Journal of Computer Science & Its Applications, 2004, Vol. 10 No. 1

A Framework for M-Commerce Implementation in Nigeria

Ayo, C. K., Olugbara, O. O., Ikhu-Omoregbe, N.A. and Atayero, A.A.
Department of Computer and Information Technology,
Covenant University
CanaanLand, Ota, Nigeria.
{ckayome@yahoo.com, olu_olugbara@yahoo.com, stnics@yahoo.com,
atayero@yahoo.com}

ABSTRACT

The Internet has brought about the concept of globalization, which has revolutionized the way business is transacted all over the world. The E-commerce is of particular interest, though widely used but still has some security challenges in terms of transparency and confidentiality of transactions. This paper focuses on M-commerce as an extension to E-commerce implementation with the Banking industry proposed as core implementation consideration in order to guarantee high level security. We have reviewed some cases of online frauds and discussed the emerging critical issues affecting software development of M-commerce applications. A framework for M-commerce implementation is therefore, proposed for countries such as Nigeria, Romania and Indonesia where cases of online scam are alarming.

KEYWORDS

M-commerce, M-payment, Telemarketing fraud and Security

1. INTRODUCTION

Mobile commerce (M-commerce) activities transcend major national boundaries as it is a global phenomenon. All countries of the world and major economic players are directly involved. Moving business online solves a number of problems such as: geographical fragmentation, inefficient labour and information interaction. The primary goal is that people who are scattered all over the world can do business with ease and at minimum cost using a combination of the old telephone/fax telecommunications system with the new Internet technology. This new direction of technology gave birth to what is referred to as M-commerce.

M-commerce [1,2,3,4], which is the process of conducting commercial transactions using mobile telecommunication networks, information communication systems and mobile devices promises to deliver electronic commerce capabilities directly to consumers anywhere, through the wireless technology. M-commerce is online financial transaction such as shipping of goods and services or electronic transfer of funds using the mobile device of the user. It can be used to connect to internet from any place, conduct online transactions, make purchases, trade stock, send e-mail, perform online enquiry, conduct market research, place advertisement and so on. The numerous application

areas of M-commerce include: M-Payment, M-Inventory management, M-Distance education, M-Workplace, M-Auction, M-Audit, M-Telemedicine, M-Advertisement, M-Audit, M-Agriculture, M-Police, M-Banking, M-Library, M-Shopping, M-Reservation, M-Government and so on.

In Nigeria, the number of users of the mobile communication devices is far more than the PC-based users. Hence, M-commerce appears more acceptable because of its availability and cost effectiveness coupled with the advent of telephone and Internet Banking in Nigeria, which can serve as backup. The greatest problem facing M-commerce is that of fraud, security and confidentiality with Nigeria being the greatest culprit. This has brought about the concept called "Nigeria scam" [5]. It has been observed that regardless of the country or countries involved in the frauds, even countries located outside Africa, the fraudsters are Nigerians [6]. There is evidence that while numerous organizations are implementing wireless technology applications, large commercial enterprises like Banks are skeptical of the level of security involved in this new technology.

Generally, there are a number of groups of consortium found to regulate the activities of both E/M-commerce. We have the World Wide Web consortium (W3C) [7] and the mobile payment forum [8] coming together to formulate policies regarding online transactions. M-commerce may only survive in an atmosphere of enhanced trust confidentiality and transparency.

Several articles have been published in literature on mobile computing and wireless technology, but very limited research on strategies for implementation of M-commerce applications. It is important to develop these areas while working on wireless technology advancements. The main contribution of this paper focuses on the fraud issue and strategy for its control. We propose that for successful M-commerce applications, Banks must be strongly considered at the core of M-commerce design architecture. This is necessary in order to guarantee high-level security and minimization of fraud rate that are serious threats to M-commerce implementation. The case study was directed at M-commerce implementation in Nigeria, which is one of the most populous black-race in the world with a large number of cellular phone subscribers than users of the Internet just like Europe, U.S. and Asia countries. Nigeria is also reported as having a large number of fraudsters along with Indonesia, Romania and some other countries. A secure M-commerce framework must consider these critical issues of security and fraud.

