IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Vol.-7, Issue-4, April 2019 E-ISSN: 2347-2693

Hybrid Model for Online Payment System with Object-Oriented Methodology

[1*]Amanze, B.C., [2]Okoronkwo, M.C., [3]Chilaka, U.L

[1]Department of Computer Science, Faculty of Science, Imo State University, Owerri, Nigeria
[2]Dept. of Computer Science, Faculty of Science, Micheal Opara University of Agriculture, Umudike, Nigeria
[3]Ph.D Student, Dept. of Computer Science, Imo State University, Owerri, Imo State, Nigeria

Corresponding Author: amanzebethran@yahoo.com

DOI: https://doi.org/10.26438/ijcse/v7i4.374385 | Available online at: www.ijcseonline.org

Accepted: 12/Apr/2019, Published: 30/Apr/2019

***Abstract*-** The business-to-consumer aspect of electronic commerce (e-commerce) is the most visible business use of the World Wide Web. The primary goal of an e-commerce site is to sell goods and services online with security of customers' giving optimum consideration. This paper deals with development of fraud detection and alerting system using Hidden Markov Model and Artificial Neural Network. The system is implemented using a 3-tier approach, with a backend database, a middle tier of WAMP Server, and a web browser as the front end client. In order to finalize payment of goods, the customer must authenticate this approach through Code and OTP match. Whereby the authentication process fails, the transaction would not be completed and real-time alert would be sent to both the e-commerce system and payment system. This will enable their (e-commerce and payment system) platform to electronically deactivate the victims' account.

***Keyword*: ANN, HMM, e-Commerce and Payment System**

I. INTRODUCTION

Fraud prevention is difficult in the faceless world of the Internet, and any measure designed to respond to it must be able to do so in a timely manner. Continuous assurance (CICA, 2009) offers a timely method of assurance where, by monitoring transactions (flows of information, especially payment and order details) in real-time, irregularities that point to illicit behavior may be promptly detected and dealt with. Continuous assurance systems capitalize on the infrastructure and real-time nature of e-commerce systems. In fact, continuous assurance systems rely on the system being assured to be a quick and reliable source of relevant data, because the assurance system must, in turn, provide its own service of delivering timely assurance and reporting information [1]. Such a system will be able to detect fraudulent activity in an e-commerce system in an unobtrusive manner. There is a need to develop an assurance system that can be easily integrated into existing systems, be flexible to adapt to different organizations and organizational change, and provide control over the assurance process.

This paper focuses primarily on improving our understanding of detecting and preventing fraud in e-commerce systems by some other fraud detection methods. It went ahead to provide a real-time alerting system as soon as potential fraud is detected or noticed. Meanwhile, a conceptual model relating the aspects and concepts associated with the real-time monitoring of e-commerce transactions for fraud will be developed.

The internet is the base for the fraudsters to make the frauds in the simply and the easiest way. Fraudsters have recently begun to operate on a truly transnational level. With the expansion of trans-border, economic and political spaces, the internet has become a new worlds market, capturing consumers from most countries around the world. The below described are most commonly used techniques in Internet fraud [2].

After the customer or the cashier swipes the credit card through a reader, the EDC software at the point-of-sale (POS) terminal dials a stored telephone number (using a modem) to call an acquirer. An acquirer is an organization that collects credit authentication requests from merchants and provides the merchants with a payment guarantee. When the acquirer company gets the credit-card authentication request, it checks the transaction for validity and the record on the magstripe for:

- Merchant ID

- Valid card number
- Expiration date
- Credit-card limit
- Card usage

In this system, the cardholder enters a personal identification number (PIN) using a keypad. The PIN is not on the card. That is encrypted in the cards database. (For example when we get cash from an ATM, that machine encrypts the PIN and sends it to the database to see if there is a match.) The PIN can be either in the bank's computers in an encrypted form or encrypted on the card itself. This type of cryptography where the transformation is used is called one-way. This means that it's easy to compute a cipher given the bank's key and the customer's PIN, but not computationally feasible to obtain the plain-text PIN from the cipher, even if the key is known. This was designed to protect the cardholder from being impersonated by someone who has access to the bank's computer files.

II. LITERATURE REVIEW

Electronic Payment System

In order to participate in the electronic payment system the customer and the merchant should access the Internet and initially they have to register the corresponding the payment service provider. The provider in turns provides the payment gateway that can be reachable from both public network and the private interbank clearing network. Here the gateway acts as the intermediary between the traditional payment infrastructure and the electronic payment infrastructure. On the other side customer and the merchant have their bank accounts at the bank that is connected to the clearing network. The customer bank (issuer bank) actually issued the payment instrument that the customer uses for his payment. The acquirer bank acquires the payment records [3]. When the customer is purchasing the goods and services, he chooses to apply through his debit or credit card. Before delivering the goods the merchant asks payment gateway to authorize the customer and his payments. The payment gateway contacts the issuer bank to get clear. If everything is fine the payment gate withdraws the money from the customer account and deposits in the merchant account and sends the notification to the merchant. Then the merchant delivers the goods and services to the customer [3].

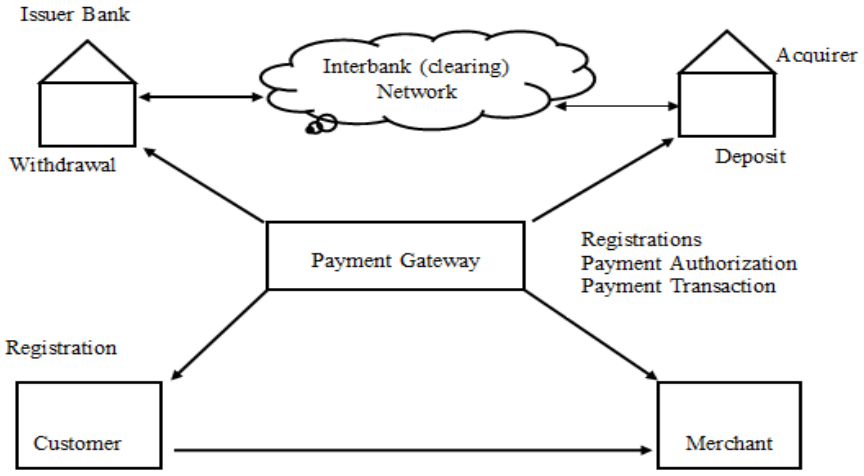

Figure 1: Security Fundamentals for e-Commerce (Hassler, 2011)

The major reason for developing an electronic payment system is that it provides organizations and consumers with a means of integrating individual commercial services into an electronic market place. According to [4], Lynch and Lundquist argue companies and consumers both of them will get benefit from the e-payment system.

