A Survey of Ecommerce Transaction Fraud Prevention Models

Akazue, M . I
Delta State University, Abraka,
Mathematics & Computer Science Department,
Delta State, Nigeria.
akazuem@gmail.com

ABSTRACT

Over the years, there has been an increasing interest in research efforts to develop customer-merchant trust models. Several types of these designed e-commerce fraud prevention models protects merchants, merchant stores and credit cards while defrauded customers uses established laws and policies to fight their cases. A survey of existing fraud prevention models was analyzed and component that checks merchant integrity within the transaction system was not present in the ecommerce models. The proposed system incorporates rule-based techniques and defined checks against fake virtual stores. Questionnaire was distributed to online customers about the acceptability of the new model. The analysis showed that the proposed Multi Authentication E-commerce (MAE) Model is acceptable by online customers. In future, the efficiency of the ecommerce proposed model will be demonstrated by developing and implementing MAE fraud prevention model. The quality of the proposed model will be measured using the data generated.

KEYWORDS

Fraud prevention, Central Merchant Registration Retrieval System (CMRRS), Local Merchant Registration System, Components, E-commerce

1 INTRODUCTION

Electronic commerce, otherwise known as e-commerce, is the act of doing business transactions over the Internet or similar communications technology [1]. In other words, e-commerce involves the buying, selling or exchange of goods, services, and information through electronic networks.

The initial widespread uptake of the Internet showed high expectations of Internet potential for e-commerce but, the lack of appropriate online payment mechanisms, consumer confidence in electronic payments and issues with the perceived security of payment mechanisms, explained the weak uptake of online shopping [2]. In other words, payment-related difficulties, products not appropriate, sellers are unknown, delivery is uncertain, were key explanation for consumers disinterest in e-commerce [3, 4]. Thus, this paper evaluated the existing merchant fraud prevention techniques with a view to exposing their flaws and proposed a Multi Authentication E-commerce (MAE) Model.

2 RELATED WORKS

2.1 Fraud Prevention Techniques

There are many types of merchant fraud such as merchant collusion fraud or triangulation fraud, Site/page cloning, and false merchant sites [5, 6, 7].

[6] proposed a proactive rule-based Fraud Management System (FMS) that uses layers of fraud protection to check credit card. The result showed that Chip and Pin is a better alternative than magnetic stripe.

[8] proposed a risk scoring system that is based on statistical models which use derived patterns from cardholder historical transactions as well as the current transaction attributes to identified

suspicious account activity. The scope was on checking Customer.

[9] proposed the use of intelligent agents in financial monitoring systems to effectively monitor financial transactions and detect and report any abnormal transactions. Their scope could not prevent abnormal transactions.

[5] elicited the security features used by the banks to protect transactions from fraudsters. Their work elicited four major processes that banks can mitigate the problems in credit card transactions. In their work, emphasis was on credit card.

[10] proposed an e-payment system that detects fraudulent transactions of Card-Not-Present (CNP) based on data mining techniques. They dealt with credit card

[11] proposed an authentication model for M-Commerce that reduce the requirement of computational resources for mobile terminals and provides security authentication, credit standing and session key for both the buyer and the seller to prevent large scale of identity theft. Their work was on identity theft.

[12] proposed an architecture that uses a Trusted Email mechanism to identify and authenticate the online customer, prevent unauthorized credit card transactions, and effectively resolve e-commerce dispute. Their work covered credit card fraud on soft-products

[13] proposed an e-fraud model of electronic fraud that allows the mechanics and context of e-fraud to be more fully understood. It took into account the various dimensions of e-fraud that is useful for practitioners in creating a comprehensive organizational view of the e-fraud phenomena. The scope was to understand the nature and extent of e-fraud, and identify the controls and mechanism.

[14] proposed a system which consisted of "predefined checks" that observes the attributes of fraudulent and non-fraudulent transactions and data was transmitted by using a pair of symmetric keys. It detected both fraudulent and non-fraudulent transactions when tested on a data set. Their scope of work was on Card Not Present scenarios

[15] proposed the use of distribution tracing within web content to identify counterfeiting source. It identified the activities of counterfeiting of popular transactional Web sites such as financial portals, stock-trading platforms and online retail sites. Scope was on Counterfeit websites.

