure) against all kind of threats. Linked concepts and business practices symbolize opportunities for opening new domestic and international business enterprises. On the contrary, as Cyber space is used more and more as a platform for eCommerce transactions, security turns out to be a crucial issue for Internet applications. Security has become as an increasingly significant issue in the growth of any eCommerce organization. The purge of trust in eCommerce applications may result into sensible business clients and operators to give up the use of the Internet for now and slip back to traditional ways of doing business. Increasing access to sensitive information and replay are some familiar threats that hackers impose to eCommerce platforms [3]. Security protections embody with the safeguarding of availability, confidentiality and integrity of data [4]. These three canons of information security are occasionally symbolized in the Authentication, Integrity and Confidentiality Triad as in Figure 1.

Figure 1. The Authentication, Confidentiality and Integrity Trio.

The Security community has documented the common security concerns as Access Control, Privacy/Confidentiality, Authentication, Non Repudiation, Integrity and Availability.

This paper proposes a novel framework that integrates several parameters including customers and merchants as stakeholders in business to guarantee secure eCommerce transactions. The paper is organized as follows: the next section is a related work regarding the eCommerce study in secure transaction is discussed followed by problem statements, which explore common technologies for secure eCommerce transactions with their pitfalls. In Section 4, the new proposed novel framework is introduced and discussed. In section 5, the developed secure plug-in for implementation of the proposed framework is presented. In section 6, showing how the developed security plug-in can be used as a protection against security threats, and its results in section 7 and finally is a Conclusion

2. RELATED WORKS

Almost all security frameworks have cons and pros. There is no one-best-fits- all frameworks that would work for every organization. Businesses and Organizations are simply too varied, ranging from large multi-national business with numerous databases to small private businesses that are largely self-contained. And the IT staffs within those firms vary widely when it comes to training and expertise.

The regulatory background has become more complex because organizations habitually find themselves required to comply with several regulations and industry mandates. As new threats emerge, standards and regulations persist to grow in number and complexity. Now-days, many laws have penalties for data violation including for not meeting timely notification of those who are affected. The most important factor of security frameworks is to defend vital systems and the processes that provide those operations.

Without a doubt, any online transaction requires clients to reveal a huge quantity of sensitive private information to the merchants, introducing themselves at significant risk. Understanding (indeed, even precisely defining) trust on the consumer side is now essential and necessary for the continuing development of eCommerce.

The main reason of Web security is to safeguard and meet the security expectations of users and providers. Therefore, generally security in web technology is concerned with: **client-side security**, **server-side security**, and **secure transmission of information** [5].

- *Server-side security* deals with the practices and techniques that protect the Web server software and hardware from break-ins, Web site vandalism and denial of service attacks.
- *Client-side security* deals with the practices and techniques that protect user's privacy and the integrity of the user's computing system.
- Secure transmission is concerned with the practices and techniques that will assure protection from eavesdropping and intentional message modification [5].

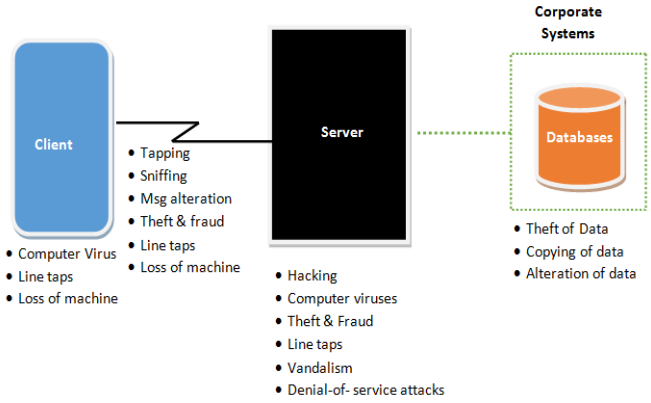

Figure 2. A model of security attacks on eCommerce Application.

