The International Journal Of Engineering And Science (IJES)
||Volume|| 2 ||Issue|| 10 ||Pages|| 43-50 ||2013||
ISSN (e): 2319 – 1813 ISSN (p): 2319 – 1805

Synthetic Software Method: Panacea for Combating Internet Fraud in Nigeria

A.P. BINITIE
Department of Computer Science Education, Federal College of Education (Technical) Asaba, Delta State

N.V. BLAMAH
Department of Computer Science, University of Jos, Jos, Nigeria

U. S. OGAH
MIS Department Federal Polytechnic Mubi, Adamawa State

----------ABSTRACT----------

Internet fraud is a growing problem in many countries of the world today including Nigeria. There are many criminals who will try to rob you off your hard earned money by using the internet to access your financial information. E-payment using Credit card remains prevalent among other E-payment systems. It affects the cardholder, issuing bank and merchant. Credit card fraud is something that can never be completely eliminated, but rather something that must be managed. Nigeria with its vision 202020 will likely grow with credit card fraud, hence the need to be prepared to fight them today and when it will become the order of the day. Many developed countries like UK, US and many others have lost a lot at this. This paper proposes an authentication mechanism that will help in reducing internet fraud especially via credit cards (Master card and Visa card) to barest minimum. This paper also discusses the effect of credit card fraud on cardholder, issuing bank and merchants.

Keywords - Acquiring bank, Authentication mechanism, Cardholder, Issuing bank, Merchant.

Date of Submission: 03th, October, 2013 ⟺ Date of Acceptance: 30th, October, 2013

I. INTRODUCTION

There are several issues associated with online credit card use. Chief among them is fraud, which is perpetrated by both individuals and merchants. Another problem is the lack of security that can lead to the compromise of credit card numbers stored in online databases [1]. Authentication is a fundamental aspect of system security [2]. Merchants must develop a delicate balance between using safeguards to prevent fraud and not creating too many hoops for customers to jump through. Protecting transaction data and cardholder information has been the main driver for the launch of smart cards based on the EMV standard around the world [3]. Transactions using plastic cards have become more popular with the introduction of internet- based shopping and banking. According to statistics from the International Telecommunications Union (ITU), Nigeria has 45 million internet users, the highest online population in Africa. Internet Service Providers (ISP's) in the country are now demanding identity verification information from their customers, following the rising trend of online fraud in the global cyberspace, including Nigeria, and the need to comply with regulations, as well as deepen customer relationship [4].

As a result of fraudulent activities using individuals credit card information, many consumers are now scared of online transactions. More secure and convenient payment options would drive additional digital purchases for a majority of consumers [5]. New survey of security in Indian banks has revealed that many of them do not follow even basic measures to ensure card security or protect your personal information [6]. Payment card Industry (PCI), data security standard (DSS) and the data security requirements defined in the standard are necessary to address the ongoing security issues, especially those pertaining to payment card data handling [7]. While strong internal controls and audit procedures play a role in preventing and detecting fraud, it is unrealistic to assume that they are completely effective. For many, there remains a strong likelihood that a significant number of frauds are simply never detected. Even when frauds do come to light, many detection methods, such as audit procedures, only occur sometime after the fraud has taken place. Some of the manual checks used in preventing frauds are far from being perfect. The longer frauds go undetected, the larger the financial loss is likely to be and the smaller the chance of recovering the funds or assets from the perpetrator. Fraudsters seek out organizational "soft spots" where there is little regular cross-system data validation .They provide a golden opportunity for frauds to continue undetected.

Credit card is most popular method of payments. Every day, there are new online shoppers, new online retailers and more ecommerce. Online fraud increases partly because there is a lot more online commerce and partly because new online consumers and retailers are still working out how to stay safe online [8].

As Nigeria is gradually going cashless, credit card usage is increasing rapidly. This is because of its easiness in online payments and the feature "buy now pay later" [9].

1.2 Problem

Fraudsters develop various means of robbing people off their hard earned money. Hence the need to develop an authentication mechanism that can beat them.

1.3 Purpose of the Paper

The purpose of this paper is to study,

- Impact of credit card fraud on card holders, merchants, issuers,
- The existing fraud detection and authentication systems,
- Propose an authentication mechanism to counter credit card fraud.