[16] examined the security of business applications in a full electronic commerce environment It reduced risks and vulnerabilities that affect the overall operation of computer systems in e-commerce environment scope was on e-commerce environment

2.2 Survey of Trust Models in E-commerce

Table 1: Survey of Trust Models in E-commerce

Author	Technique Proposed	result	Scope
[17]	A hybrid trust management MAS model that allows agents to manage trust using a few combinations of different types of trust in different situations	It coped with the world's uncertainties by allowing agents to reason with different degrees of trust through the combination of objective, subjective and reputation based trust management.	Trust in world 's uncertainty
[18]	A trust model using fuzzy logic for the safe communication between source and destination node in wireless sensor network	It showed the trustworthy of sensor node to participate in sending and receiving data safely in the wireless network	Trust in safe communication

2.3 E-commerce Vulnerability Threats

[19] proposed a model for evaluating the vulnerabilities, threats and quality of B2C e-commerce Web sites using four main quality factors: security, privacy, design, and content. The proposed model when implemented offered a high precession of quality prediction.

[20] proposed a conceptual framework for an extended SOA model that allows for customer-

centric e-commerce. The extended SOA model inserts at the top of the typical SOA model two layers that introduce the customer logic for the composition of products and services into complete solutions that meet customer needs. Hence, the underlying business logic of a SOA is merged with the customer logic and business processes were associated with their outputs in terms of products and services.

3 PROBLEM FORMULATION

The E-commerce fraud prevention models should not just be to protect the virtual store, merchant goods, proffer solutions to card-not-present transactions, prevent identity theft and identify fake credit cards. It should also be able to identify online fake merchants. Thus, a survey of existing e-commerce models are carried out to ascertain if merchant integrity as regards merchant's physical location is made obvious to the customer.
Hence, a CMRR component, which will increase customer's trust and confidence online through the use of predefined checks to authenticate and distinguish fraudulent virtual stores, is presented and its acceptability is tested.

4 RESEARCH FRAMEWORK

4.1 Analysis of the Existing System

The general e-commerce components of existing model are designed using six components. These components are

1) Retail Service (RetS): the retail service entails the work of a retailer. In online transaction, a retailer owns a website where merchants and customers can transact business. In other words, it is an online market where merchants goods are stored and showcased for sale.

2) The Merchant Service (MS) is actually a bank or a payment service. It is a special account tied to a credit card processor that works with the customer's bank to help route payments into the sellers' bank account. Merchant services are provided by specialized companies called merchant service providers or independent sales organizations that offer payment processing.

3) The Switching Service (SwS) unifies the different banks together.

4) The Shipping Service(ShS) handles the delivery of goods to customers.

5) The Report Service (RepS) is responsible for generating shipping report and transaction report.

6) List Service (LS) is the component that handles customer's complaints.

The general e-commerce components of other model are shown in Figure 1.

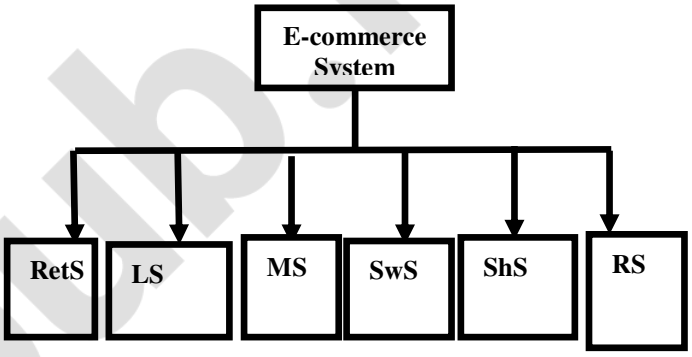

Figure 1: General E-commerce components of Other Model

In such a scenario, the verification of the merchant is unknown to the customer due to the absence of centralized merchant registration retrieval (CMRR) component. As a result, when problem arises and the customer complains to the list service, the merchant may not be found.

