Academic Journal of Applied Mathematical Sciences
ISSN(e): 2415-2188, ISSN(p): 2415-5225
Vol. 6, Issue. 8, pp: 153-160, 2020
URL: https://arpgweb.com/journal/journal/17
DOI: https://doi.org/10.32861/ajams.68.153.160

Academic Research Publishing Group

Original Research

Open Access

Response Triggered Architecture for E-Payment Examined for General Purpose Transaction

Akomolafe Dipo Theophilus (Corresponding Author)
Department of Mathematical Sciences, Olusegun Agagu University of Science and Technology, P.M.B. 353, Okitipupa, Nigeria
Email: dtakomolafe@yahoo.com

Adeola Oladele Stephen
Department of Computer Science, Federal University of Technology, P.M.B. 704, Akure, Nigeria

Article History
Received: July 30, 2020
Revised: August 17, 2020
Accepted: August 21, 2020
Published: August 25, 2020

Abstract

The explosive growth in internet coupled with advancement in Information and Communication Technology (ICT) has made business transactions much easier than it used to be in the past. For example, e-commerce has particularly benefited from the introduction of GSM system. One of the major challenges, however, is how to isolate fraudulent transactions from genuine businesses. This becomes more imperative as the advancement in ICT has brought with it fraud and related scams. In this work, we examined different types of e-commerce as well as the challenges being encountered in the course of daily transactions. We took advantage of the current trends in mobile communication networks, particularly GSM and proposed a system based on Response Triggered Architecture for electronic transaction. Our proposed system is platform independent which means only little modification is needed when switching from one platform to another. We used Visual.basic.net and knowledge in fraud for our system prototype and presented the results in the body of this work.

Keywords: E-commerce; Fraud; Database; Security; Internet.

1. Introduction

Dated back to pre-historical times, man has always found some means of transacting business. There was an era of trade by barter where goods were exchanged for one another based on face values. Normal and John [1], describes barter as transaction in which goods are exchanged without the use of money. Originally, it was on a person-to-person basis, but now occurs more frequently in the form of international trade. With time, man invented more abstract ways of representing values. For instance, in South-western Nigeria, primordial means of business transaction was the use of cowries as a means of payment. But as civilization improved, man began to device easier means for financial transaction. This era witnessed the use of currencies in different national denominations. Also, explosive growth and improvement in the understanding of economic principles has led to the introduction of Postal Order, Money Order, Bank Drafts and Bank checks. All these have their advantages and disadvantages.

However, the advent of Electronic Technologies particularly the Internet ushers in the birth of Electronic Commerce (e-commerce) and all that it entails. Amos [2], describes e-payment as a subset of e-commerce transactions that makes possible electronic payment for goods and services through the Internet. Thus, the use of Master card, VISA card, e-money transfer (eco-transfer, Western Union Money transfer) and lately GSM activated e-banking are some of the innovations brought about by explosive growth of Internet and allied technologies. Each of these technologies has some benefits and its own set of complexities and disadvantages.

As advancement in technology increases, the level of complexities in managing fraud increases too. It becomes increasingly difficult to monitor the networks for effective real-time transaction. In typical real-time scenario, the transaction takes place simultaneously in probably thousands of nodes around the world, so also is the issue of security of the networks. The safety of a transaction depends largely on the safety of the network. Cyber-fraud is not peculiar to Nigeria only; it has become synonymous with Internet browsing around the world [3].

The advent of Internet technologies ushers in the birth of internet commerce. Also, the introduction of Global Mobile System (GSM) in Nigeria [4] has opened up Nigeria's economy and Nigeria is gradually being integrated into the global economy. Our concern here is not how versatile, but how reliable the Internet payment system is. In fact in Nigeria, [5] reported cases of Nigerians defrauding foreigners of millions of dollars. From the foregoing, there is an avalanche of evidence to conclude that extra-security is needed when transacting business electronically in Nigeria today.

This work is therefore proposing a response triggered security model for electronic commerce. Before going to the details of the design, it is necessary to give an insight into the current payment methods and how fraudsters operate. Nigerian fraudsters operate in diverse ways and their tricks and activities are limitless.