The contribution of this work is to solve the more severe problem of fraud using control-oriented framework that we have developed. The strategy for software implementation of this model is presented in form of a flowchart for easy comprehension. The rest of the paper is briefly summarized as follows. In section 2, we discuss some fears inherent in M-commerce implementation. Section 3 considers some important issues on M-payment, which is a strong requirement for M-commerce applications. Section 4 discusses quite a number of issues that are of paramount interest to the present work. Some fraud cases were reviewed and a framework that may be used to solve these problems is presented. The paper is concluded in section 5 with a brief note.

2. CONFIDENTIALITY, SECURITY AND FRAUD

Security is one of the core issues in M-commerce applications, because wireless devices, including cellular phone and personal digital assistants were not originally designed with security as a top priority [4]. Confidentiality (or privacy), which is the property with which information is not disclosed to unauthorized individual, entities or processes is one of the major goals of Wired Equivalent Privacy (WEP). Wireless network security countermeasures are based on the premise that network access is by restriction. M-commerce configuration requires a little different network model because large group of participants will access the network in order to participate in M-commerce transactions. M-commerce model therefore, should support open business activities with the major goal of maximizing profit.

The problems of network security are numerous and they vary from cases of theft, to physical damage, to data corruption and even to denial of service. A comprehensive list of surreptitious network security problems have been identified and reported by the National Institute of Standards and Technology (NIST) [9]. According to NIST report, security requirements are basically: Authentication, Non-repudiation and Accountability. Three classes of countermeasures that are available for securing wireless networks are management, operational and technical countermeasures. In general, security and trust transactions can be achieved with authentication and non-repudiation, integrity, confidentiality and message authentication. Techniques like the asymmetric cryptographic algorithms are used to achieve these results [9].

However, an important issue neglected in the previous works is that of online fraud. Security is not accurately synonymous to fraud. Security is a broader concept but fraud is a more severe problem to manage. Fraud in a system may not be due to insecurity but because of corruption and gross abuse of power by political leaders. Security challenges may be perfectly tackled by stringent rules and careful monitoring. But, fraud may be controlled using check and balance (i.e. auditing). Scammers gain access to network through passive eavesdropping, traffic flow analysis or active masquerading and replay. In most cases, fraudsters are either legal network users or people with well-established collaboration with the insider to perpetrate fraud.

The activities of fraudsters have been so alarming in Nigeria that the phrases: "Advance fee fraud", "419 fraud", "Four-one-nine" and "Plain old 419" became household after the relevant section of the criminal code of Nigeria. The stakes in security and fraud are becoming absolutely higher as burgeoning wireless technology and data services take new shape. New types of frauds are really extensions of the old ones. We now have telemarketing fraud (Tele-fraud), Mobile fraud (M-fraud), Mobile 419 (M-419) and so on. These are new dimensions of frauds that electronic and mobile communication technologies have brought.

The federal government of Nigeria has constituted a security agency called "Economic and Financial Crimes Commission (EFCC) to checkmate the activities of fraudsters. The commission must be aided by

appropriate working tools in order to be fully effective. In a similar effort, the 419 coalition website [5] was created to combat the Nigeria scam by educating the populace.

3. M-PAYMENT TRANSACTION

M-payment is another important issue of M-commerce applications. Mobile users pay for the mobile connection services and the acquired contents, services or goods received. Hence, they are concerned about payment procedures and whether payment transactions are secured, reliable and convenient enough or not.

Furthermore, a serious barrier to online transactions is lack of familiarity with items to procure. There is the need for consumers to physically see and thoroughly examine the items before procurement. The full perspective of an item cannot be gained online and this is in many ways restricting purchasing. However, there are many online transactions such as "mobile enquiry" and "mobile notification" that do not involve payment. This hindrance therefore, cannot diminish the good image of M-commerce. To help drive M-commerce, four leading European mobile phone companies: T-mobile, Orange, Vadafone and Telefonica movies have teamed up to establish the Mobile Payment Service Association that aims to create an interoperable standard for payments using a mobile phone [10]. The aim of the association is to provide a secure platform to drive more customers, content-providers, banks and merchants to stimulate M-commerce growth.