- Companies will benefit from virtual markets because the concept of online shopping can make their business communication easier and cheaper.
- Consumers will benefit because on-line shopping is convenient and saves time.

The types of Electronic Payment System are Offline versus online, Debit versus credit, Macro versus Micro, The paper cash, credit cards and the checks are the types of electronic payment system but newly electronic payment system has introduced two types of payment instruments:

- Electronic money (digital cash)
- Electronic checks.

Common to the entire payment instrument is the fact that the actual flow of the money from payers account to the payee account [3].

Online Payment Using Credit Card

A credit card is a card that allows you to borrow money to pay for things. There will be a limit to how much you can spend called your credit limit. At the end of each month you can either pay off the whole of the amount you owe or make a minimum repayment" [5]. With the rising interest in e-commerce, electronic payment techniques have increased more in number. The most popular way is payment-using credit card, probably because of its simplicity and comfortable. The user just enters the relevant numbers, the merchant gets these validated and payment has been made. For extra security, the communication between user and merchant should be encrypted. Payment by credit card is the most popular and the easiest way to pay for goods and services online. A user simply enters his credit card number, his name and the expiry date of the card; the merchant validates this information and upon approval from the credit card company, ships the goods or provides access to the service. The only thing that needs to pass between the merchant and the buyer is the credit card number.

Evolution of Credit Card

A credit card is a great financial tool. It can be more convenient to use and carry than cash and it offers you valuable consumer protections under federal law. However, it is also a big responsibility. If not used carefully, you may end up owing more than you can repay, damaging your credit rating and creating credit problems for yourself that can be difficult to fix. Credit cards, as we know them today, have been around for just over half of a century. One of the first credit cards appeared in 1951 when loan customers of Franklin National Bank of New York were screened for credit and those approved were given a card they could use to make retail purchases. Participating merchants copied the customer information from the card onto a sales slip and the bank would credit the merchant account for the loan less a flat fee to cover the costs of providing the loan.

In 1958, The American Express Company (a company built on the traveler's cheque business) began issuing a charge card for travel and entertainment charges, which was accepted at participating restaurant, hotel and airline merchants [6]. Cardholders enjoyed the convenience of plastic charge cards (especially when on the road for business) as well as the line of credit offered by the new bank credit cards. Merchants found that credit card customers usually spent more than if they had to pay with cash (which is still true today – the average credit card purchase is 112% more than if cash is used). Accepting bank-issued cards was safer for the merchant than dealing with cash (more secure from internal and external theft and error) and less expensive than creating and maintaining a merchant-specific credit program [6].

Credit Card Processing

As the credit card processing became more complicated, the outer service companies started to sell processing services to Visa and MasterCard association members. This makes to reduce the cost of programs for banks to issue credit cards and settle accounts with cardholders and this makes the greater expansion for the payments industry [6].

The rules and standardized procedures of Visa and MasterCard are developed for handling the bankcard paper flow in order to reduce fraud and misuse of cards. The two associations also created international processing systems to handle the exchange of money and information and established an arbitration procedure to settle disputes between members.

[7] Developed a work on fraud prevention by describing the security measures to avoid unauthorized individuals from initiating transactions on an account for which they are not authorized. The key point of this work was to identify unauthorized activity once the fraud prevention has failed. [8] Had a work whose main objective is to evaluate if it is possible to combine two statistical methods, Benford's law together with statistical quantiles, to find a statistical way to find fraudsters within a Mobile Money system. [9] Developed credit card fraud detection model using Hidden Markov Model (HMM) which is a statistical tool and extremely powerful method used for modeling generative sequences characterized by a set of observable sequences. However, all the above mentioned works concentrated on fraud detection. They lack fraud monitoring and real-time alert. The idea of generating one time password (OTP) and email code using a standard statistical approach like HMM, Support Vector Machine (SVM) was not captured. These codes should be generated and sent to the customer through different media (email and phone) before transactions are completed.

Analysis of the Existing Systems

1. Data Mining and Detection Techniques

This uses data mining approach and techniques in detecting credit card fraud. Data mining refers to a family of machine learning techniques capable to analyze and extract non-trivial patterns from data (Chen, et al., 2012). The detection techniques using data mining are:

a) **Artificial Neural Network:** This imitates the way human brain works. It makes use of nodes which are called neurons. The neurons are computational units which are used to process some input information and produce some output [10].
b) **Support Vector Machines (SVMs):** This is suitable for credit card fraud detection because only two classes are needed; namely the "legitimate" and "fraudulent" class. SVM tries to calculate an optimal hyper plane which will separate the samples of the two classes [11].

2. **Fraud Detection Using Mathematical Statistics Approach**: This technique as described used statistical quantiles to find a statistical way to find fraudsters within a mobile money system. To achieve this, the following algorithm is used.

Fraud detector Algorithm

```
1.  procedure Detect Fraud (quantile, time Span, logs Path)
2.  if quantile = 95 then
3.   limits = limits for 95%-quantile*time Span
4.  else
5.   limits = limits for 99%-quantile*time Span
6.  records = read Records (logsPath)
7.  for all record in records do
8.   if records = transaction Record then
9.   Is Fraud =  check If Fraud (record, rule, limits)
10.  if is Fraud = true then
11.  Alarm (record)
```

Disadvantages of the Existing System

Implementing a fraud detection tool using data mining techniques involves a number of challenges which needs to carefully be considered.

1. **Noise:** This is simply the presence of errors in the data, for example incorrect dates". Missing values are also considered as noise. Noise can result in an erroneous model construction with bad predictive accuracy. The process of removing noise is called data cleansing. Depending on the concerned data set; data cleansing can be a very complex task.
2. **Supplying Labeled Training Samples:** Finding training samples and providing the right class labels for model construction can also be a very complex task. This is one of the biggest challenges of supervised learning techniques since labeled training samples may not always be available.
3. **Overlapping Data:** Overlapping occurs when a fraudulent transaction looks very similar to a legitimate one or when a legitimate transaction looks very similar to a fraudulent one. This is also a problem because it can lead to an erroneous model construction.
4. **Choosing Parameters:** Most of data mining techniques require a number of parameters including thresholds to pre-set by the user. Different parameters can lead to completely different model performance. This increases the complexity of model construction.
5. **Feature Selection:** Selecting the features – also known as attributes or columns – of the data set that should be used to construct the detection model can also be a challenge. Many articles in the literature suggest the features that should be used to achieve better results.
6. **Over-fitting:** Generally the training data set always contains few errors or random values even after data cleansing. These are known as "small fluctuations" in the data. Over-fitting occurs when the algorithm used in model construction, tries to learn as many information as possible from the training data set including this small fluctuations which do not represent the real situation. This can lead to a very complex model with poor predictive accuracy.