Determining threats is a mountain to climb as well as time consuming but secure approach cannot be built without understanding the threats that may occur throughout the transaction communication. It is not easy to decide on a specific technology for tackling these threats. But, it is known that the threats that can break eCommerce security are clarified as follows:

- Man-in-the-middle attack
- Reply attack
- Repudiation threat
- Data Tampering attack and
- Information disclosure threat

Other researchers have been discussing security aspects in eCommerce, as a software solution aligned with Secure Electronic Transfer (SET) or Secure Socket Layer (SSL) technologies for encryption of data transmissions. SSL protocols allow transmission of encrypted data across the Internet by running above the traditional TCP/IP protocols [6].

Essentially, the SSL guards the communication between a server and client and provides authentication to both parties for the purpose of securing communication. It also provides a point-to-point security. It is for this reason that storage of sensitive data in repositories or databases makes eCommerce systems ideal targets [6]. Unfortunately hackers targets data repositories due to availability of data on a single place.

SSL permits many key exchange algorithms, however some other algorithms like Diffie-Hellman key exchange have no certificate concept [7], which is not compliant to eCommerce security.

3. PROBLEM STATEMENT

The most common security protocols used in eCommerce secure framework are Pretty Good Privacy (PGP), Secure Socket Layer (SSL) and Secure Electronic Transaction (SET). Buth these Common securities protocols deployed for the purpose of achieving eCommerce objectives have own pitfalls.

PGP has been considered to provide security to eCommerce [7]. It is a software that combines several high-qualities, protocols and existing public-key encryption algorithms into one package for protection, file transfer and reliable electronic mail. PGP not only provides encryption of data, but also data compression, digital signatures and smooth compatibility with email systems.

PGP is pretty well-liked now, especially in the e-mail system, but it is not full proof solution for eCommerce because it provides Confidentiality and Authentication only which are pretty good enough for email security and not for eCommerce security. Pretty Good Privacy **cannot** deal with Reply and Man-in-the-Middle attacks in eCommerce transactions.

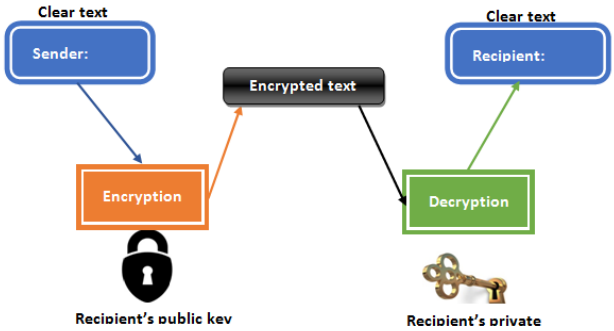

Figure 3. PGP Based E-commerce Cryptography [8].

In order to have a strong security framework, some security parameters must be kept in mind. Normally the main security objectives are Authentication, Confidentiality and Integrity. However, for internet and web related applications, major security objectives include non-repudiation, man-in-the-middle and reply attack. That's why this study aimed to propose an eCommerce security framework capable of guiding to achieve major security objectives against common threats known as pinpointed in the Figure 4.

Figure 4. Comparison of Security Objectives vs eCommerce protocols.

4. PROPOSED FRAME WORK

The proposed framework integrates different security parameters, policy and general business ingredients thus making it a Novel security Framework eCommerce Transactions. To achieve this, security requirements analysis was conducted and the results were used in proposing the framework. The framework is intended to facilitate and enhance security in eCommerce by providing a clear way of interactions, security measures and general awareness.
The proposed framework is divided into three sub frameworks namely; Secure Technical

framework, Business/Organization framework and Operation Model [9].

4.1 Secure Technical Parameters

This sub framework is considered as the technical part of the main framework, which consists of the following components [9]:

- **Customer/Merchant**; these are the main actors throughout an entire eCommerce transaction; these actors will be initiating all activities inside this sub framework.
- **Security Objectives/Goals**; this paper, this security objective consists of Authentication, Non-Repudiation, Integrity as well as Reply and Man-in-the-Middle Attack handling components.
- **Third Party Trustee;** this includes parameters that permit parties to communicate securely over public networks with the use of public key cryptography.
- **Service Oriented Architecture (SOA);** In an eCommerce transaction, interactions are typically machine-to-machine exchange. The main reason of a SOA in these Parameters is to achieve the availability security objective/goal, when deployed with web services. Simply because web services are technically unbiased. As a result, a web service produced by any business can be utilized by another business organization regardless of differences in technical platforms in the two businesses.
- **Attribute-based access control;** it defines an access control paradigm whereby access rights are granted to users through the use of policies that combine attributes together.
- **E-commerce Ontologies**; this required because eCommerce allows the definition of attributes that are implemented in access control and authorization decisions. In an eCommerce transaction, where there may be no human involvement, an incorrect authorization may be made since an assertion originates from the requesting machine, which may be interpreted in other way round from the consumer's policies. By using a familiar ontology, semantic interoperability is achieved.