The E/M-payment systems currently in use are classified into three broad classes: Prepaid or cash-like payment systems (e.g. M-purses, Digital wallets and Certified checks), Pay-now or check-like payment systems (e.g. Smart cash card) and Pay-after, which is also a check-like payment system (e.g. Credit card). The challenge facing most payment protocols is lack of common acceptable standard. Within currently available electronic payment systems, payments are done electronically, but the mapping between the electronic payment and the transfer of real value is still guaranteed by Banks through financial clearing systems. These clearing systems are built on the closed network of financial institutions that are considered more secure than open network, such as the Internet [11]. Again, lack of standard is a debilitating factor because current electronic payment systems differ in details, but has the same purpose of facilitating the secure transfer of monetary value between parties involved in the transaction. Two acceptable M-commerce payment protocols used in the framework are the direct payment and operator billing methods.

4. CONTROL-ORIENTED M-COMMERCE FRAMEWORK

Security, fraud and payment procedure have been previously mentioned as the inherent fears in M-commence transaction patronage. The framework proposed in this paper aims at resolving the problems discussed. The model is built on third party involvement in M-commerce transactions and retailer directive requirements [10]: retailers should offer clear contact information, a fast acknowledgement of orders and the chance for customers to amend an order.

4.1. Case Study of Online Fraud

We present two cases of fraud perpetrated via online transactions using Internet, Mobile phone and Credit cards. For details of these stories and others refer to the reference materials [5,6,12].

Case 1: The Nigeria Scam [5]

The bait is the fictitious millions of dollars described in a letter. The goal is to get the victim come up with money for the expenses required to ship goods or money to him. The victim thinks a few thousands of dollars is trivial when compared to the transaction gain. Each demand for more money is claimed to be the very last obstacle before the big money or goods is released. Sometimes, the victims are lured to Nigeria, where even worse things happen.

Case 2: Credit Card Scam [6]

Somebody ordered for 14 sets of a Marci wheel from a seller. He sent three credit card numbers and asked the seller to split the charge amongst the three cards. At the peak of the transaction the buyer was suspected to be playing funny. During this course of transaction, more cards were requested for by the seller due to some difficulties in getting through. Funny enough, the numbers on the cards were observed to have similar pattern and it was discovered that all the cards were not his and of course the buyer was a scammer.

4.2. Conducting M-Payment

Credit card method of payment carries a high risk as scammers have neat ways of using cards that are not theirs. There are also the problems of expiry dates with operators to avoid tapping into the details of the cards. This is not encouraging on the part of the retailers and buyers. Finally, with time, techniques for faking credit and debit cards would be common and this will jeopardize the reputation of M-commerce. Two methods of conducting M-Payment appear to be more practical. These methods are Direct Payment and Operator billing. The second payment method is clearly described below [11]:

a.) Vendor has an agreement with WSP or consortium of providers

b.) Consumer initiates transaction with vendor

c.) Consumer receives service or product

d.) WSP pays vendor

e.) Consumer receives a bill form WSP

4.3. Conducting M-commerce Transactions

For small-scale transactions, the operator billing method of payment is in order. However, for a more capital-intensive transaction this method needs to be improved upon. We suggest the involvement of third party such as Law Enforcement Agents, Authorized Agents, Financial Institutions and trusted Wireless Service Providers (WSPs) to monitor and control transactions. The control-oriented framework proposed here is based on this approach. There is a direct involvement of customer, merchant and their Banks, another third party acquirer or issuer. The acquirer gathers and stores useful information concerning merchants, customers, and cases of previous history of frauds and uses this information to control, monitor and guide transactions between parties. The acquirer can terminate and inform the concerned parties in case of suspected fake or insidious

transaction. The transaction between the initiator and the initiator's Bank may not be guided by the acquirer but transaction involving different parties is to be monitored by the acquirer. The model is to be implemented as a software application on wireless platform with the following characteristics. The operation of the acquirer is transparent to the parties involved in the transaction and the control algorithm should be "light-weight" to guarantee efficiency. The model is pretty simple and alleviates many fraud problems anticipated in M-commerce applications. The complete description of the model is given by the flowchart that appears in appendix 1.