II. SECURITY CODE

Credit card security code is one the information needed to authenticate online transactions. It is important to secure our security code since it is a safety feature, just like PIN number. You can only provide it during online transaction when the connection is secure. Never provide it through E-mail, since it is unsecure connection [10]. As long as someone has your card number, security code and card expiration, it will appear to the merchant that he is the right owner. The location of the security code on a card depends on the type of card. For cards like Visa, Master or Discover, it is the last three digits of the series of digits on the signature box, located at the back of the card. From the Visa card displayed below, the circled number, 123 is the security code.

Figure 1, security on a Visa Card

III. RELATED WORK

The technology for detecting credit card frauds is advancing at a rapid pace. This has attracted much researchers attention recently due to increase in credit card fraud. Some of the popular techniques employed by Issuing and Acquiring banks these days are; rule based systems, neural networks, data mining, grid based hidden Markov Model, etc.

Protecting transaction data and cardholder information has been the main driver in introducing smart cards worldwide and for the adoption of the EMV standard. Data authentication in EMV checks whether the card is genuine using the Card Authentication Methods (CAM) supported by the chip, all of which rely on public key cryptography. EMV has dramatically reduced fraud where it has been deployed, but counterfeiting is still a risk. [11]

Sequence of operations in credit card transaction processing was modeled by [12] using a Hidden Markov Model (HMM) and show how it can be used for the detection of frauds. It is able to detect frauds by considering a cardholder's spending habit. They model a credit card transaction processing sequence by the stochastic process of an HMM. An HMM is initially trained with the normal behavior of a cardholder. If an incoming credit card transaction is not accepted by the trained HMM with sufficiently high probability, it is considered to be fraudulent. Various authentication mechanisms were considered by [13], bringing out the pros and cons of each. Two factor authentications can also be implemented using mobile phones.

An approach involves using a mobile phone as a onetime password generation with an SMS-based mechanism which serves as a backup mechanism for retrieving the password and as a possible means of synchronization [14]. Snap2Pass and snap2Pay are two consumer friendly techniques that leverage a mobile phone to improve the security of web logins and web payments on a PC [15]

Recently [9] proposed an authentication mechanism using Grid codes. In this approach each credit card is associated with a Grid Card. Without the Grid Card, no one can do the online payments. An approach that involves advanced data mining techniques and neural network algorithms to obtain high fraud coverage has been developed by [16]. Parallel granular neural networks (PGNNs) was used by [17] for improving the speed of data mining and knowledge discovery process in credit card fraud detection. A complete system has been implemented for this purpose.

Credit card fraud detection with a neural network proposed by [18] was trained on a large sample of labeled credit card account transactions. These transactions contain samples of fraud cases due to lost cards, stolen cards, application fraud, counterfeit fraud, mail-order fraud, and non received issue (NRI) fraud. CARDWATCH as presented by [19] is a database mining system used for credit card fraud detection. The system, based on a neural learning module, provides an interface to a variety of commercial databases.

A game-theoretic approach to credit card fraud detection was proposed by [20]. They model the interaction between an attacker and fraud detection system as a multi stage game between two players, each trying to maximize his payoff.

Web services and data mining techniques were proposed by [21] to establish a collaborative scheme for fraud detection in the banking industry. With this scheme, participating banks share knowledge about the fraud patterns in a heterogeneous and distributed environment. To establish a smooth channel of data exchange, Web services techniques such as XML, SOAP, and WSDL are used. Meta-learning techniques could be used to learn models of fraudulent credit card transactions. Meta-learning is a general strategy that provides a means for combining and integrating a number of separately built classifiers or models. A meta-classifier is thus trained on the correlation of the predictions of the base classifiers [22]

Most of them are post methods which help to detect and then take the measures on the fraud that is occurred. Most approaches above require labeled data for both genuine, as well as fraudulent transactions, to train the classifiers. Getting real-world fraud data is one of the biggest problems associated with credit card fraud detection. Also, these approaches cannot detect new kinds of frauds for which labeled data is not available. These methods work based on the unusual patterns in payments. For Grid based system, which requires that every credit card have Grid card Inconveniences the user. Also if both the credit card and Grid card are lost then there is a chance for the credit card frauds. The proposed system will be more convenient for the user and above all will be able to detect and prevent fraud.