2. Payment Methods

Payment methods could be classified into two main categories viz-a-viz offline and online systems. Offline payment system involves only two parties' vis-à-vis the payer and the payee. These include physical cash payment system and all hardware based payment systems such as Mondex. Mondex has the capacity of handling different currencies but it is not widely used. On the other hand, online payment system is a more advanced form of payment system, more complex, and difficult to secure. Online payment system typically involves remote based transactions which encompasses communication between two remote computers. Some could be in a secure domain which could be public. The public domain is more susceptible to attack possibility but one has to pay for maintenance for using the secure domain. Also fees are charged depending on which type of transaction you are carrying out on the system. Some of the popular payment systems in Nigeria are discussed below.

2.1. Electronic Fund Transfer (EFT)

Electronic Fund Transfer (EFT), according to Margaret Rouse Electronic Funds Transfer (EFT) [6], is a system of transferring money from one bank account directly to another without any paper money changing hands. Comptroller's Handbook [7], refers to EFT as "any transfer of funds which is initiated through an electronic terminal, telephonic instrument, computer, or magnetic tape so as to order, instruct, or authorize a financial institution to debit or credit an account [7]. EFT is an instruction to transfer money from one account to another remote location using electronic machine. EFT refers to any transfer of funds initiated through an electronic terminal, including credit card, ATM, Fedwire and point-of-sale (POS) transactions. Example of this is Direct Deposit, in which case payroll is deposited straight into an employee's bank account. It is used for both credit transfers, such as payroll payments, and for debit transfers, such as mortgage payments. This service is provided by banks and other financial institutions for the sake of making money available immediately or in real time. It acknowledges receipt of transfer soon as the money is transferred. Examples of this are Western Union Money Transfer and Economy Transfer. Also, almost all Banks are now involved in these types of transfer.

The major drawback of this scheme is the fact that banks and other financial institutions involved in this scheme are not transparent in the handling of cash transfer through them particularly in Nigeria. The issue of transfer here involves being committed to the transacting parties vis-à-vis the sender and the recipient. It is not unusual in Nigeria to find a situation where money is sent to the recipient in dollars and the bank refuses to pay in dollars and instead pays in local currency. The main motive in this case is to short-change the recipient during the process of converting to local currency.

2.2. Automated Fund Transfer

This mode of cashing fund is rapidly becoming a de-facto means of withdrawing relatively small amount of money up to the tune of #80,000.00 from banks nowadays. Upon registering for the product, the user is given a machine readable card which is used for any transaction with the bank. The User is made to select his withdrawal options when registering for the card. The options include the amount to withdraw and pin code. The machine works in an interactive manner. Users are asked to supply their identification code (PIN). This pin code is used to give access to the account. Cash balance could be assessed before and after withdrawal. A user is, however, not allowed to withdraw huge amount from his account basically for security reasons. Fraudsters are working fervently to subvert the noble objective behind this scheme. Multiple cashing of fund has been occasioned in Nigeria. The fraudsters take advantage of slow servers of some of the financial institutions by collecting money in quick succession from multiple machines before the transaction is committed.

2.3. Purchase Order

This is an order based on transaction system that does not really involve instant payment. What is essential here is the client instruction that certain amount of goods should be supplied with guaranty that the money would be paid later. It should be noted that it is not a payment system per se but an order for good with the assurance of paying later.

2.4. GSM Payment System

The latest innovation to payment system is the use of GSM for transferring money. Money could be transferred from friends and relatives in form of credit units through GSM. Some network vendors offer subscribed services that provide means of settling School bill, NEPA bill, School bill and other designated bills. The services provided by each vendor could be found on their websites.

2.5. Internet Payment System

The advent of internet technologies has radically changed the ways in which cash is being paid. This has led to electronic commerce. The scenario created is the world that has become a global village. One can call, work and trade over the internet. Such payment systems include First Virtual, Cyber-cash e.g. VISA Card, Master Card, Debit Card, Wirecard and Micro-payment Card. These are the most widely used among them.