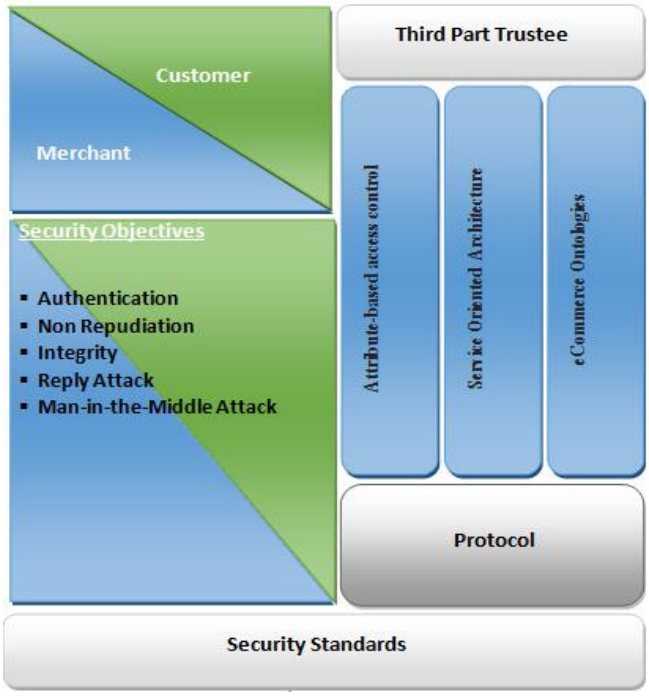

Figure 5. Secure Technical Parameters.

4.2 Business Parameters

The Business or Organization Parameters sub-framework sum-ups policy level mechanisms for tackling the information security requirements for eCommerce transactions. Its parameters consist of Business/Organizational plan, Regional and National laws and regulations, Contract/MoU as well as a Policy. This normally is implemented by top level management in an organization.

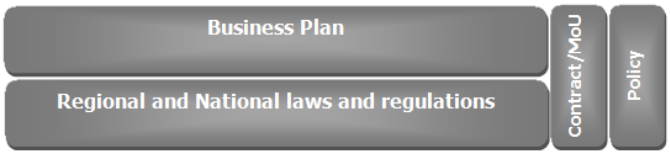

Figure 6. Secure Business Parameters.

Since an eCommerce transaction normally takes place across more than one business organizations then the framework should take into consideration the existing legislation and at the same time be flexible enough to accommodate new laws/changes to existing legislation.

4.2 Operation Parameters

The Operation Parameters sub-framework summarizes organizational plans and practices that an individual business organization can use to satisfy the information security requirements. Its parameters include organizational programs and plans, common terminology for eCommerce

transactions and certificate authority agreements. This model is implemented by operational departments in individual organizations and some components are implemented across businesses.

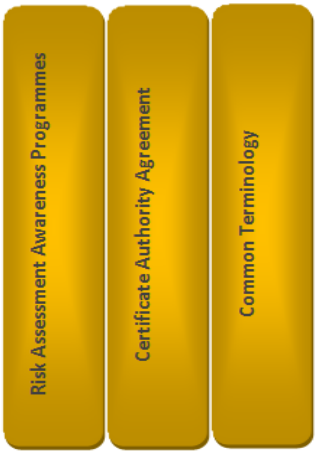

Figure 7. Secure Business Parameters.

4.4 The Novel Framework

The relationship between the proposed security factors is also indicated in Figure 8. The purpose of the proposed novel framework is to enhance security in eCommerce by including several security factors resulting from prior security requirements analysis [9].