IV. IMPACT OF CREDIT CARD FRAUDS ON MERCHANT

Credit cards are the most frequently used payment method, online transactions [1]. Occurrences of credit card frauds have only shown an upward trend so far in Nigeria. The fraudulent activity on a card affects everybody, that is, the cardholder, the merchant (Website, retail store etc), the acquirer as well as the issuer. It is interesting to note that cardholders are the least impacted party due to fraud in credit card transactions. This is true for both card-present as well as card not-present scenarios. Merchants are the most affected party in a credit card fraud, particularly more in the card-not-present transactions, as they have to accept full liability for losses due to fraud, when you decide to accept electronic payment, business owners must also consider the potential cost of fraud.

Whenever a legitimate cardholder disputes a credit card charge, the card-issuing bank will send a chargeback to the merchant (through the acquirer), reversing the credit for the transaction. In case, the merchant does not have any physical evidence (e.g. delivery signature) available to challenge the cardholder's dispute, it is almost impossible to reverse the chargeback. Therefore, the merchant will have to completely absorb the cost of the fraudulent transaction. In fact, this cost consists of several components, which could add up to a significant amount. The cost of a fraudulent transaction on merchant consists of [23]:

1. Cost of goods sold: Since it is unlikely that the merchandise will be recovered in a case of fraud, the merchant will have to write off the value of goods involved in a fraudulent transaction. The impact of this loss will be highest for low-margin merchants.

2. Shipping cost: Since the shipping cost is usually bundled in the value of the order, the merchant will also need to absorb the cost of shipping for goods sold in a fraudulent transaction. Furthermore, fraudsters typically request high-priority shipping for their orders to enable rapid completion of the fraud, resulting in high shipping costs.

3. Card association fees: Visa and MasterCard have put in place fairly strict programs that penalize merchants generating excessive chargeback's. Typically, if a merchant exceeds established chargeback rates for any three-month period the merchant could be penalized with a fee for every chargeback. In extreme cases, the merchant's contract to accept cards could be terminated.

4. Merchant bank fees: In addition to the penalties charged by card associations, the merchant has to pay an additional processing fee to the acquiring bank for every chargeback.

5. Administrative cost: Every transaction that generates a chargeback requires significant administrative costs for the merchant. On average, each chargeback requires one to two hours to process. This is because processing a chargeback requires the merchant to receive and research the claim, contact the consumer, and respond to the acquiring bank or issuer with adequate documentation.

6. Loss of Reputation: Maintaining reputation and goodwill is very important for merchants as excessive chargeback and fraud monitoring could both drive cardholders away from transacting business with a merchant. Based on the scheme rules defined by both MasterCard and Visa, it is sometimes possible that the Issuer/Acquirer bears the costs of fraud. Even in cases when the Issuer/Acquirer is not bearing the direct cost of the fraud, there are some indirect costs that will finally be borne by them. Like in the case of chargeback issued to the merchant, there are administrative and manpower costs that the bank has to incur. The issuers and acquirers also have to make huge investments in preventing frauds by deploying sophisticated IT systems for detection of fraudulent transactions.

V. IMPACT OF FRAUD ON ISSUING BANKS/ ACQUIRERS

The issuers and acquirers also have to make huge investments in preventing frauds by deploying sophisticated IT systems for detection of fraudulent transactions. With all the negative impacts of fraudulent credit card activities, financial and product losses, fines, loss of reputation, etc, and technological advancements in perpetrating fraud, it is easy for merchants to feel victimized and helpless. According to once a transaction is proven to be indeed fraudulent, the bank will refund the original value to the card holder.

However, technological advancements in preventing fraud have started showing some promise to combat fraud. Merchants, Acquirers & Issuers are creating innovative solutions to bring down on fraudulent transactions and lower merchant chargeback rates. One of the main challenges with fraud prevention is the long time lag between the time a fraudulent transaction occurs and the time when it gets detected, that is, the cardholder initiates a chargeback [23]. Analysis shows that the average lag between the transaction date and the chargeback notification could be as high as 72 days. This means that, if no fraud prevention is in place, one or more fraudsters could easily generate significant damage to a business before the affected stakeholders even realize the problem [24].