2.6. Electronic Cash

Various systems have been developed which permit transactions to be carried out securely on the Internet through the use of electronic cash, or value tokens which are recorded digitally on computers. The Digicash system, for example, which is based in the Netherlands, uses a form of electronic money known as 'E-cash'. Before purchases can be made, both the merchant and the customer need to establish banking arrangements and Internet links with the bank issuing the E-cash. The customer first requests a transfer of funds from his or her bank account into the E-cash system. This is similar to withdrawing cash from an ATM. The E-cash system then generates and validates E-cash coins which the customer is able to use on the Internet. The coins are data streams digitally signed by the issuing bank using its private key. The customer is then able to send E-cash to any merchant who will accept this form of payment using the software provided by the E-cash service provider. The customer encrypts the message and endorses the coins using the merchant's public key. The merchant then decrypts the message with its private key and verifies the validity of the coin using the issuing bank's public key. The merchant is then able to turn E-cash into real funds by presenting the E-cash to the issuing bank with a request for an equivalent amount of real funds to be credited to the merchant's bank account [8].

3. Electronic Fraud

3.1. Electronic Chatting

In Electronic chatting, the primitive ways of the fraudster operation is through instant messaging or chatting. Unsuspected victims are lured into revealing their credit card information through dubious transactions normally arranged to generously reward the victim. Also victims are lured to juicy contract or money making venture and in the process made to reveal details of his account with the ultimate aim of duping through advance fees fraud. It should be noted here too that the victims are culpable too as they seek to get reward where they did not sow. For example, victims are made to believe there is a lump of money left unclaimed by dead relations, personality or government officials. They then seek gratification typically 10% from unsuspecting individual to facilitate transfer of the money to their account.

3.2. Attacks Through Unscrupulous Site

This is the means of defrauding people through unscrupulous websites. The site advertises goods and services which are tempting through reduced prices and bogus offers. Victims are then made to pay for the goods and services using the facilities of the sites. Their credit card number is now hacked through some means which may include use of sophisticated software and reused on behalf of the real owner. Also, it is common for fraudsters to clone an authentic site with just little variance in the address of a popular site. Through this means, unsuspecting victims are defrauded.

3.3. Crypto-Analysis Attack

Eric Conrad [9], describes cryptographic attacks as attacks designed to subvert the security of cryptographic algorithms. The primary goal of cryptographic attacks is to attempt to decrypt data without prior access to a key. This is a means of attack to the security of a system in order to gain entry into the systems. This form of attack is more sophisticated and only a learnt analyst could infiltrate the system. Cryptographic analysis is based on mathematical proof where the encryption of the original message, which could be PIN or other information, is decoded. The information is now used at the original owner's disadvantage.

3.4. Unauthorized Access to PIN Code

One of the points not yet mentioned here is the outright stealing of the security PIN of the subscriber. When the PIN number of the subscriber is stolen, it can be used on behalf of the original owner by the thief. This has been used on several occasions to defraud subscribers.

Normally, subscribers are supposed to keep the PIN code secured as possible but cases of husband/Wife/Children gaining access to each other's PIN, either based on ignorance or due to number of trust, abound. Presently, there is no way the system could detect whether the real owner is using the PIN code or not. This work would therefore provide a lead way by introducing acknowledgement of receipt of the transaction before it is committed.

3.5. Phishing

There exists a class of people popularly known as "Yahoo-Yahoo" boys and girls in Nigeria whose activities include "phishing". Phishing is a deceptive way of stealing personal information. The modulus operandi involves sending emails to prospective victims purported to have come from companies that look very official. The links to the company's Web site may be included. The e-mails usually discuss a problem with billing or use of a credit card and ask the recipient to provide personal information such as a credit card number, the credit card holder's name, security pin number, and expiration date. If such information is supplied, then the yahoo boys would use it to impersonate and carry out nefarious transaction(s).

3.6. Telemarketing Fraud

It is a known practice for many companies to sell their products and services through advertisement on the internet. In most cases, this is legitimate. They may offer to call the consumer or alternatively provide their phone number for prospective consumer to call them. Also charities use telemarketing. Fraudsters can also disguise as charities to woo their prospective clients.

