
nigeria computer society
ncs
www.ncs.org.ng

# Conference Proceedings

Volume 23

**Theme:** "Towards a Cashless Nigeria: Tools and Strategies"

## Cashless 2012

**Edited By:**

Professor Charles O. UWADIA,

Professor Adesola ADEROUNMU

Dr. Adesina SODIYA

ISSN: 2141-9663

# ACKNOWLEDGEMENT

**The Nigeria Computer Society (NCS)** wishes to gratefully recognize the immense and revered support received from the following:

- Chams Plc
- Computer Professionals (Registration Council of Nigeria) **(CPN)**
- Data Foundation
- Data Sciences Nigeria Limited
- Dataflex Limited
- Galaxy Backbone Plc
- Image Technologies Limited
- Iris Smart Technologies Limited
- National Identity Management Commission **(NIMC)**
- National Information Technology Development Agency **(NITDA)**
- Omatek Computers Limited
- Sidmach Technologies Limited
- Zinox Technologies Limited

We equally recognize the laudable efforts of all other supporters in cash or in kind towards the success of the 24th National Conference

**REVIEWERS**

Prof. G. A. Aderounmu
Prof. J. O. A. Ayeni
Prof. L. O. Kehinde
Dr. G. M. M. Obi
Prof. 'Dele Oluwade
Dr. V. E. Asor
Dr. ' Sesan Adeyemo
Dr. (Mrs.) S.A. Onashoga
Dr. A. P. Adewole
Dr. A. O. Ajayi
Dr. S.E Adewumi
Dr. I. K. Oyeyinka
Prof. O. S. Adewale
Dr. D. K. Alese
Dr. S. O. Olabiyisi
Dr. O. B. Ajayi
Dr. O. Folorunso
Dr. (Mrs.) O.S. Onaolapo
Dr. A. I. Oluwaranti
Dr. A. T. Akinwale
Dr. E. O. Olajubu
Dr. O. A. Ojesanmi
Dr. E. Essien
Dr. E. G. Eseyin
Dr. (Mrs.) O. R. Vincent
Dr. Olumide B. Longe
Dr. A. A. O. Obiniyi
Dr. A. S. Sodiya

**Publication Office**
Nigeria Computer Society (NCS); Plot 10, Otunba Jobi Fele Way, Behind MKO Abiola Garden, Alausa, Ikeja
P.M.B. 4800 Surulere, Lagos, Nigeria. Phone: 01-7744600, 8962552
E-mail: publication@ncs.org.ng, ncs@ncs.org.ng Website: www.ncs.org.ng

# FORWARD

It is my pleasure and delight to welcome all of us to the 24th National Conference of the **Nigeria Computer Society (NCS)** which is holding at the beautiful City of Uyo, Akwa Ibom State, Nigeria from July 25 to 28, 2012. The theme of this year's Conference is **'Towards a Cashless Nigeria: *Tools and Strategies'***. To ensure real, inclusive development and transformation through Information Technology, the Conference will address the benefits, opportunities, sustainability and of course challenges of cashless especially as they relate to technology.

A total of 10 relevant topics, 15 well-written and peer-reviewed papers have been slated for presentation at different sessions of the Conference. In addition, 6 articles and 8 work in progress reports have been slated for poster presentations and **Research Consortium on Information Technology Innovations (ReCITI)** respectively. The programme of the Conference has been threaded into two major sections with eight principal tracks. The eight tracks will focus varied topics ranging from innovative software and hardware tools, entrepreneurship development and wealth creation strategies, capacity building and job creation, e-Government, call center issues and security to mention just a few. Indeed the next few days hold an ace for highly educative, thought-provoking, and elucidating discussions.

The Governor of the Central Bank of Nigeria will give the keynote address. There would be paper presentations by high profile speakers from different sector of the economy which include Executive Vice Chairman/CEO Nigerian Communication Commission, Country Managing Director, Accenture Nigeria, Managing Director, SystemSpecs Limited, Head Information and Technology Risk, Deloitte Nigeria, Director General/CEO, National Identity Management Commission, Managing Director, Red Star Express, Chief Executive officer, The Nigerian Stock Exchange, Partner and Head, Management Consulting, KPMG, among others.