VI. IMPACT OF CREDIT-CARD FRAUD ON CARDHOLDER

Credit card fraud is often an afterthought to consumers since their liability is limited, depending on their institution policy [23].This is true for both *card-present* as well as *card not- present* scenarios. EMV secures credit and debit card transactions by authenticating both the card and the customer presenting it through a combination of cryptographic authentication codes, digital signatures, and the entry of a PIN. Despite these, criminals can still use a genuine card to make a payment without knowing the card's PIN, and to remain undetected even when the merchant has an online connection to the banking network. The fraudster performs a man-in-the-middle attack to trick the terminal into believing the PIN verified correctly, while telling the card that no PIN was entered at all. Frequently, banks deny such fraud victims a refund, asserting that a card cannot be used without the correct PIN, and concluding that the customer must be grossly negligent or lying [25]. Many banks even have their own standards that limit the consumer's liability to a greater extent. They also have a cardholder protection policy in place that covers for most losses of the cardholder. The cardholder has to just report suspicious charges to the issuing bank, which in turn investigates the issue with the acquirer and merchant, and processes chargeback for the disputed amount. Customers should properly log off from their online browsing session.

VII. TRADITIONAL CREDIT CARD PROCESSING

Apart from technological advances, another trend which has emerged during the recent years is that fraud prevention is moving from back-office transaction processing systems to front-office authorization systems to prevent committing of potentially fraudulent transactions [26].

Below are traditional steps for credit card authentication

Step 1: The merchant submits a credit card transaction to authorize.net payment gateway on behalf of a customer via secure website connection, retail store, Moto center or wireless device.

Step 2: Authorize.net receives the secure transaction information and passes it via secure connection to the merchant banks processor.

Step 3: The merchant banks processor submits the transaction to the credit card Network (a system of financial entities that communicate to manage the processing, clearing, and settlement of credit card transactions).

Step 4: The credit card Network routes the transaction to the customer's credit card issuing bank.

Step 5: The customers issuing Banks approves or declines the transaction based on the customer's authentication credentials and available funds and passes the transaction results back to the credit card network.

Step 6: The credit card Network relays the transaction results to the merchant banks processor.

Step 7: The merchant banks processor relays the transaction results to Authorize.Net.

Step 8: Authorize.net stores the transaction results and sends them to the customers and/or merchant. This step completes the authorization process- all in few seconds.

Step 9: The customer's credit card issuing bank sends the appropriate funds for the transaction to the credit card Network, which passes the funds to the merchants Bank. The bank then deposits the funds into the merchant's bank account. This step is known as the settlement process and typically the transaction funds are deposited into your primary bank account within two to four business days.

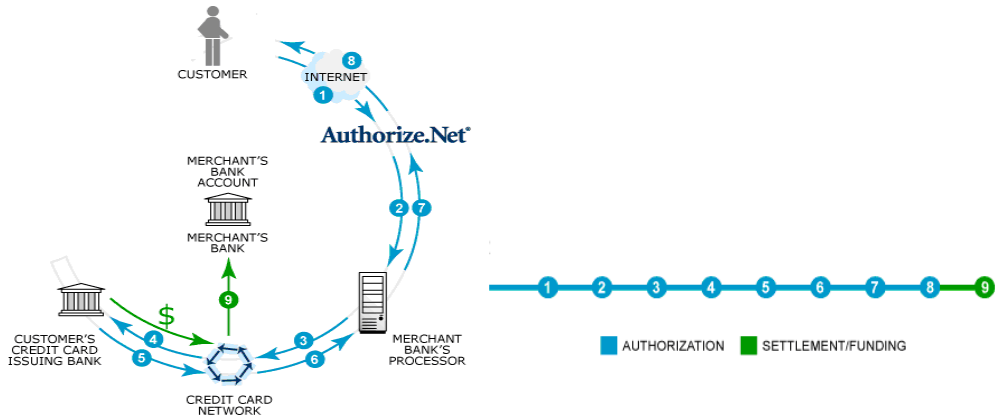

Figure 2, Traditional credit card processing [27].

7.1 Proposed Credit Card Authentication Mehanism

Step 1: The merchant submits a credit card transaction to authorize.net payment gateway on behalf of a customer via secure website connection, retail store, Moto center or wireless device.

Step 2: Authorize.net receives the secure transaction information and passes it via secure connection to the merchant banks processor.