3.7. Advance Fees Loans Schemes

This group of fraudsters promises to give loan irrespective of a person's credit position. They however ask for a token fee before the loan is disbursed. The gist of so-called 'advance fee schemes' is to trick prospective victims into parting with funds by persuading them that they will receive a substantial benefit in return for providing some modest payment in advance. The characteristics of this type of fraudulent scheme usually entail enlisting the services of the prospective victim to assist in an activity of questionable legality, thus providing some assurance that the victim would be unlikely to report the matter to the police, once defrauded. Examples of online advance fee schemes include pyramid schemes that have the primary purpose of enlisting individuals to earn money through recruiting other persons such as through the use of Email chain letters and electronic mailing lists. The Internet is also being used as a medium for Ponzi investment schemes and a variety of fraudulent business opportunity schemes as well as schemes that make use of on-line auctions [8].

3.8. Credit Repair

Good credit is important. A bad credit history can prevent you from getting a loan, housing or a job. Promises to fix your credit report may be tempting but they are not true.

3.9. Government Grants

This category of fraudsters' claim they have free government grants from US government asking for personal information. This information may include your social security number and bank account number. Also prospective victims are asked to pay processing fees. All these they do to steal your personal identity.

3.10. Job Scams

These people promise to get you lucrative jobs anywhere in the world or as the case may be. At times you are asked to provide lengthy information and undergo some legal formality to make the transaction look real but they eventually dupe you by asking for processing fees.

3.11. Bogus Credit Card Offers

The formal way of purchasing goods and services on the internet is through the use of credit card. However the site you are using the card may be a phony site. The purpose of the card at times is to steal your credit card information.

3.12. Telephone Cramming

Extra services can be obtained from the telephone operator apart from the normal voice service. Such services include voice mail, paging, internet access etc. But when charges show on your bill for services you never agreed to buy, the possibility is that you have been crammed. Other fraud cases on internet include the following: Auction Fraud; Counterfeit Cashier's Check; Credit Card Fraud; Debt Elimination; Parcel Courier Email Scheme; Employment/Business Opportunities; Escrow Services Fraud; Identity Theft; Internet Extortion; Investment Fraud; Lotteries; Letter or "419"; Phishing/Spoofing; Ponzi/Pyramid; Reshipping; Spam. Eric Conrad [9], discusses other means of defrauding people.

3.13. Phoning Journal

The latest invention of the fraudster is the introduction of phoning or in some cases non existing journal on internet and requesting the non-suspecting authors to pay some money for publication. If he pays he may be requested for further payment until they are satisfied he would not cooperate with them again.

3.14. Cash the Cheque System

Cheques still account for billions of payments each year, making them a prime target for criminals. Cheque fraud commission can be described as cheque that is being counterfeited, forged and altered. In cheque counterfeit, defrauders negotiate large purchases with the victim and agree to an advance payment via bank wire transfer. After ordering, the fraudster claims that paying via wire transfer is impractical, and instead sends a counterfeit cheque drawn on the account of a real, uninvolved organization as an alternate payment. After the cheque clears, the victim's company ships the goods. When the uninvolved organization notices the fraudulent transaction against their account, they request a charge back, resulting in the victim losing both the money and the goods. In some cases, defrauders learn the address of a merchant's bank, and send counterfeit cheques directly to the bank. They then claim a direct deposit was made after the cheque is deposited by bank staff, hoping the victim will only notice the apparently available funds, and not the fact that it was a cheque deposit that the bank has not yet fully cleared [10].

3.15. Purchase Fraud

This is a kind of fraud that occurs when a criminal approaches a merchant and proposes a business transaction, and then uses fraudulent means to pay for it, such as a stolen or fake credit card. As a result, merchants do not get paid for the sale.

Merchants who accept credit cards may receive a chargeback for the transaction and lose money as a result [10].

3.16. Trojan Horse Scheme

The Trojan horse scheme is based on embedding a computer virus type of software program onto the customer's PC. Trojans often tie themselves into the keyboard driver and record keystrokes. Once a Trojan detects that the customer opens an online banking website, it captures login name and password, and sends it to the criminal. In the year 2004, banks experienced a sharp rise in Trojan fraud scheme attacks [11].