The organizers of the Conference owe special thanks to our Chief Host, the Executive Governor of Akwa Ibom state, **Chief (Dr.) Godswill Akpabio**, towards the success of this Conference. We wish to extend our gratitude to all our collaborating partners, sponsors, and all those who have worked in putting this Conference together, Our President, Sir Demola Aladekomo FNCS, members of the National Executive Council, Provost COF and Fellows, Conferences Committee Members, members of the Akwa Ibom State Chapter of NCS, Secretariat staff and the Chairman Local Organizing Committee and his team. You are all great.

**Professor Sola ADEROUNMU**
Chairman Conferences Committee

# TABLE OF CONTENT

## Section 1

## Innovative Software and Hardware Tools; Entrepreneurship Development and Wealth Creation Strategies; and Capacity Building and Job Creation

# SECURED BANKING BY AUTOMATED SIGNATURE VERIFICATION AND FACE RECOGNITION

**T.S. Ibiyemi**
Dept. of Electrical & Electronics Engineering
University of Ilorin, Ilorin, Nigeria
ibiyemits@yahoo.com

**S.A. Aliu**
Dept. of Electrical & Electronics Engineering
University of Ilorin, Ilorin, Nigeria
aliu_adeiza@yahoo.com

**A. S. Daramola**
Dept. of Electrical & Information Engineering
Covenant University, Ota, Ogun State, Nigeria.
dabaslectcu@yahoo.com

***ABSTRACT***

*Face and signature are the two most acceptable means of authentication in the banking industry in spite their foolproof deficiency. Hence, it makes imperative the automation of the process of signature verification and face recognition in order to remove human factor in the authentication deficiency. This paper presents our work in the development in-house a two-in-one portable low cost dsPIC30F3013 digital signal processing microcontroller based system for real time handwritten signature verification and face recognition. The system has two C3188A 640 x 480 pixel colour cameras, one for face capture, and the other serves as handwritten signature scanner. A 12-dimensional feature vector extracted from the geometric shape and attributes of an offline signature image is used for verification. The face recognition algorithm is based on the principle of principal component analysis, PCA, to determine the basis vector known as eigenface.*

Keywords: *Automated banking, eigenface, face recognition, offline signature verification*

## 1. INTRODUCTION

Handwritten signature and face or facial photograph have been the two dominant and acceptable means of personal identification in authentication and authorisation. In spite of their shortcoming in foolproof identification, they still remain the most popular particularly in financial transaction, legal document, and institutions of higher learning. This attributable to the fact that facial photograph passport and handwritten signature can easily be used for personal identification in absentia of the person. In spite of other, even more secured, biometric modes, the banking industry still talk about signatory to an account with the signatory's facial photograph attached. Hence, there is a provoked research worldwide in provision of automatic signature verification and face recognition by machine. We have moved a bit further by developing a low-cost portable system for offline that is handwritten, signature verification and face recognition in one stand-alone package. A Microchip 16 bit digital signal processing microcontroller, dsPIC30F3013 DSC is the heart of our system.

Signature verification can be in two forms depending on method of acquisition for processing, namely, offline signature; and online signature. Signatures appended on papers, bank cheques, or documents and later scanned for automatic verification are referred to as offline signature verification. This verification process is based on the image of the signature, hence, susceptible to forgery. On the other hand, online signature verification is based on dynamic features of the signature extracted as the signature is being signed. It is a process that is more resilient to forgery than offline signature verification since the process is not directly visible to man but machine. But in the banking industry, signatures are required to be first signed on materials such as cheque, and financial document. Hence it is offline signature verification that is of concerned in this paper.

Signature forgery processes are in three levels , namely, random forgery, simple forgery, and skilled forgery. Random forgery is a signature written by an impostor who has neither the knowledge of the owner's name nor his/her genuine signature. But in the case of simple forgery, the impostor forges a signature based only on the knowledge of the owner's name. A skilled forgery, on the other hand, is based on a signature forged after having an unrestricted access to the owner's genuine signature (Daramola and Ibiyemi, 2010a and 2010b). This system is tested against the three types of forgeries.

The face recognition part of the system is based on the principle of principal component analysis, PCA, used for extracting the basis vectors also known as eigenfaces in a face space for face recognition (Ibiyemi and Aliu, 2002 and 2003). These eigenfaces are used as feature vectors as templates. The eigenface method is now widely used in face recognition because of its effectiveness and modest computational requirement (Brain, 2006). However, face recognition rate using eigenface is easily degraded by variation in illumination conditions, inconsistency in size of acquired face image, and rotation in face. Hence, measures are put in place in this work to handle these sources of degradations.