Step 3: The merchant banks processor submits the transaction to the credit card Network (a system of financial entities that communicate to manage the processing, clearing, and settlement of credit card transactions).

Step 4: The credit card Network routes the transaction to the customer's credit card issuing bank.

Step 5: The customers issuing Banks sends an alert to the customer whose phone number matches the information provided. The customer will be prompted to key in 1 to accept or 0 to decline from his/her mobile phone.

Step 6: The customer's response is sent back to the customers' credit card issuing bank.

Step 7: If the customer accepts the transaction, the customer's credit card issuing bank approves the payment otherwise it declines and passes the transaction result back to the credit card Network.

Step 8: The credit card network relays the transaction results to the Merchant Banks Processor.

Step 9: The merchant Bank processor relays the transaction results to Authorize.net. (Payment gateway (a network node that allows you to gain entrance into a network and vice versa) to accept all online payment)

Step 10: Authorize.net stores the transaction results and sends them to the customer and/or the merchant. This step completes the authorization process- in just few seconds

Step 11: Once the customer is authenticated, the customer's credit card issuing bank sends the appropriate funds for the transaction to the merchant's bank. The bank then deposits the funds into the merchant's bank account. This step is also known as the settlement process and funds deposited into your primary bank account within two to four business day

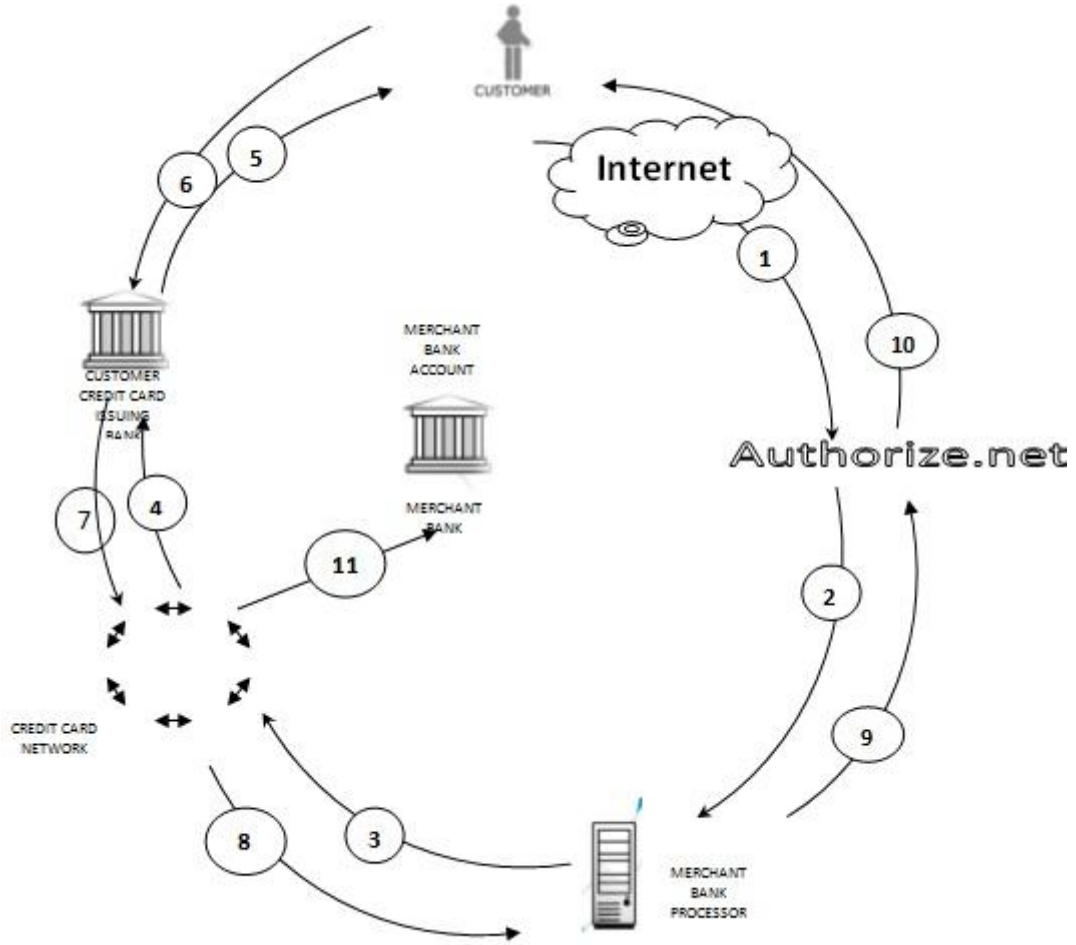

Figure 3, proposed authentication mechanism

To maximize its effectiveness as a fraud detection and Authentication system, the transactional analysis needs to work with a comprehensive set of indicators of potential fraud, taking into account the most common fraud schemes. Analyze all transactions within a given area and test them against the parameters that highlight indicators of fraud. Perform the analyses and tests as close to the time of the transaction as possible. Ideally, even before the transaction has been finalized, and preferably on a continuous monitoring basis, allow easy comparisons of data and transactions from separate business or operational systems, this last point is of particular relevance. Many suspicious transactions or patterns only come to light when transactional data from one system is compared to that of another.

VIII. LIMITATIONS

This system proposed, enhanced and revised the existing traditional credit card authentication mechanism. If the customer's mobile phone battery is not charged, then a genuine transaction will be cancelled. The process is slow, but if implemented will tackle credit card fraud.

IX. CONCLUSION