The interaction of the various components of other existing e-commerce transaction model is shown in Figure 2.

ISBN: 978-1-941968-05-5 ©2015 SDIWC

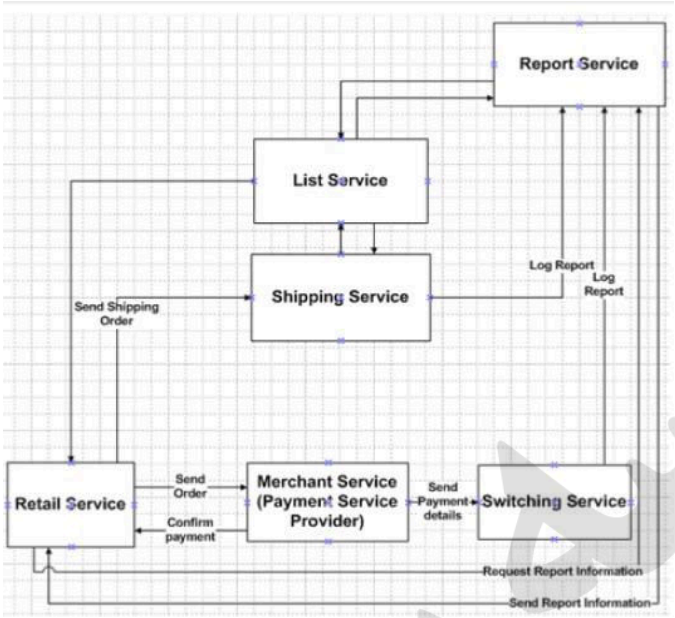

Figure 2 The other model for e-commerce fraud prevention

4.2 Analysis of the Proposed MAE Model

The seven system components of the MAE fraud prevention model is shown in Figure 3.

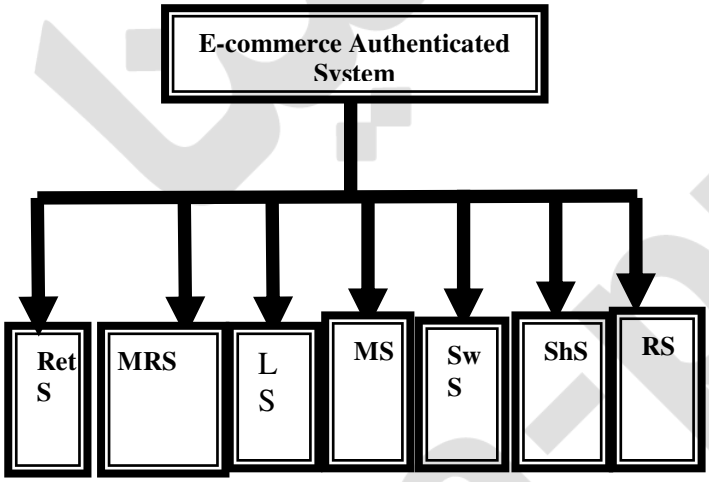

Figure 3 E-commerce components of MAE model

The Merchant Registration Service comprises of the Local merchant registration system (LMRS) and the Central Merchant Registration and Retrieval System (CMRRS). The LMRS component takes into account the registration of merchants' company's corporate office in the country where it is domiciled. In other words, the merchant, allowed by legislation, apply to the government for an independent organization to be created. The data or information filled by the merchant is physically inspected to affirm data authenticity by the country's Corporate Affairs Commission. After which, the merchant registered information is made available on the Internet. When LMRS registers a company, it is broadcasted to CMRRS. The CMRRS service provider centrally house Merchant information via referencing the LMRS. It is assumed that the CMRRS is handled by the internet community. In a nutshell, the Retail Service component retrieves merchant registration details via CMRRS.

The components interaction of the model is presented in Figure 4.