Analysis of the New System

The new system is a joint approach of Hidden Markov Model (HMM) and Artificial Neural Network (ANN) in online fraud detection and monitoring as shown in figure 2. The HMM will be used to generate PIN, One Time Password (OTP) and e-mail Code. These authentication codes will be manipulated using ANN before online transaction will be completed. This system will be embedded in the present e-commerce system to enhance security and reduce external fraud. This approach will enable the system detect fraudsters and send alert to the admin if imposture (intruder) tries to complete financial transaction with customer's e-commerce account. As soon as this alert is sent to the main e-commerce system, the account is temporary blocked

and the Internet Protocol (IP) address of the intruder is automatically sent and stored in the fraud database as an evidence for forensic investigation.

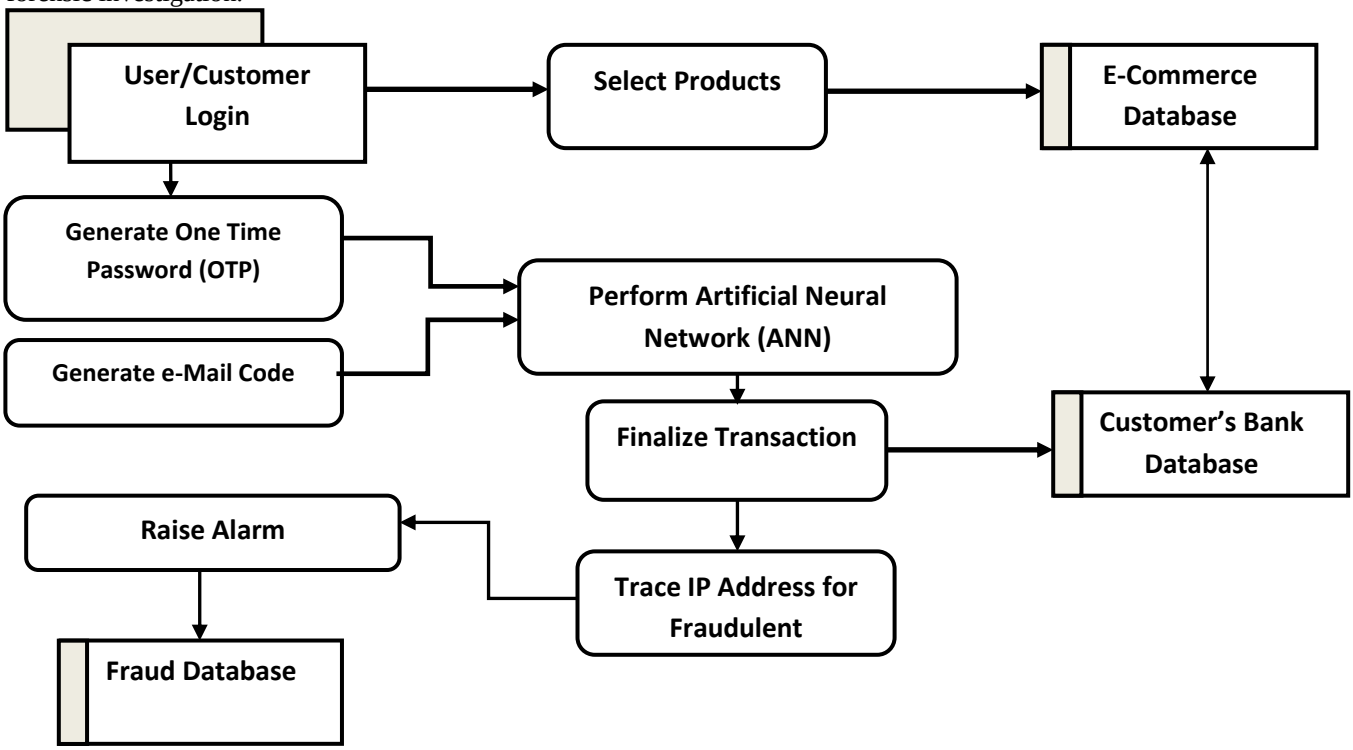

Figure 2: DFD of the New System

Methodology

Research methodology (methodology) shows the procedure to be taken in order to achieve the objectives of the research study. This shows how relevant information about the study would be sourced and also, the instruments or techniques that would be applied in the analysis.

There are acceptable international systems developments or research standards for transforming ideas into the design phase. Some of the acceptable standards or methodologies include the following:

1. The structured systems analysis and design methodology (SSADM)
2. Unified modeling language
3. Prototyping
4. Usability Engineering Methodology

Methodology Adopted

In this paper, the Object Oriented Design Methodology was adopted. This model commonly use objects for analysis. Meanwhile, the requirement analysis, system analysis and design and implementation of the process of OODM for the new system is shown in table 1.

Table 1: Process of OODM for the New System

Requirement Analysis	**Functional**	**CBD Methodology**
	Non Functional	**UML Methodology**
System Analysis and Design	**Functional**	**CBD Methodology**
	Non Functional	**UML Methodology**
Implementation	**Functional**	**Object Oriented Programming**
	Non Functional	**UML Methodology**

CBD: Component Based Development

Fraud Detection System of the New System

The new fraud detection system works using two approaches:

1. Hidden Markov Model and
2. Artificial Neural Network.

A. Hidden Markov Model

The Hidden Markov Model is used generate the one time password and e-mail code. The password and code generation system is shown in Algorithm.

Algorithm

1. given: Transaction Model T (S, S')
2. Sensing Model S (S,O)
3. Observations O_1, ……, O_T
4. Find: Most probable S_1, ……..., S_T
5. Initialize S x T matrix V with O_S
6. $V_{0,0} \leftarrow 1$
7. for each time t = 0 to T – 1
8. for each state S
9. for each new state S'
10. score ← Vs,t * T(S,S') * S(S',Ot)
11. if score ≠ 0 and > 0,
12. generate codes
13. Else
14. back from S with Max $V_{S,T}$
15. End If
16. End

A. Artificial Neural Network

After successful generation of one time password and e-mail code artificial neural network model of them with the customer code (PIN) are integrated to generate output. The password, email code and PIN act as the input layers. They are integrated in the hidden layer to form the output layer. Figure 3 shows the Artificial Neural Network approach.