This paper presents an authentication mechanism which will help to reduce online credit card fraud. The system ensures that the user, the issuer/acquirer, the merchant are all involved. Though it might take a longer time depending on how fast the user responds to the SMS alert, it will go a long way in frustrating the efforts of internet fraudsters. The system proposed will detect and also prevent online credit card fraud. As Nigeria economy is gradually going cashless we need to get ourselves armed against internet fraudsters. Here comes the relief to the menace unleashed to many countries economy by these internet hoodlums.

X. RECOMMENDATION

Finding the optimally balanced measures outlined in this article useful will assist merchants, acquiring and issuing banks in combating frauds more efficiently. It is quite important to stress here that for the fight against credit card fraudsters to be successful, issuing banks need to work alongside merchants and customers. A well-designed and implemented software method, based on transactional analysis of operational systems, can significantly reduce the chances of frauds occurring and then remaining undetected. The sooner indicators of fraud are available, the greater potential to recover losses and address any control weaknesses. The timely detection of fraud directly impacts the bottom line, reducing losses for individuals and organization. Effective detection techniques serve as a deterrent to potential fraudsters.

REFERENCES

[1] U. Shankar, M. Walker, A Survey of Security in Online Credit Card Payments, *UC Berkeley Class Notes*, 2001.

[2] P. Jadhao, L. Dole, Implementation of Secure Authentication Scheme for Mobile Device, *International Journal of Emerging Science and Engineering*, 1(8), 2013, 2319–6378.

[3] B. Dodson, D. Sengupta, D. Boneh, M. S. Lam, Secure Consumer-Friendly Web Authentication and Payments with a Phone, *Proc. MobiCASE*, 2010, 17-38.

[4] O.O. Loveday, Nigeria Internet Fraud- Internet users now required to submit personal details to ISPs, *Sunnewsonline.net/news*, March 26, 2013.

[5] R. Dan (2011): Survey: 80% of consumers want alternative payment methods to credit cards online. *Readwrite.com.*

[7] L. Jing, S. Yang, Yang, C. Yang, S. Ozdemir, (2010): a survey of payment card industry data security standard, *IEEE Communication survey &Tutorials, 112(3).*

[8] H. Michelle, Social media Surge fuelling Credit Card scam: Report, *Financialnewsfocus.com/news*, June 23, 2011.

[9] S. Nayani, An approach for grid based authentication mechanism to counter cyber fraud with reference to credit car, *Global Journal of computer Science and technology, 11* (1) *1.0, 2011.*

[10] T. Bitler, How to Find your Credit Card Security Code, *CreditCards.com*, 2013

[11] D. C. Sharma, Banks not taking credit card data security seriously: Survey, *India, News - India Today*, February 8, 2011, updated 11:02 IST.

[12] S. Abhinav, K. Amlan, S. shamik, K.M. Arun, Credit Card Detection Using Hidden Markov Model, *IEEE Transactions on Dependable and secure Computing, 5*(1), 2008.