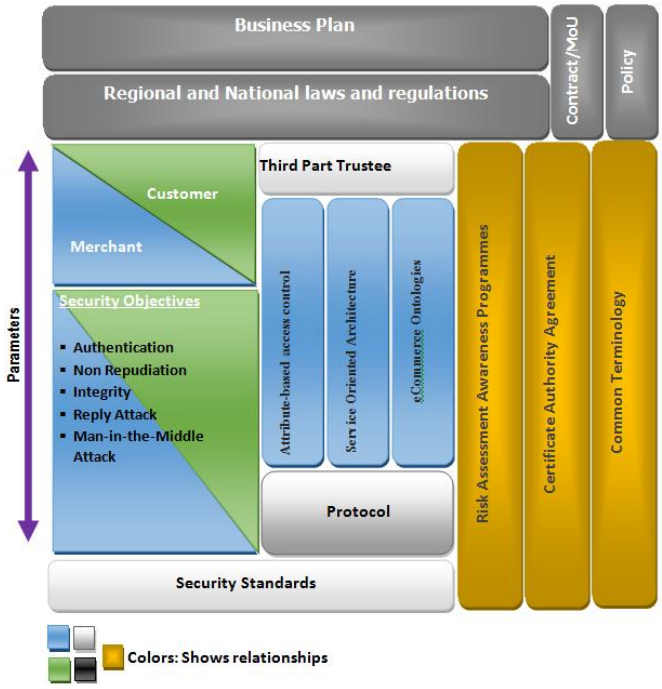

Figure 8. Proposed Collaboration novel framework for secure eCommerce Transactions

All these three sub-frameworks cannot work independently, they need to coordinate between one entity and another as in Operational sub-framework certificate Authority Agreement, which is supposed to be working simultaneously based on the Contract/MoU parameter found at the level of business sub-framework; where by this collaboration should be done without violating the regional or/and national laws and regulations. Therefore, for this framework to work perfectly all these sub-frameworks need to be aligned and working in a collaborative way to achieve all five objectives as in Figure 9.

Figure 9. Comparison of; Security Objectives vs eCommerce protocols for the new proposed unified protocol.

5. IMPLEMENTATION

Based on proposed Novel framework (Figure 8), a security plug-in was developed aiming to achieve secure eCommerce transactions. The developed plug-in consists of three entities, namely; customer, merchant and third party trustee (Tk).

Prior to commencing an eCommerce transaction, merchant and customer parts must be registered by the Third Part trustee (TPT); which will provide tokens for transaction to all customers and Merchants parts involved with sending data. Thus, when each customer and Merchant gets their transactions tokens then both parties start to communicate. And this proposed framework will offer protection against security attacks.

Table 1: Customer, merchant conversation steps

Steps	Customer actions	Third part trustee actions	Merchant actions
(1)	Customer requests token from Tk (third part trustee) EKU (Tk) [IDC, ReqC, Time, KUC, NC]	Tk sends a token to customer TC=EKR (TTP) [IDC, ReqC, Time, KUC, NC]	When merchant receives customer token, then merchant would have to request for an issuance of token to TTP. EKU (Tk) [IDM, Time, KUM, NM]
(2)	Customer sends token to merchant TC→M	Tk provides a token to merchant and encrypts it. TM=EKR (TTP) [IDM, Time, KUM, NM]	Merchant sends token to customer TM →C
(3)	Customer sends information to merchant Eku (M) [NC, EKR (C) [IDC, Time, NC]]		Merchant sends information to customer Eku (C) [NM, EKR (M) [IDM, Time, NM]]
(4)	Customer acknowledgement passed to merchant		Merchant acknowledgement passed to customer

Table 2: Notations for Customer and merchant conversation steps.

Notation	Description
Tk	Third Part trustee
TC	Token Issued to Customer
TM	Token Issued to Merchant
NC	Nonce generated by Client
NM	Nonce generated by Merchant
Time	Time Stamp
IDC, IDM	Identity of Client and Merchant
EKR (C), EKR (M)	Private encryption using private keys of Client and Merchant
EKU (C), EKU (M)	Public encryption using public keys of Client and Merchant

Using the tabulated steps (Table 1) results into transactions such that a merchant and a customer share a bunch of information for the purpose of recognizing each other and solve future disputes (if any) in regards to an eCommerce transaction.