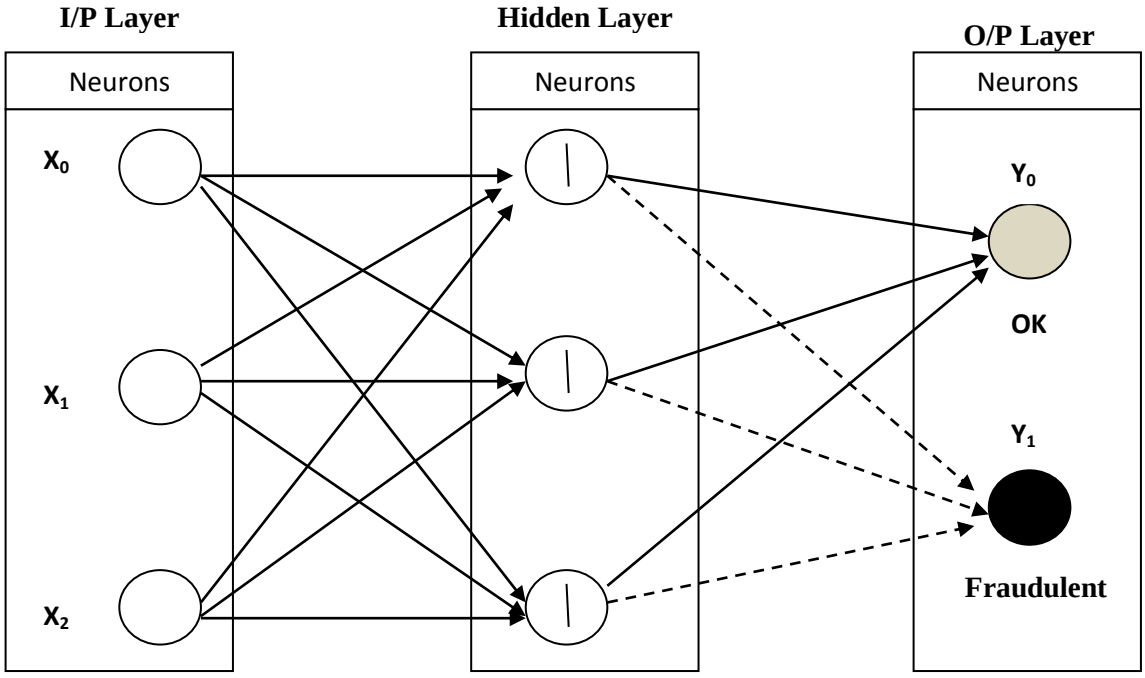

Figure 3: Artificial Neural Network of Fraud Detection System

Explanation:

X_0, X_1 and X_2 are the input neurons which generated as follows:

X_0 = customer's PIN

X_1 = OTP (one time password)

X_2 = eMail code

These input neurons are integrated in the hidden layer to form output layer Y_0 or Y_1.

Y_0 = successful integration of the input neurons.

Y_1 = unsuccessful integration of the input neurons.

Object Diagrams

Activity Diagram of the Ordering System

The activity diagram of the ordering system is shown in figure 4.