[13] C. Maryln, Authentication Mechanisms: which is best? *Global Information assurance certification paper*, 2002, *594.*

[14] F. Aloul, S. Zahidi, W. El-Hajj, Two factor authentication using mobile phones, *Proceeding of IEEE/ACS International Conference on Computer Systems and Applications*, ISBN: 978-1-4244-3807-5, 2009

[15] Smart Payment Association, Strengthening Card Authentication –A Migration to DDA, *Munich, Germany – The Smart Payment Association (SPA),* 4th February 2010

[16] R. Brause, T. Langsdorf, M. Hepp, Neural Data mining for Credit Card Fraud Detection, *Proc. IEEE Int'l Conf. Tools with Artificial Intelligence,* 1999, *pp. 103-106.*

[17] M. Syeda, Y.Q. Zhang, Y. Pan, Parallel Granular Network for Fast Credit Card Fraud detection, *Proc. IEEE Int'l conf. fuzzy Systems*, 2002, *pp. 572-577.*

[18] S. Ghosh, D.L. Reilly, Credit Card Fraud detection with a Neural-Network. *Proc. 27th Hawaii Int'l Conf. system sciences: Information systems: Decision Support and knowledge- based systems. Vol. 3*, 1994, *pp. 621-630.*

[19] E. Aleskerov, B. Freisleban, B. Rao, Cardwatch: A Neural Network based database mining system for credit Card Fraud Detection, *Proc. IEEE/IAFE: Computational Intelligence for Financial Eng.*, 1997, *pp. 220-226.*

[20] V. Vatsa, S. Sural, A.K. Majumdar, A Game- theoretic Approach to Credit Card Fraud Detection, *Proc. first Int'l conf. Information system security*, 2005, *pp. 263-276.*

[21] C. Chiu, C. Tsai, A Web services-Based collaborative scheme for credit card Fraud Detection. *Proc. IEEE Int'l conf. e-Technology, e-Commerce and e- service*, 2004, *pp. 177-181*

[22] S.J. Stolfo, D.W. Fan, W. Lee, A.L. Prodromidis, P.K. Chan, Credit Card Fraud Detection using Meta-Learning: Issues and Initial Results, *Proc. AAAI Workshop AI Methods in fraud and Risk Management*, 1997, *pp. 83-90.*

[23] P.B. Tej, P. Vikram, D. Amit, Understanding Credit card fraud, *Cards Business review*, 2003, www.popcer.org/problems/creditcardfraud/PDFs/Bhatla.pdf.

[24] C. Khyati, M. Bhawna, Credit card fraud Bang in E-commerce, *International Journal of Computational Engineering Research, (2)*3, 2012

[25] J. Murdoch, S. Drimer, R. Anderson, M. Bond, Chip and PIN is Broken, *IEEE Symposium on Security and Privacy*, 2010, *pp433-444.*

[26] S. Maguire, Identifying Risks during Information System Development: Managing the Process, *information-Technology-Risk-Management-Journal*, 2002.

[27] Credit card payment processing: A diagrammatic illustration, http://www.authorize.net/resources/how it works/111

BIOGRAPHY

Binitie Amaka

Patience is a lecturer with Federal College of Education Technical Asaba, Nigeria. She is a master student in the department of computer science at Adamawa State University, Mubi, Nigeria. She is a member of Nigeria Computer society. She obtained her Bsc in computer science in 2005 from Nnamdi Azikiwe University Awka, Nigeria. Her area of research interest is Social Networks and Artificial Intelligence.

Nachamada Vachaku Blamah

Is a Senior Lecturer with the University of Jos, Nigeria. He obtained his Bachelors of Technology, Master of Science, and Doctorate degrees in Computer Science. Dr. Blamah is a member of the IEEE Computational Intelligence Society and the Computer Professionals (Registration Council of Nigeria), and his research interests are mainly in the areas of computational intelligence and multi agent systems.

Ugbowu Stephen Ogah

Is a Lecturer with the Federal Polytechnic Mubi, Adamawa State. He obtained a PGD Computer Science at Adamawa State University and a B.sc (Ed.) Statistics/Computer Science of the Federal University of Agriculture Makurdi, Nigeria. He is a member Nigeria computer Society (NCS) and his research interests are in internet security and networking.