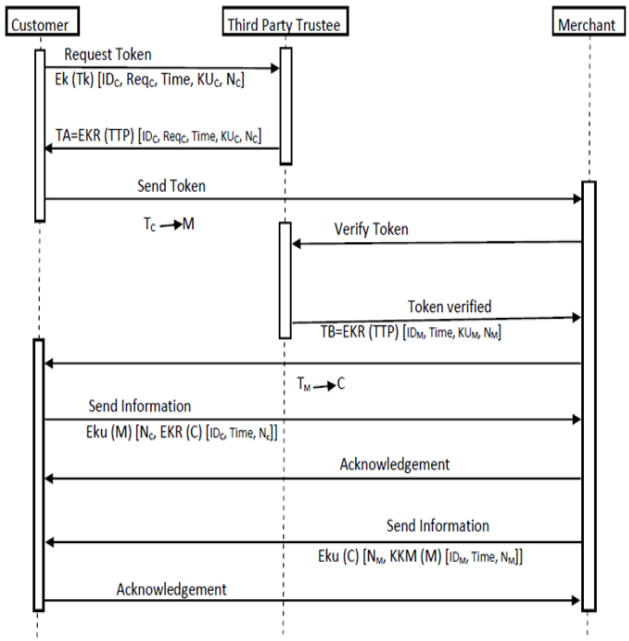

Figure 10. Customer, merchant conversation Sequence Diagram.

6. PROTECTION AGAINST SECURITY THREATS

The proposed eCommerce security framework is designed with the capacity to overcome all major security objectives as described in Table 3, as follows;

6.1 Authentication

In this scenario; Customer sends ID, nonce and time that is signed by customer using private key and then encrypts the whole package by public key of Merchant (step 3). Merchant decrypts the package with its private key. After decrypting the

Customer Package, the merchant will access the customer ID; as the package is signed by private key of customer. So in this way Merchant can determine that customer is Authentic.

6.2 Reply Attack

In case of key exchange, a reply attack can take place, which is easily solved in the proposed solution.

For example; a reply attack can take place in step 1. The un-trusted party can grab the token requested by the user and there after reply to the TPT for getting a fake token. But since the requested token contains ID, time and nonce; the TPT can use this information to easily recognize it as a replay attack, and the request produced by unauthorized party will be discarded.

6.3 Integrity

In order to solve the integrity issue; on the customer part the hash code is produced using SHA-1, of which is encrypted with the customer's private key. The encrypted hash code is combined with the original transaction message and then sent to the merchant. Then the merchant part splits the hash code from the message, and decrypts it with the customer's public key. At the same-time, the merchant will have to analyze the hash code of the received transaction message using the same SHA-1 algorithm. Transaction message will be received correctly if the analyzed hash code and decrypted hash code will be the same.

6.4 Non-repudiation

Both customer and Merchant get their tokens from TPT , which contains their IDs, Nature of request, time of issuance of token, their respective public keys and a nonce (produced by the customer and Merchant correspondingly). The third party trustee will keep a copy of the novel request for the token sent by the customer and merchant (see step 1 in Table 1 on customer and merchant columns) and a copy of the transaction tokens issued to them. As a result a Non-Repudiation problem can be solved using the third party trustee.

6.5 Man-in-the-Middle Attack

This kind of attack happens when three entities are involved (server, client and UNTRUSTED third part) during a transaction session. UNTRUSTED third part positions itself between the client and the server on the network and learns about the traffics that are coming from client to server and from server to client. Using this security plug-in developed based on the proposed security framework; Third Part Trustee (TPT) generates a token that comprises of ID, Public key, issuer name, Hash code, Nonce and token appended with the Third Part Trustee private key. The client checks the token novelty by examining the signature and name of the issuer.

7. RESULTS

A security plug-in[1] (algorithms) was developed purposely to secure an eCommerce transaction based on proposed novel framework.