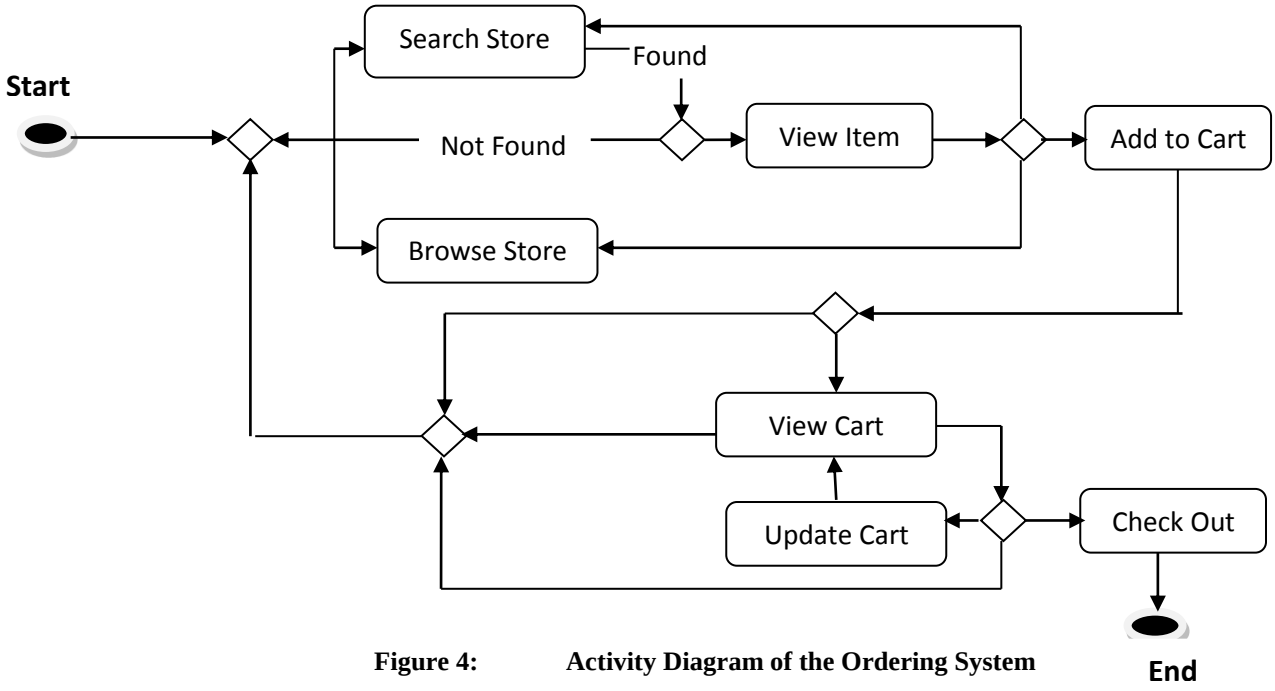

Figure 4: Activity Diagram of the Ordering System

Activity Diagram of the New Payment System

The activity diagram of the new payment system is shown in figure 5

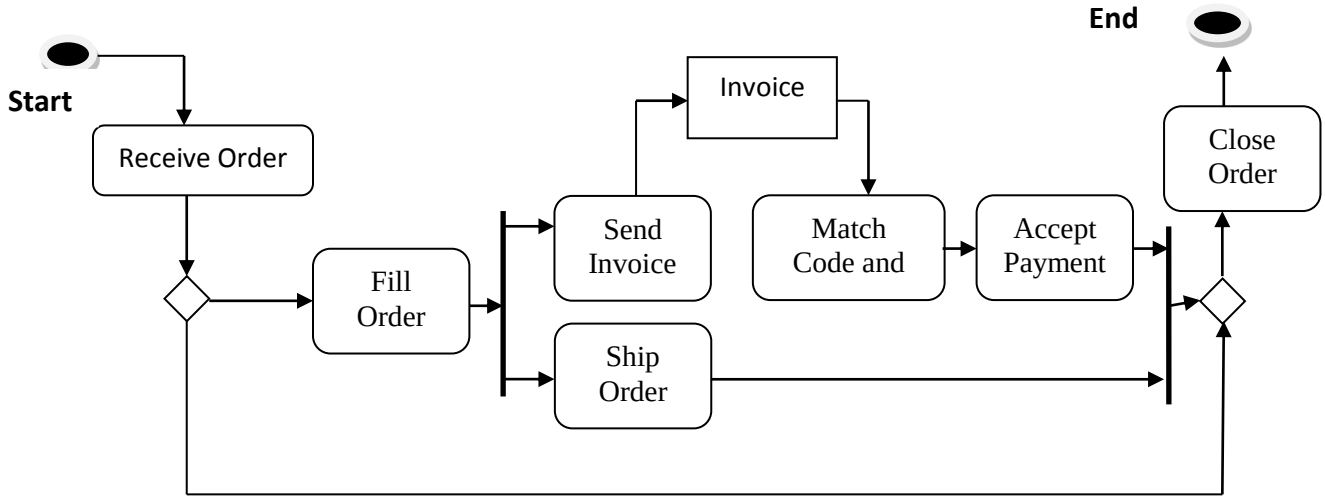

Figure 5: Activity Diagram of the New Payment System

4.8 Components Diagram of the Ordering System

The components diagram of the ordering system is shown in figure 6

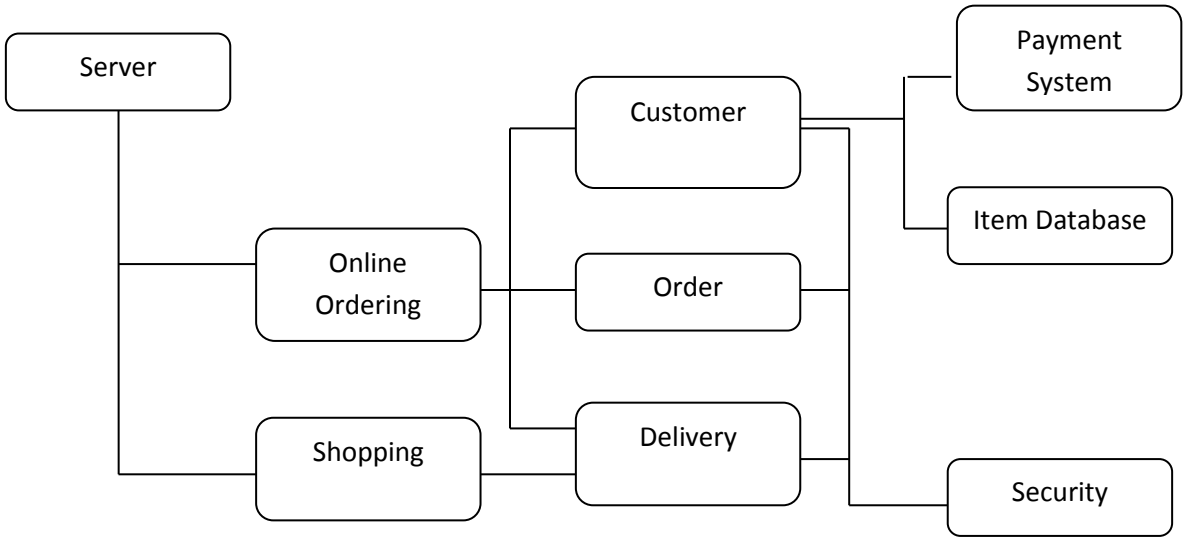

Figure 6: Components Diagram of the Ordering System

Components Diagram of the New System