4.4 Software Implementation Consideration

M-commerce applications combine the advantages of mobile communications with existing E-commerce services but operate partially in an environment different from E-commerce, which is usually conducted in fixed Internet. The challenges of M-commerce are mainly induced by the characteristics of wireless communications, device constraints, mobility, security and human behavior [4]. There are several solutions such as Wireless Application Protocol (WAP), Java 2 Micro Edition (J2ME), I-mode and Binary Runtime Environment for Wireless (BREW) currently available for developing M-commerce applications. A number of factors must be considered in developing M-commerce applications. See appendix 2 for the list of these useful considerations.

5. CONCLUSION

This paper analyzed and described a conceptual framework for monitoring and controlling cases of M-commerce frauds. The implementation of M-commerce model to control fraud in Nigeria the acclaimed giant of Africa with a population of over 120 million definitely has lot of economic, social and political gains. Hence, control-oriented M-commerce framework is proposed to solve the problem of telemarketing fraud. We are currently working on developing a prototype-software that implements the strategy utilizing technologies such as teleconferencing, mobile XML, Mobile SOAP, Data mining techniques and application of mobile agents. This work is currently under development at Covenant University.

REFERENCES

1. Barnes, S. (2002), the mobile commerce value chain: analysis and future developments. Int. journal of information management, 12, pp. 91-108

2. Elsevier (2003), special issue on mobile commerce: strategies, technologies and applications. Decision support systems, 35, pp. 187-188

3. Jukic, N., Sharma, A., Jukic, B. and Parameswaran, M., M-commerce: analysis of impact on marketing operation. http://www.sba.inc.edu/research/wpapers/011020.pdf

4. Leung, K. (2002), M-commerce applications: emerging issues. http://www.cs.ust.hk/~scc/csit510/assignment/kelvin.pdf

5. Sierp, G., Nigria-the 419 coalition website. http://www.potifos.com/fraud

6. White, P.J. (2003), credit card scams. http://www.peterwhitecycles.com/scams.htm

7. Daly, J., Forgue, M.E. and Tachenchi, S. (2002), world wide web consortium issues. http://www.w3.org

8. Mobile payment forum inc., mobile payment forum white. http://ww.mobilepaymentforum.org/pdfs/mpf_whitepaper.pdf

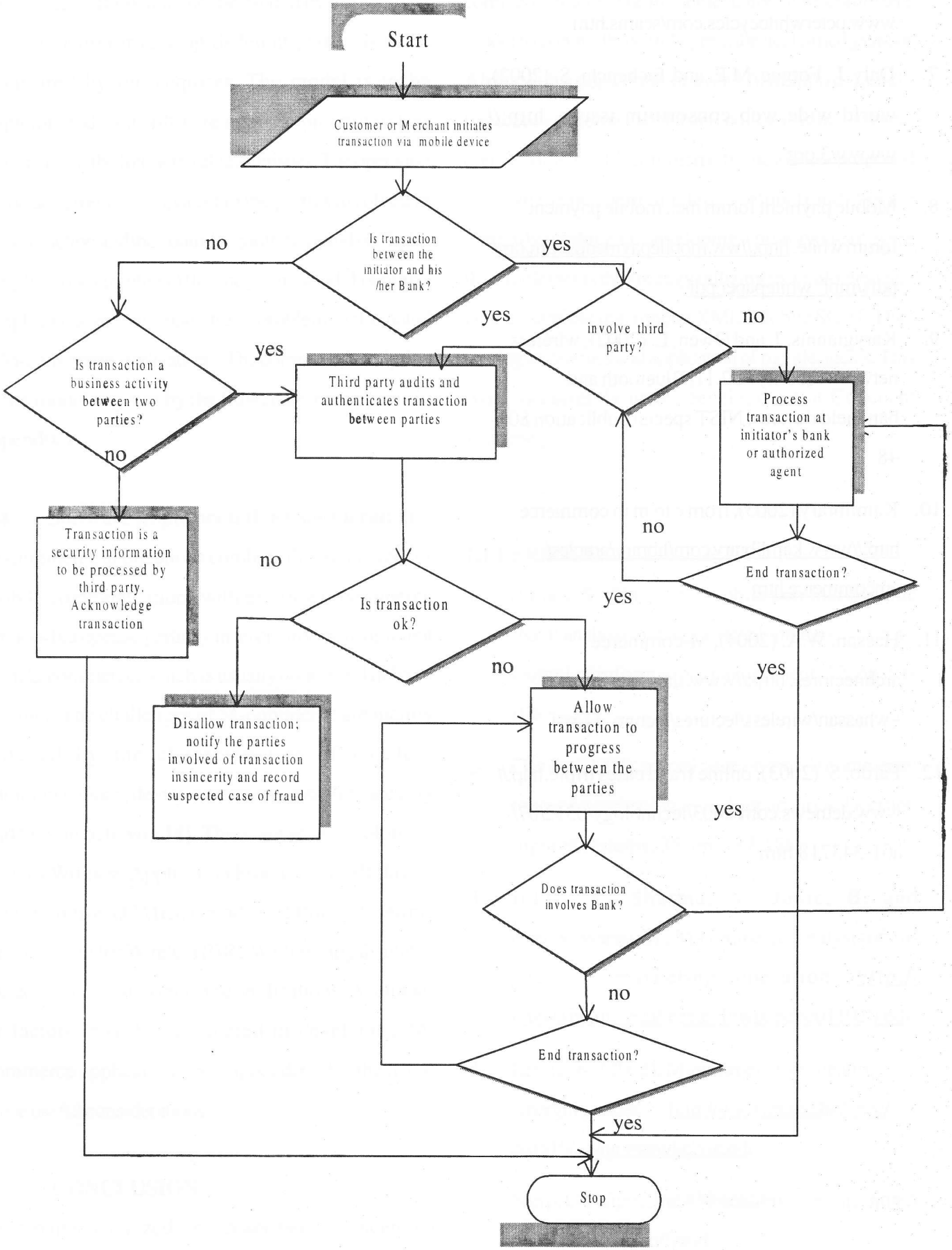
9. Karygiannis, J. and Owen, L. (2002), wireless network security 802.11, Bluetooth and handheld devices, NIST special publication 800-48