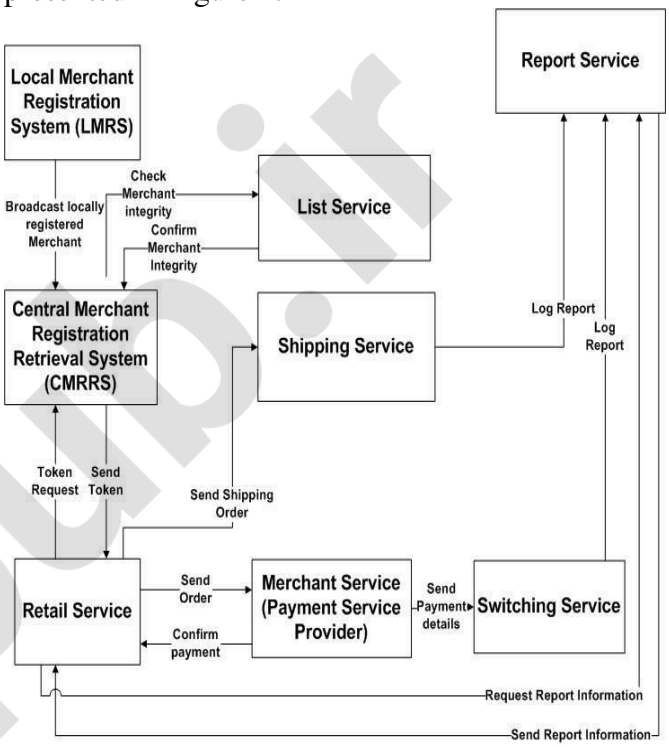

Figure 4 Architecture of the proposed Multi Authentication E-commerce (MAE) model for e-commerce fraud prevention using CMRR

4.3 Evaluating the Acceptability of the Proposed MAE Model

Questionnaire is used to elicit information about the acceptability of the incorporation of the CMRR component into the e-commerce model.

In other words, most questions were broad to give room to respondents to define situation.

The focus is on the acceptability of CMRR component in e-commerce system transaction. To test this acceptability, some online customers were administered a set of questionnaire consisting of two sections. Section "A" is based on other e-commerce transaction model and Section "B" is based on the acceptability of the CMRR component. The data of the users that responded was analyzed using frequency distribution and descriptive statistics.

The questionnaire used a five scale type to measure the CMRR component acceptability.

The respondents were asked to express their opinions on each question and each question was a 5-point Likert item from which respondents were to pick an option ranging from; Neutral, Strongly Agreed, Agreed, Disagree, Strongly disagreed.

The scaling of the options were done with scale of 0-4, where Neutral = 0, Strongly Agreed = 4, Agreed = 3, Disagree = 2, Strongly disagreed = Cronbach's alpha in SPSS was used to check for internal consistency of the scale used. The result showed a Cronbach's Alpha of 0.757 which is good.

From the generated result the acceptability of the CMRR component in the MAE model was compared with the general e-commerce models and the findings are tabulated in Table 2.

Table 2 A comparative study of CMRR acceptability in e-commerce model

Characteristic	Other e-commerce model	CMRR
In the ecommerce site, it is obvious that every merchant that showcase goods online are verified	No	Yes
In the ecommerce site, am able to identify fraudulent virtual stores	No	Yes
It is obvious in identifying Merchants that are registered with their corporate affair	No	Yes
In an ecommerce site that I visited, Information of every merchant that showcase goods online can be retrieved by me when problem arises	Not obvious to customer	Possible because of CMRR function
In ecommerce sites that I visited, an guided in the choice of merchant to patronize	No advisory sign to customer	Yes

The acceptability of the CMRR component into the general e-commerce model is shown by the average mean values of the respondents in Figure 5.