The components diagram of the new system is shown in figure 7

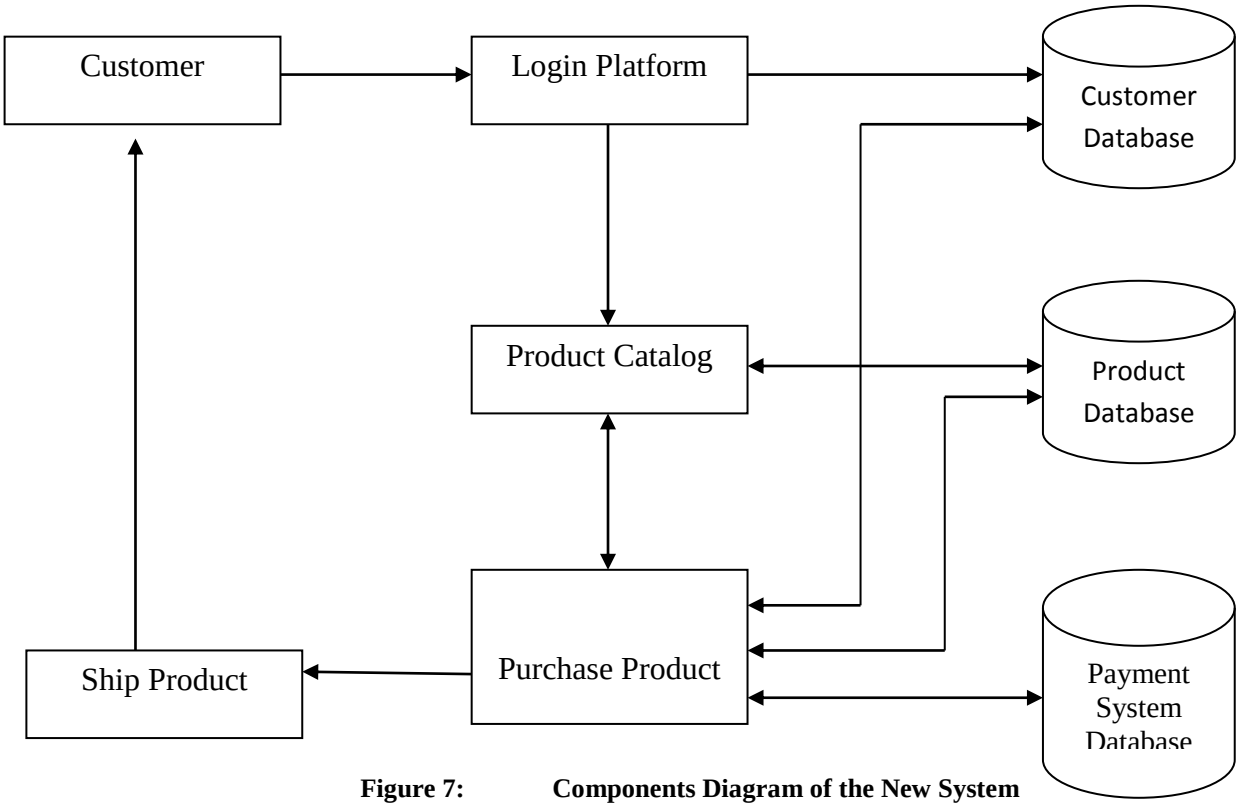

Figure 7: Components Diagram of the New System

4.9 Sequence Diagram of the Products Ordering System

The sequence diagram of products ordering system is diagrammatically represented in figure 8

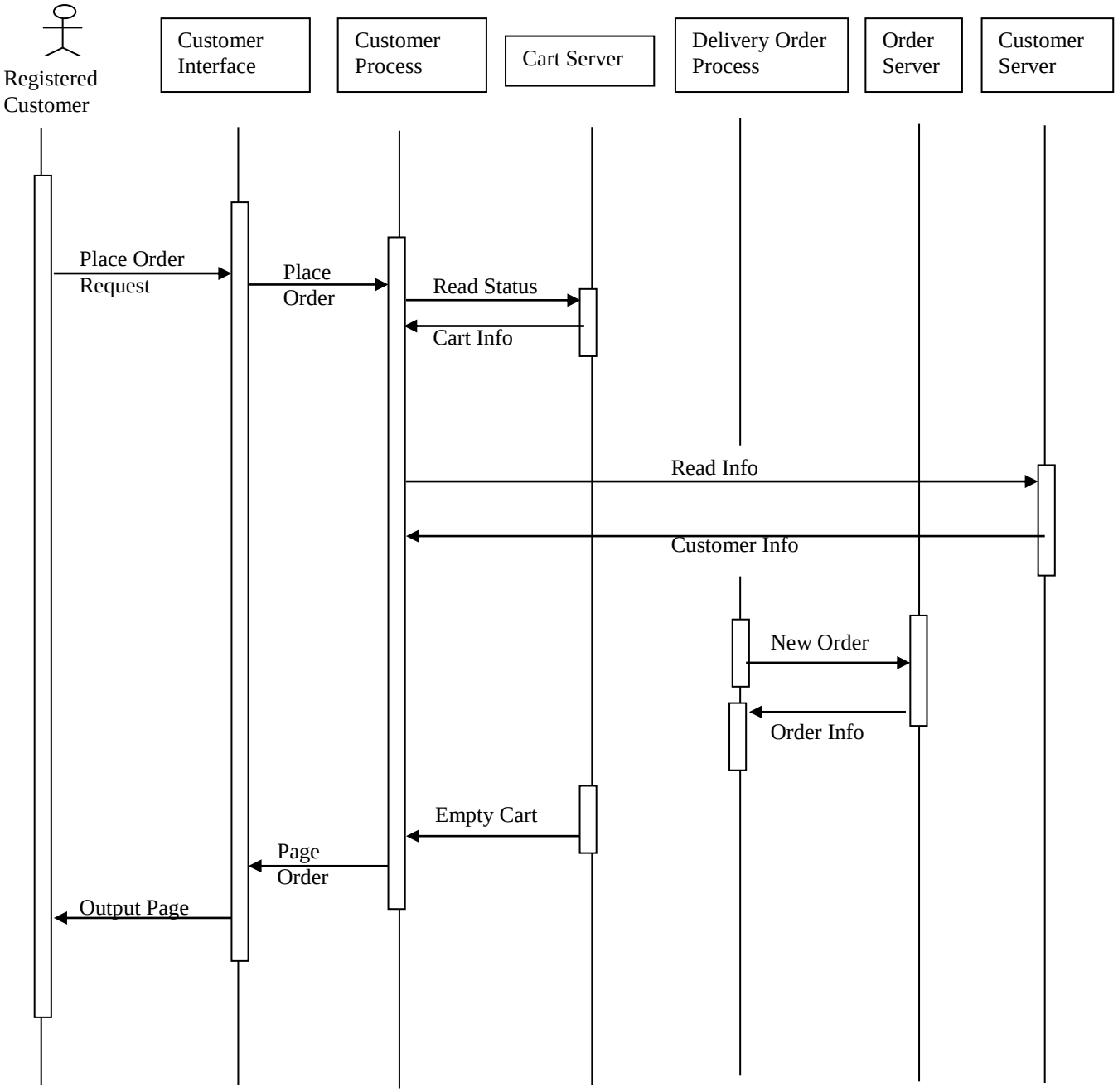

Figure 8: Sequence Diagram of the Products Ordering System

Sequence Diagram for the Payment Process

The sequence diagram of the payment process is diagrammatically represented in figure 9