The developed algorithm was implemented using the java programming language. The implementation procedure consists of transactional parameters. First; is the root entity (the Main parameter) and the others are customer and merchant parameters. The main parameter acts as an interface for the other two parameters. The parameters concerned in the transaction need an authentic token via a security plug-in to the main parameter. Meanwhile, the root entity offers genuine tokens to both transaction parameters through the developed plug-in. The parameters involved in the transaction, requests for authentic token via security mechanism plug-in. Again, the main entity provides an authentic token to all transaction entities through plug-in security module. Figure 10 depicts the implementation process in detail.

In order to secure an eCommerce transaction, plug-in generates tokens that are used by both the customer and merchant. Tokens have different parameters such as serial number, subject, hash code, issue name and public key. Customer and merchant first confirm the authenticity of tokens and then start to communicate in a secure domain shown in a couple of conversation's Diagrams here under.

[1] The developed plug-in is in GUI for the purposely of elaboration, plug-in normally are not in a graphic user interface

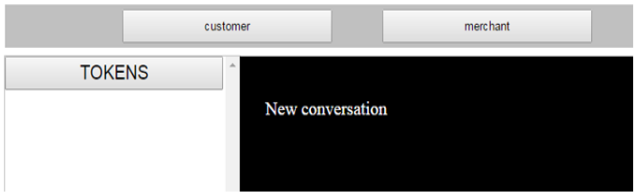

Figure 11. The case when customer and Merchant haven't started to communicate.

When the customer starts to converse with merchant, the customer requests a token from TPT. Then TPT sends a token to customer side; and the customer sends the message to merchant with a token received from TPT.

Before requested for a token | After requested for a token

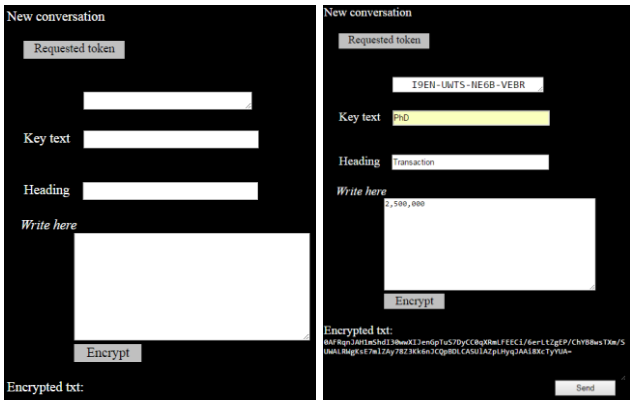

Figure 12. The case of Customer side before and after requesting for a token from TPT.

Figure 12, shows two sides of merchant side where by on the left hand side the customer has not yet requested for a new token; while on the right hand side the customer has been provided with a token, which was requested before, and hence used the token given to send an encrypted message to merchant side.

Figure 13. Merchant's side received a token from customer.

After the customer sends his encrypted message to merchant's side, the merchant will receive the token which was initially provided by Third Part trustee to customers (see Figure 13).

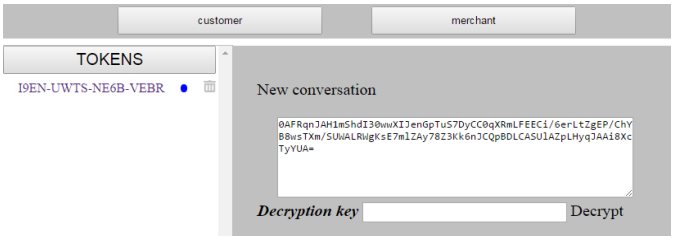

Figure 14. The case when a Merchant receives encrypted message from customer.

After the merchant receives a token from customer, he will decide to open it with the help of the decryption key that was used by the customer to encrypt the message. The decrypted message will show the time at which the message was sent; as shown in Figure 15.

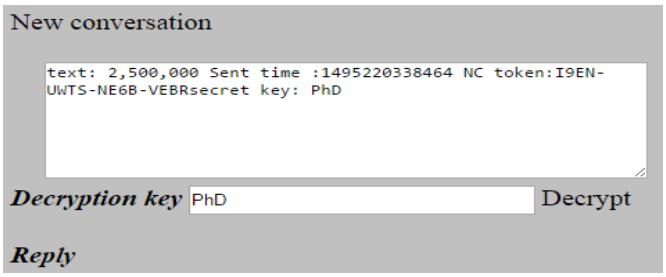

Figure 15. Merchant's side with the decrypted message.