3.17. PayPal Fraud

In a collection in person PayPal scheme, the scammer targets eBay auctions that allow the purchaser to personally collect the item from the seller, rather than having the item shipped, and where the seller accepts PayPal as a means of payment.

The fraudster uses a fake address with a post office box when making their bids, as PayPal will allow such an unconfirmed address. Such transactions are not covered by PayPal's seller protection policy. The fraudster buys the item, pays for it via PayPal, and then collects the item from the victim. The fraudster then challenges the sale, claiming a refund from PayPal and stating that they did not receive the item. PayPal's policy is that it will reverse a purchase transaction unless the seller can provide a shipment tracking number as proof of delivery; PayPal will not accept video evidence, a signed document, or any form of proof other than a tracking number as valid proof of delivery [10]. This form of fraud can be avoided by only accepting cash from buyers who wish to collect the goods in person.

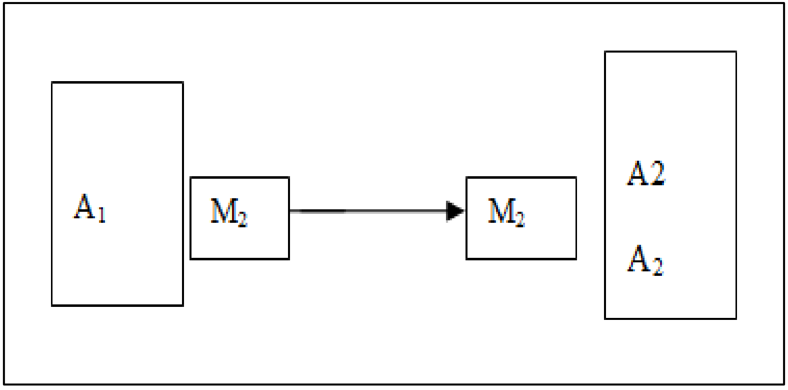
4. Security Issues

Funds could be transferred electronically through private and cooperate financial networks [12]. In terms of security, private network is more secured than financial networks. More protocols are observed when transmitting over corporate network. Also the network is not vulnerable to attack as in the case of open network. Even within the open network such as internet, there is considerable number of security layers involved with some layers more secured than others. The only difference here is that the more secured a site is the more the cost. Furthermore, for any payment system to be considered worthwhile it must exhibit the following properties:

4.1. Integrity

Integrity here means the system should be resilient to crypto-attack or various forms of attack. As depicted in fig 1, when a message A1 is transmitted from a point A1 to a point A2 there must be 100% assurance that the data received at point A2 is the same as the data sent at point A1without any modification.

Fig-1. Message routed without modification or compromise



4.2. Authorization

There must be a way to authenticate that it is the actual owner of the account that is authorizing the payment. This is normally done through the use of password and secret pin. The message could be authenticated using digital signature.

Digital signature was introduced by Diffie and Hellman [13]. Digital signature is a public key algorithm that allows message authentication by means of a piece of information referred to as signature. The algorithm generates the signature using public key that only personal private key could digitally sign [14].

4.3. Availability

This is a feature which makes the system always available. Subscribers to the payment system must have access to his money irrespective of the day and time of the week.

4.4. Reliability

The system must be reliable. This necessarily implies that charges should not be entered against the subscriber in the event of network failure. Also, no error encountered by the system must have any noticeable adverse effect on the subscriber.

4.5. Confidentiality

There must be a reasonable degree of secrecy in the transactions made by the subscribers. The transaction should not be disclosed without the express permission of the subscriber. This is usually made in form of agreement by the parties involved at the onset of the transaction.

4.6. Accountability

This is the ability of the system to be accountable for all the transactions that go on within the system. This is arbitrarily done by the system making receipt for transaction that goes on within the system.

4.7. Non Repudiation

This is the ability of the system to provide a tool for confirming that the original account owner is truly responsible for the transaction. Digital signature described in Camenisch, *et al.* [14] could be used to provide non-repudiation.