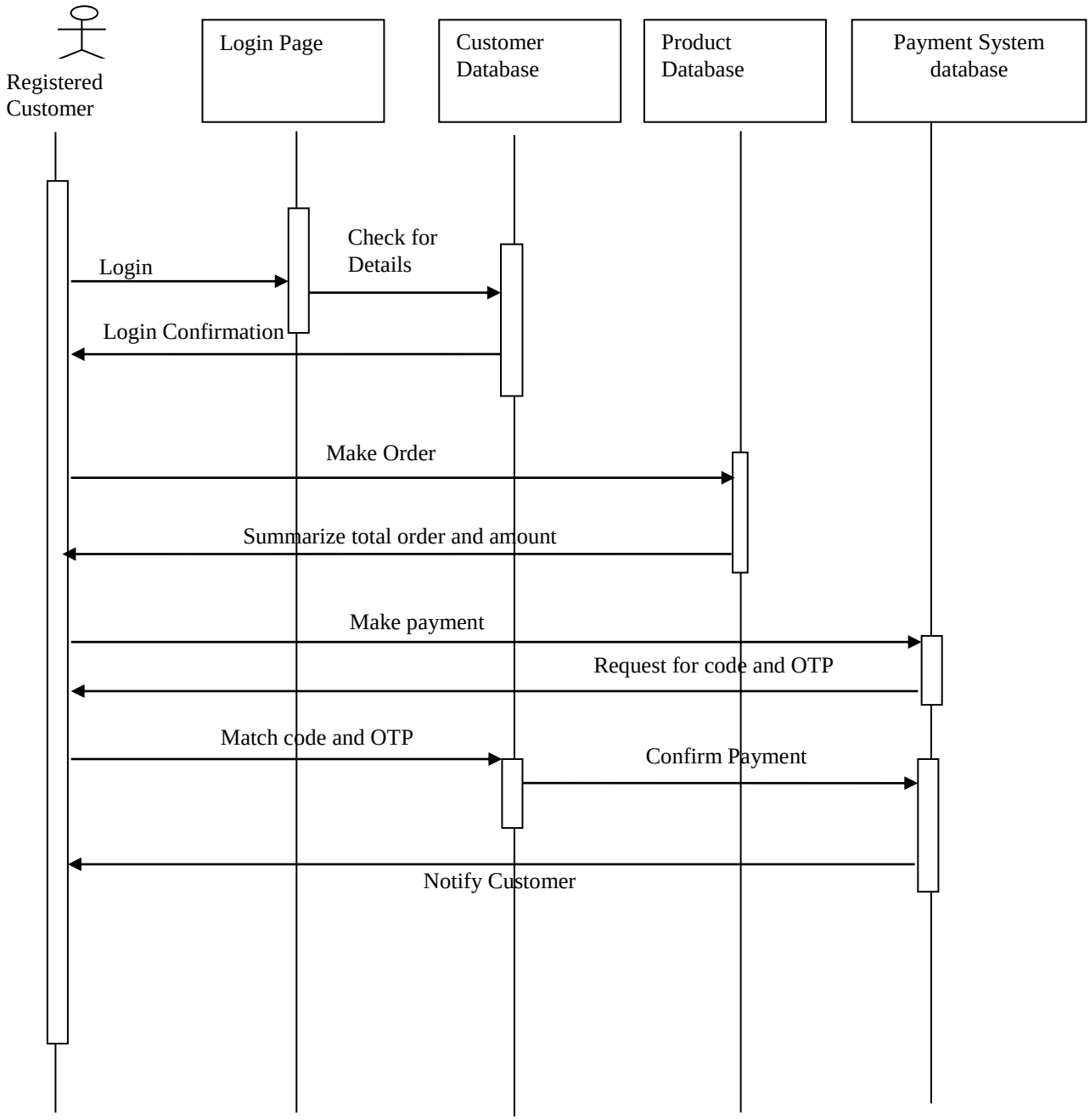

Figure 9: The Sequence Diagram of the Payment Process

Collaboration Diagram for Customer Login

The collaboration diagram for customer login of the new system is shown in figure 10.

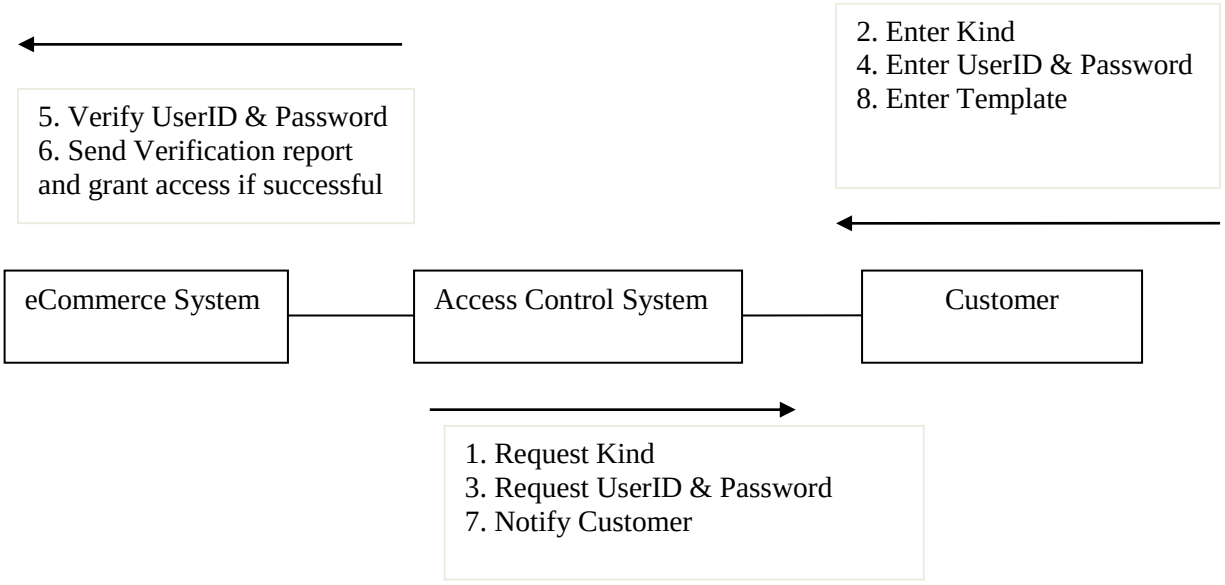

Figure 10: Collaboration Diagram for Customer Login

Figure 10 represents the collaboration diagram for customer login. The requests and responses are labeled in their order of precedence. The order of precedence is as follows: request kind, enter kind, request username and password, enter username and password, verify credentials, send verification report and notify customer. Once the username and password are verified the customer is allowed to log into the e-commerce software.

Collaboration Diagram for Customer Payment Completion

The collaboration diagram for Customer Payment Completion of the new system is shown in figure 11.