Then once a message has been decrypted, the merchant will decide to acknowledge receipt of the message to customer, with the help of a third part trustee; again merchant will have to request a token from a third part to finish the conversation with customer side.

Before a merchant requests for a token | After a merchant requests for a token

Figure 16. Merchants side before and after requesting for a token from TPT.

The plug-in encodes the package to pass on over the communication channel and then decodes it at receiving side to achieve the original data. It also provides authentication and integrity verification to customer and merchant packages so as to protect against threats.

After exchange of tokens between customer and merchant, the application stores the tokens in XML data files to eradicate non-repudiation problem in the future.

8. CONCLUSION

Online business (eCommerce) in developing countries especially in Tanzania is still at infant level and in its formative stages of development; however with this speed of development over the past years, it is a clear signal of its enormous potential for conducting online business. These new opportunities, however, come accompanied with a large number of concerns and questions about security issues that need to be resolved.
As such, security remains to be a major concern for eCommerce. It is an impediment to expanding e-commerce services and business. Due to this, consumers need protection beside fraudulent, unfair and misleading business practices, including when things go wrong, to be able to gain redress. Regularly, organization/companies need to safeguard themselves against attacks to guarantee data integrity, confidentiality, authenticity and including some other major attacks like Reply and Man-in-the-middle Attack of data domain. Hence, it is necessary to occasionally review the regulatory framework so that consumers have effective protection when conducting eCommerce transactions. Equally necessary, eCommerce companies will need to develop and adopt a set of industry standards as addressed in the proposed framework to protect consumer privacy as a way of supplementing the formal legal obligations. Further, eCommerce businesses can build trust at an individual level by implementing industry best practices, which are underpinned by the proposed security framework that are enforceable.

There are many issues concerned in securing eCommerce Transaction e.g. Privacy, Access Control, Integrity, Non Repudiation and Confidentiality. These concerns are still ongoing research problem. The Internet, which is the crucial medium used for conducting eCommerce transactions, is not planned to handle transactions securely. In this paper an approach has been recommended, which covers Authentication, Non Repudiation and Integrity security objective in a secure manner.

In this paper secure eCommerce Protocol is proposed to provide protection against attacks. This Novel framework for secure eCommerce transaction is presented a new security framework to address security issues that face eCommerce consumers, merchant's organizations and policy makers along three dimensions—security, privacy and trust based on security objectives/goals. It also outlines a number of managerial policy and technical implications that will have to be taken into consideration going forward.

REFERENCES

1. Niranjanamurthy, M., and DR Dharmendra Chahar. "The study of e-commerce security issues and solutions." *International Journal of Advanced Research in Computer and Communication Engineering* 2.7 pp. 2886 - 2895 (2013).
2. Vahradsky, D. Cloud risk: 10 principals and a framework for assessment. ISACA,5, pp 1-12 (2012)
3. D. Berlin, "*Information Security Perspective on Intranet*," presented at Internet and E-Commerce Infrastructure, (2007)
4. C. Barnes, "*Hack Proofing Your Wireless Networks*," Syngress Publishing, Rockland, (2002).
5. Jose A. Onieva, "*Multiparty Nonrepudiation: A Survey*", ACM Computing Surveys, Vol. 41, No. 1, Article 5, pp. 1-5.42 (2008).
6. Anup K. Ghosh "*E-Commerce security: No Silver Bullet*" IFIP Conference Proceedings; Vol. 142, pp. 3 – 16, (1998)
7. L. X. Qin Zhiguang, Gao Rong, "*A survey of E-commerce Security*," Electronic Science and Technology of China vol. 2, no. 3, pp. 173 - 176 (2004).
8. N. M. A. Al-Slamy, "*E-Commerce Security*," IJCSNS International Journal of Computer Science and Network Security, vol. 8, no. 5, pp. 340 – 344 (2008).
9. Kenneth Longo Mlelwa and Zaipuna O Yonah. *Requirement's for Proposed Frameworks for Secure Ecommerce Transactions*. Communications on Applied Electronics 6(9): pp. 1-15, (2017).