5. Encryption and Cryptography

Encryption and Cryptography have become standard methods of securing a network against all sorts of security threats. Typically, all the characteristics described above vis-à-vis: integrity, authorization, reliability, confidentiality and non-repudiation can be obtained by using cryptography. Since at present there is no way the system could detect whether the real owner is the one using the PIN code provided for the original account owner when transacting business on internet or via other networking systems thus allowing forgery of fraudulent use of account on the network. This work therefore provides a lead way by introducing a prototyped design/system with means of acknowledging receipt of transaction before the transaction is finally committed (accepted as authentic).

The conventional way of authentication is to provide a matching module in a program, which uses various encryption/decryption algorithms [15] for verification. It may also use just a simple pin code matching from the original code provided in the database. But this simple matching of code lacks the security and complexities required in real commercial payment system particularly in this era of sophistication in fraudsters.

The work does not seek to elaborate on the existing matching algorithm or methods used by the present system. What we are interested in is in exploiting a way of verifying or otherwise authenticating the identity of the person carrying out a virtual transaction on a particular account.

When the transaction is initiated at the client side, the authentication server authenticates the veracity of the client claim i.e. the ownership of the transaction. This is confirmed using the authority code at the server side (Authentication Server). Another thing to note here is the issue arising from transaction in varying what happens when the verifying medium (e.g. handset, email browser) is illegally accessed by the imposer. As shown in fig. 2, the design incorporates the idea of verification before the transaction is accepted. The user usually initiates the transaction. The transaction TS1 terminates at the Authentication server of the transaction service provider X1. The service provider, apart from the normal authentication, introduces a third party component server X2 otherwise called verification server to verify the authenticity of the transaction.

The user A1 initiates the transaction (TS1). The transaction (TS1) terminates at the main server (X1). On receiving the request for transaction at (X1) the transaction subsystem requests the authentication server X2 to authenticate the signature of A1. If the signature verification succeeds then TS1 is sent to transaction verification server X3 for verification. Otherwise the request for the transaction is out rightly rejected.

At X3, TS1 Is sent back to the user at X4 who is the legitimate owner of the credit facility for confirmation or for possible rejection of the transaction before it is committed. X4 may however be GSM or Computer console where the legitimate owner of the card resides. If X4 rejects the transaction, X2 is immediately notified for immediate contact with A1. The beauty of the architecture here is that each time the credit facility is in use, the legitimate owner is notified.

Fig-2. Response Triggered Architecture for E-Payment Transaction

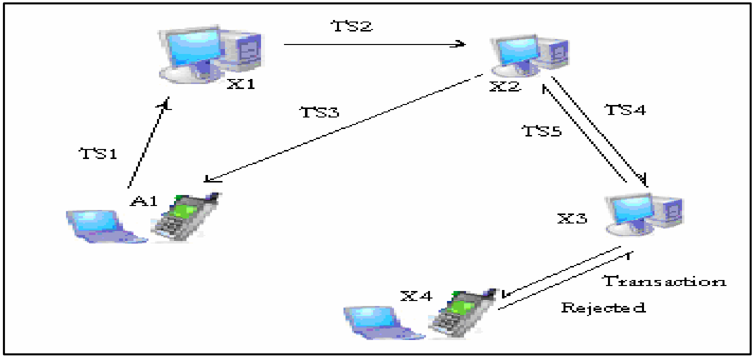
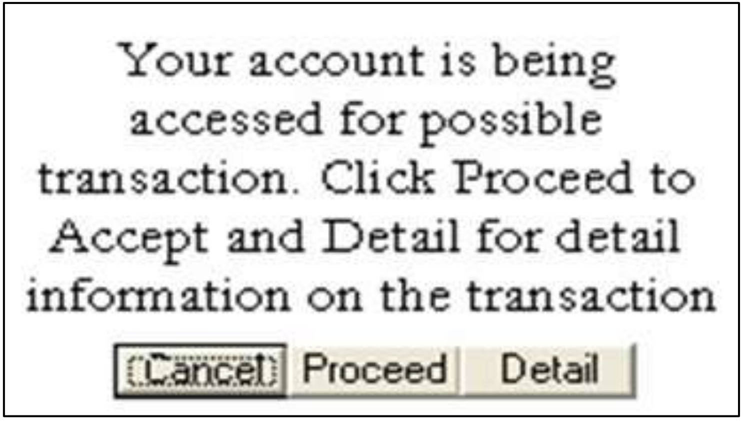