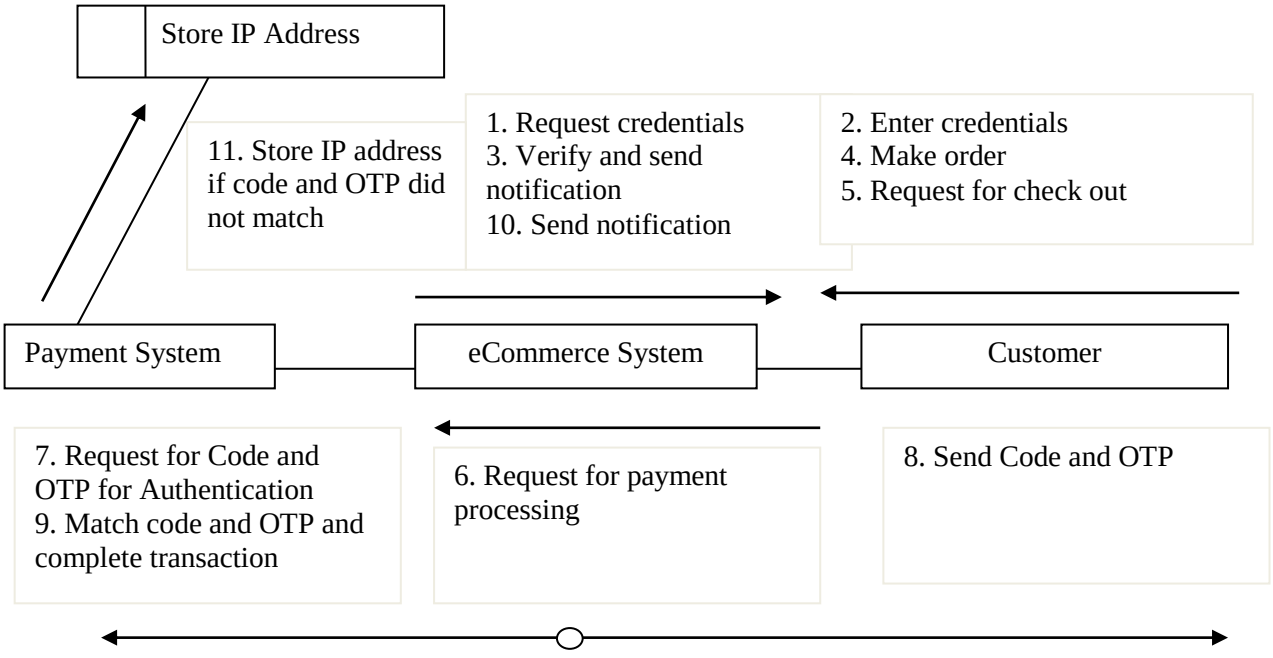

Figure 11 Collaboration Diagram for Customer Payment Completion

Figure 11 represents the collaboration diagram for customer payment completion. The requests and responses are labeled in their order of precedence. The order of precedence is as follows: request kind, enter kind, verify credentials, make order, request for check out, request for payment processing, request for Code and OTP, send Code and OTP, perform Code and OTP match, complete transaction and store IP address.

Conclusion

The Internet has become a major resource in modern business, thus electronic shopping has gained significance not only from the entrepreneur's but also from the customer's point of view. For the entrepreneur, electronic shopping generates new business opportunities and for the customer, it makes comparative shopping possible. As per a survey, most consumers of online stores are impulsive and usually make a decision to stay on a site within the first few seconds. E-commerce store is like a conventional shop interior. If the shop looks poor or like hundreds of other shops the customer is most likely to skip to the other site. Meanwhile, the issue of security and fraud has discouraged many not patronize and make effective use of e-commerce. Hence one have designed the paper to help e-commerce companies and payment companies to detect fraud.

In this paper, the user is provided with a scalable security platform that is to be attached to the existing e-commerce platform that can be used to buy products and authenticate payments online. One will surely agree with me that e-commerce is not a new nomenclature within the modern day economic parlance but yet has not yet been fully embraced amongst many people because of fear of fraud.

In this paper one have successfully taken a full plunge to unveil these constraints to the commonwealth of global opportunities; and not just to recommend solution but to develop an enduring solution comparative to what obtains anywhere in the world. In the course of trying to find out on the veracity of these problems we had tried to follow the standard procedure by visiting the product-dealers to ascertain their extent of knowledge of opportunities inherent in e-commerce and their level of acceptability or constraints to acceptance. The result one got was more a propeller this research enquiry. Thereafter, one had reviewed various scholarly publications to get acquainted with details of earlier research-works in this regard. However, though this research-work seemed ended at the moment having covered its earlier stated scope, but a seemingly endless next phase comes with sensitization which would go beyond the scope of the earlier conducted survey to ensure global awareness, trust and acceptability. Very important to note also, the process of developing this application and the adjoining literary exposures had been very exploratory; expounding on the various technological implementations had also been very interestingly awesome; as one becomes acquainted with the nitty-gritty of the various components such that when integrated performs the "wonders" of internet. One therefore have achieved a technology that demonstrates a high level of trust, security and cost-effectiveness and very user-friendly.

Recommendation

One recommend that this system be deployed by every e-commerce and payment system to detect and reduce fraud. This would encourage customers and non-customers into using e-commerce. One also recommend that more security features be added by subsequent researchers.

REFERENCE

[1] Vasarhelyi, M.A. (2010): 'Expert System in Accounting and Auditing/f Artificial Intelligence in Accounting and Auditing.
[2]Bhatla, T. P. (2013): "Understanding Credit Card Frauds" Card business review. http://www.tcs.com/0_whitepapers/htdocs/credit_card_fraud_white_paper_V_1.0.pdf.
[3] Hassler, V. (2011): "Security Fundamentals for E-commerce", computer security series.
[4] Tae-Hwan, S., Paula, S. (2008): "Identifying Effectiveness Criteria for Internet Payment Systems", A Journal of Internet Research: Networking Applications and Policy, v-8 number 3, pp 202-218.
[5] Edwards.com
[6] Creditcard.com
[7] Kovach, S and Ruggiero, W. V. (2011): "Online Banking Fraud Detection Based on Local and Global Behavior" ICDS 2011: The Fifth International Conference on Digital Society.
[8] Kappelin, F. and Rudvall, J. (2015): "Fraud Detection within Mobile Money: A mathematical statistics approach" MSc Thesis submitted to the Dept. Computer Science & Engineering Blekinge Institute of Technology SE–371 79 Karlskrona, Sweden.
[9] Chen, M., Han, J. and Yu, P. S. (2012) "Data mining: An Overview from a Database Perspective," IEEE Transactions on Knowledge and Data Engineering, vol. 8, no. 6, pp. 866-883.
[10] Ngai, E., Hu, Y., Wong, Y., Chen, Y. and Sun, X. (2011): "The application of data mining techniques in financial fraud detection: A classification framework and an academic review of literature," *Decision Support Systems,* pp. 559-569, 2011.
[11] Meyer, D. (2012): "Support Vector Machines," Technische Universit¨at Wien,, Austria, 2012.