10. Kamlibrary (2003), from e to m in commerce. http://www.kamlibrary.com/library/articles/emcommerce.htm

11. Hassan, W.A. (2004), M-commerce architectures. http://www.site.uottawa.ca/~whassan/wireless/lectures/lecture_11.pdf

12. Pardo, S. (2003), online fraud cases triple.http://www.detnews.com/2003/technology/0312/07/a01-343718.htm

Appendix 1: Control-oriented M-commerce Transaction Algorithm



Appendix 2: M-commerce Application Development Consideration

S/N	CONSIDERATION	EXAMPLE
1.	Purpose of the application	Internal, Commercial, Customer and Infrastructure
2.	Processor to be used by the wireless application	Strong Arm, MIPS, Motorola Dragon ball, Power PC, Sparc, X86 and X scale
3.	Wireless devices to deploy the application	Cell phone, Smart card, Embedded processor, Personal digital assistants, Web pad, Pagers and Notebook
4.	Target operating system	BREW, J2ME, Linux, .Net compact framework, Nokia's series. Smart phone, Symbian / EPOC, Windows CE and Palm
5.	Capabilities of the wireless application	Colour support, Video support, Voice support, Keyboard support, Location positioning, Screen size and resolution, Bluetooth, Messaging, Animation, Printing, Transactional security and Alert
6.	IDE for the wireless development	Adobe, Borland C++ Builder, Borland JBuilder, Borland Kylix, Borland C# Builder, Eclipse, IBM web sphere, Macromedia Dreamweaver MX, Microsoft Visual Studio, Nokia's SDK, Openware tools, Oracle JDeveloper and Sun Java Studio
7.	Security method to incorporate with wireless LAN (WLAN)	Extensible authentication protocol, Wi-Fi protected access, Wired Equivalent Privacy (WEP), Wireless Transport Layer Security (WTLS), and Secure Sockets Layer (SSL)
8.	Security mechanisms to use on wireless application	Public Key Infrastructure (PKI), Wireless PKI (WPKI), Biometrics, Digital Signatures, Virtual Private Network (VPN) 2.0 security, SSL connections, Encryption
9.	Application software for the mobile application	Apache/Tomcat, ASP.Net, ColdFusion, HP application server, IBM WebSphere Everyplace, JRUN, Microsoft IIS, Oracle, iApp server wireless edition, WAP servers, Sun Java System Application Server and Borland Enterprise Server
10.	Connecting the back-end application to the Wireless application	Messaging CGI, ODBC, JDBC, JCA