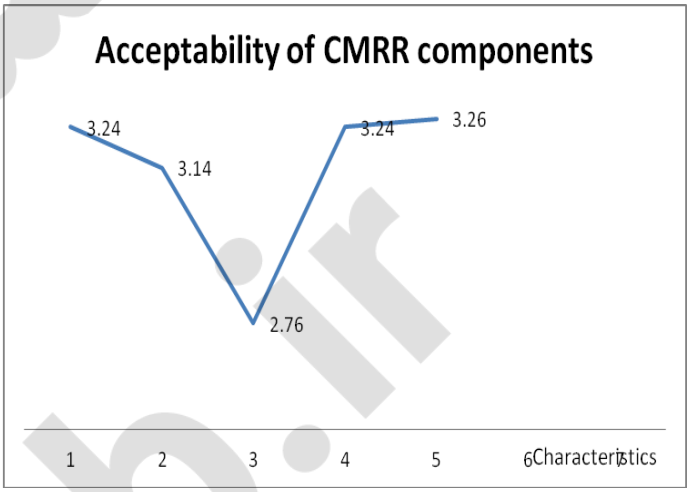

Figure 5 the acceptability of CMRR component into the E-commerce model

4.4 Implications of our Proposed CMRR component

- The proposed model has economic value since a customer receives advisory report to transact business with a merchant duly registered with their country's corporate affair. Thus, mitigating the fear of fake merchant online and enhancing customer trust.
- It will help the developing countries to have a database of all registered merchant and their physical location. The dodging of tax by merchants is reduced to a minimal.
- The ability to track the merchant will be possible when this model is implemented.
- The CMRR component has the ability to consistently check every merchant that showcase good(s) online. The authenticity of such merchants is shown to the customer by generating token in the merchant details. This is

an improvement on the previous e-commerce website.

• The CMRR component guides the customer against fraudulent merchants in the aspect of knowing the merchant physical locations which have not being the case with existing models.

6 DISCUSSION

In this paper, incorporating a CMRR component into existing e-commerce model is proposed because it will address the problem of fake web traders and to a great extent mitigate the problem of undelivered goods and services to customers since the merchant is traceable. Therefore, the proposed MAE model incorporated the seven components: Retail Services, Central Merchant Registration Retrieval Service (CMRRS), List Service, Merchant Service, Switching Service, Shipping service and Reporting service. The discussion of the components of the MAE model suggests that the model allows for the individual elements to be adequately considered in their own right. This invariably encourages the flow-on effects and relationships between elements to be considered. The model now needs to be implemented and tested in the field for both validity in describing the process of mitigating the problem of fake web traders and once the validity is established, its usefulness in enhancing customer online trust would be a reality.

Also this paper implicitly showed the acceptability of the CMRR component into the e-commerce model. The Figure 5 showed that the acceptability of CMRR component is not because the merchant is registered with their country corporate affairs but rather because every merchant that showcase goods online are verified and that the customer can use the CMRR to identify and distinguish fraudulent virtual stores from non-fraudulent virtual stores. Thus, when the good merchant decides to be bad, the customer can report to the Central List Service who will investigate and if the merchant defaulted, he will be blacklisted. When fraud is detected, legislative organization will ensure that customer's money is refunded by using the LMRS to trace the physical location of the merchant.

7.0 CONCLUSION

In this study, the incorporation of the CMRR component into the e-commerce transaction model has addressed the problem of fake web merchants and will invariably restore confidence to those individuals that are involved in e-commerce. Findings from this paper can be used for future research work in the area of trust in B2C e-commerce and to address further the importance of fraud prevention management on the Internet.

REFERENCES

[1] D. Morley and C. S. Parker, Understanding Computers: Today And Tomorrow Introductory, 12th Edition, Course Technology publishers, pp1-423, 2008. ISBN: 1423925203

[2] OECD/OCDE, "Report on Disclosure Issues related to the Use of Copy Control and Digital Rights Management Technologies", OECD, Paris, 2006. www.oecd.org/dataoecd/47/31/36546422.pdf. Accessed January 2010

[3] OECD, "OECD Conference on Empowering E-consumers: Strengthening Consumer Protection in the Internet Economy", Background Report, Washington D.C., 8-10 December 2009. DSTI/CP(2009)20/FINAL. Accessed January 2010

[4] Z. Zhongwei, "Improving Efficiency and Scalability of Service Network Graph", IEEE Transactions on Image Processing 15(5), pp. 1300-1312, 2006