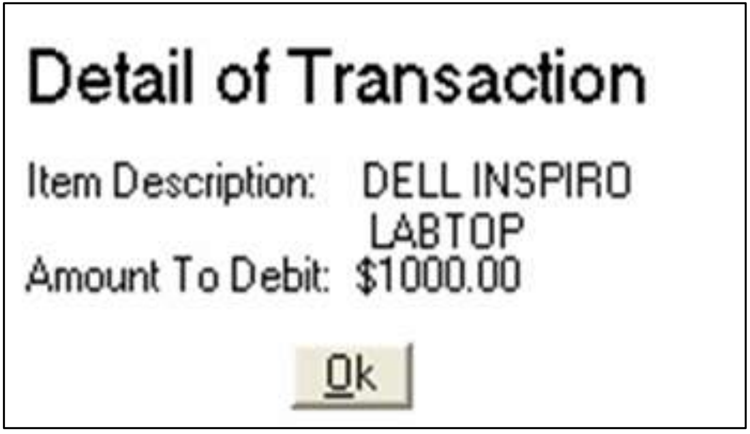
Fig. 3 depicts the simulated interface of the activities that occur on X4 that requires the response of the credit card owner of the initiated transaction whether to accept or decline the transaction. Fig. 4 depicts the detailed information of the type of transaction initiated for commission.

Fig-3. Simulated Activities that go on X4



Your account is being accessed for possible transaction. Click Proceed to Accept and Detail for detail information on the transaction

Fig-4. Detailed information of the transaction



Detail of Transaction

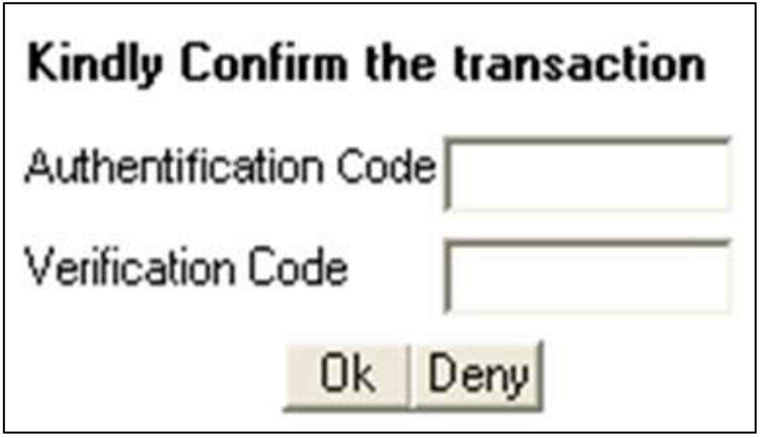
Item Description: DELL INSPIRO LABTOP

Amount To Debit: $1000.00

The legitimate owner of the card is requested to either repudiate or reject the operation. If operation is accepted, the transaction is continued; otherwise the transaction is immediately terminated.

The implementation of this is done by assigning different authentication codes as well as verification code. By doing this, it is very unlikely that the imposer could get both the authentication as well as the verification code. In the event that the transaction passed the authentication and verification test, fig. 5 represents the simulated output as received from the subscriber handset or e-mail box.