[5] D. Jithendra, "Credit Card Security and E-payment, Enquiry into credit card fraud in E-Payment. Masters project", Luleå University of Technology. http://epubl.ltu.se/1653-0187/2006/23/LTU-PB-EX-0623-SE.pdf. pp. 2006. Accessed January 2012

[6] S. Dejan,"Reducing fraud in electronic payment systems", The 7th Balkan Conference on Operational Research, BACOR 05 Constanta, Romania, pp. 1-11. http://users.sch.gr/baloukas/papers/BACOR_2005.pdf. 2005. Accessed 25th January 2011

[7] K. Yufeng L. Chang-Tien, and S. Sirirat, "Survey of Fraud Detection Techniques in Networking, Sensing and Control", IEEE International Conference, 2, pp. 749 – 754, 2004. ISSN: 1810-7869

[8] A. Vikram, S. Chennuru, H. R. Rao, and S. Upadhyaya, "A Solution Architecture for Financial Institutions to Handle Illegal Activities: A Neural Networks Approach", IEEE Proceedings of the 37th

Hawaii International Conference on System Sciences, pp. 181 – 190, ISBN: 0-7695-2056-1, 2004 http://csdl.computer.org/comp/proceedings/hicss/2004/2056/07/205670181a.pdf. Accessed 15th May 2011

[9] H. Wang, J. Mylopoulos and S. Liao, "Intelligent agents and financial risk monitoring systems", Communications of the ACM, 45 (3), pp. 83-88, 2002.

[10] D. Micci-Barreca, "With Criminal Intent". Fraud International, 22, pp. 30-34, 2004.

[11] S. Mingqiu, H. Xiangpei, L. Jiahua, and D. Guishi, "An Authentication Model Involving Trusted Third Party for M-Commerce. ICMB '07 Proceedings of the International Conference on the Management of Mobile Business, pp. 53, 2007

[12] I. A. Saleh, T. S. Nien, and M. Dennis, "Using Trusted Email to Prevent Credit Card Frauds in Multimedia Products", World Wide Web 5 (2), pp. 245-262, 2002.

[13] P. Malakedsuwan, and K.J. Stevens, "A Model of E-Fraud", 7th Pacific Asia Conference on Information Systems, pp. 18-28, 2003. http://aisel.aisnet.org/pacis2003/2. Accessed 20th January 2010

[14] A. Rehab, B. Shiraz, S. Malik, K. Hayat, K. Aihab, and K. Memoona,. "online credit card fraud prevention system for developing countries", International Journal of Reviews in Computing, pp 62-70, 2010

[15] O. Gunter, "ANTI-FRAUD IMAGE SOLUTIONS: The use of distribution tracing within web content to identify counterfeiting sources", 2009. http://www.technicalinfo.net , Accessed 18th September, 2011

[16] W. Harsha, and K. Parwaiz, "A New Model for the E-Commerce Security", Proceedings of the Third Security Conference, April 14-15, 2004, Las Vegas, www.information-institute.org/security/3rdConf/Proceedings/8.pdf. accessed 18th 2011.

[17] K. Kanagaraj, and M. Muhammad, "A Hybrid Trust Management Model for MAS Based Trading Society" The International Arab Journal of Information Technology, 1(0), pp. 60-68, 2003

[18] K. K. Tae, and S. S. Hee, "A Trust Model using Fuzzy Logic in Wireless Sensor Network", World Academy of Science, Engineering and Technology 42, pp. 63-68, 2008.

[19] M. A. Radwan, and A. K. Mumtaz, "Business-to-consumer e-commerce Web Sites: Vulnerabilities, Threats and quality evaluation model", International Conference on Electronics, Communications, and Computers – CONIELECOMP , pp. 206 - 211 , 2010.

[20] F. Garyfallos, and T. Konstantinos, An Extended SOA Model for Customer-Centric E-Commerce, IEEE International Conference on e-Business Engineering – ICEBE , pp. 771-775, 2008.