Fig-5. Simulated Interfaces for Subscriber Verification



Kindly Confirm the transaction

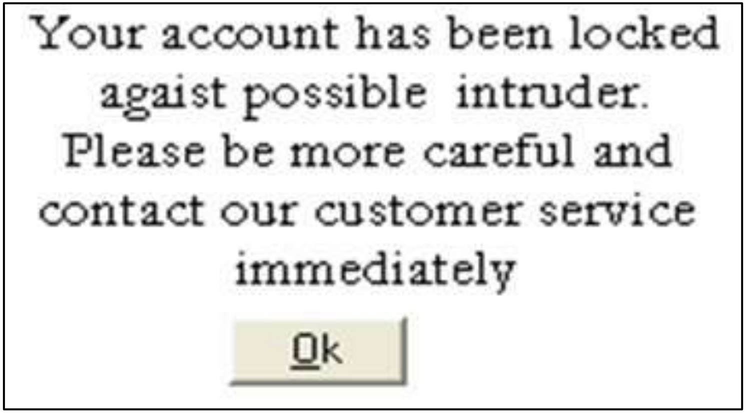
Authentification Code

Verification Code

In fig. 5, the subscriber is prompted to enter his authentication code as well as the verification code before the transaction can continue. If wrong pin code is supplied in the specified number of times, the account is blocked. The user would therefore be made to supply certain agreed information before the account is reopened.

In fig. 6, if the test at the verification server fails, then the user is immediately alerted that an attempt is being made on the user account and call for more security measure on the part of the subscriber. Fig. 6 shows a typical result on the subscriber handset. If the transaction is denied, the following information is sent to the legitimate owner of the account.

Fig-6. Simulated message Alert of Suspicious Transaction



Your account has been locked agaist possible intruder. Please be more careful and contact our customer service immediately

6. Conclusions

In this work we have proposed the use of Response Triggered Architecture against the backdrop of recent surge in cyber crime in the emerging economy. The simple Architecture takes care of the various misrepresentations on internet concerning the cloning of pin code by the internet fraud star popularly called “Yahoo Boys/Girls” in Nigeria.

It is expected that when the architecture is fully implemented, it would offer hope to thousands of people who are defrauded daily on internet. Also, it would restore people’s confidence in e-transaction and maintain a leveled playing ground for both developing and developed economy when it comes to implementing e-business.

References

[1] Normal, A. H. and John, S., 1981. *Glossary of marketing terms*. 2nd ed. William Heineman Ltd.

[2] Amos, E., 2013. "Smart content for smart people." In *Seminar organised by the Association of Information Technology and Telecommunications’ ICT cluster World Summit Award (WSA) in Austria.*

[3] The Freeman Institute, 2006. "Nigerian frauds 419 scam central." Available: www.419scams.com

[4] 10 Years of GSM Mobile in Nigeria, 2013. Available: http://www.naijatechguide.com/2011/08/10-years-of-gsm-mobile-in-nigeria.html

[5] Nigeria - The 419 Coalition Website. "The Nigerian scam (419 advance fee fraud) defined." Available: http://home.rica.net/alphae/419coal/

[6] Margaret Rouse Electronic Funds Transfer (EFT), 2014. Available: http://searchwindowsserver.techtarget.com/definition/Electronic-Funds-Transfer-EFT

[7] Comptroller’s Handbook, 1990. "Payment systems and funds transfer activities." Available: http://www.occ.gov/publications/publications-by-type/comptrollers-handbook/paymentsys1/.pdf

[8] Russell, G. S., 2000. *Electronic fraud, Australian society of certified practicing accountants (cpa) congress*. Sydney Hilton Hotel, pp. 1-19.

[9] Eric Conrad, 2013. "Types of cryptographic attacks." Available: http://www.giac.org/cissp-papers/57.pdf

[10] Wikipedia, 2010. "Internet Fraud." Available: http://en.wikipedia.org/wiki/Internet_fraud

[11] Institute for Operation Research Management GmbH (INFORM), 2013. "How can a bank prevent online banking fraud?" Available: www.inform-software.com/products/riskshield

[12] Prince Ogbenekaro, A. and Enoch, O. N. "Current state of electronic swift credit card payment system." Available: http://www.scamdex.com/HYPMAIL/0701/12868.php

[13] Diffie, W. and Hellman, M., 1976. "New directions in cryptography." *IEEE Trans. Info. Theory*, pp. 644-654.

[14] Camenisch, J. L., Pivetean, J.-M., and Stadler, M. A., 1994. "Security in payment systems." In *Processing of ESORICS "94.*

[15] Alese, B. K., 2000. *Vulnerability analysis of computer network security system*. M.Tech Thesis, Federal University of Technology, Akure, Nigeria.