## 2. SYSTEM HARDWARE ARCHITECTURE

Fig.1 shows the block diagram of face recognition and signature hardware system. The hardware core is the Microchip 16bit dsPIC30F3013 digital signal controller with an in-built DSP, microcontroller, 24 KB on-chip flash program memory, 1 KB on-chip non-volatile data EEPROM, and can operate up to 30 MIPS. Two C3188A colour camera modules are interfaced to the dsPIC30F3013 DSC, one camera captures

face image while the other camera is either used as an offline signature scanner or as ID card scanner. The C3188A camera module is based on OV7620 image sensor with f6mm, f1.6 lens fitted , and 640 x 480 pixels digital data output. The signature scanner supports 300 dpi. Two set of external banks of memory are serially interfaced to the DSC. One set has 2 MB flash memory, and 2 MB serial SRAM for signature images and signature templates. The second set has a similar configuration for face images, eigenfaces, and weight vectors.

The face images captured by the face camera are down sampled into 200 x 160 pixels, while the signature scanner operates at 300 dpi. The system has DS1307 real-time clock integrated for time and date stamping of any authenticated transaction. The offline signature algorithm and the eigenface algorithm as described in section 3 are coded in C language using MikroC Pro for dsPIC and ported to dsPIC30F3013 on EasydsPIC6 development system.

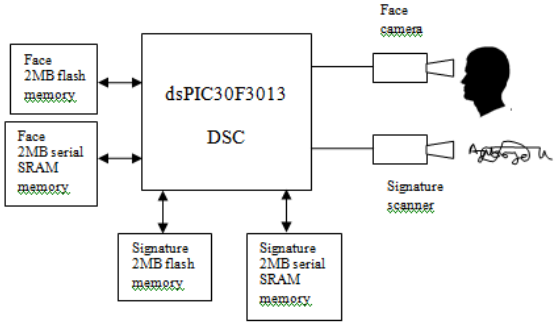



*Fig 1: The Face Recognition and offline Signature verification System Hardware Architecture*

## 3. SYSTEM SOFTWARE ARCHITECTURE

Fig.2. shows the system software architecture consisting of offline signature algorithm path and face recognition algorithm path.

### 3.1 OFFLINE SIGNATURE VERIFICATION ALGORITHM

The offline signature verification algorithm (Ashish et al, 2004; Huang and Yan, 1997) is made up of the following sequence:

**Signature Pre-processing:**

Given K training colour signature images, each of size M x N:

(a) Convert each RGB colour signature image to grey scale

(b) Invert the grey scale of each image such that the signature image has higher grey levels:

$$S'_{i,j} = 255 - S_{i,j} \quad ,i = 1,2,\cdots,M \quad ; j = 1,2,\cdots,N \qquad (1)$$

(c) Perform signature segmentation:

(i) Obtain row zero-mean of the signature image:

$$S''_{i,j} = S'_{i,j} - \frac{1}{M}\sum_{l=1}^{M} S'_{l,j} \quad ; i = 1,2,\cdots,M \; ; \; j = 1,2,\cdots,N \qquad (2)$$

(ii) Segment signature:

$$S''_{i,j} = \begin{cases} S''_{i,j} & ,if \; S''_{i,j} > 0 \\ 0 & ,otherwise \end{cases} \qquad (3)$$

(d) Smooth Signature Image using 3 x 3 averaging window

$$S'''_{i,j} = \frac{1}{9}\left(\sum_{h=i-1}^{i+1}\sum_{k=j-1}^{j+1} S''(h,k)\right), i = 1,2,\cdots,M; \quad j = 1,2,\cdots,N \qquad (4)$$

(e) Perform Binarisation using global threshold [ ]:

$$S'''_{i,j} = \begin{cases} 1 & ,if \; S'''_{i,j} > T \\ 0 & ,otherwise \end{cases} \qquad (5)$$

(d) Apply thinning algorithm of [6,7 ]

**Signature Feature Extraction:**

Some geometric features are extracted and used as a feature vector:

(i) Aspect Ratio, $\eta$ :

Aspect ratio, $\eta$ , is the ratio of signature width to signature height which is considered fairly consistent.

(a) Compute horizontal projection and vertical projection:

$$x_i = \sum_{j=0}^{N-1} S'''_{i,j} \quad ,i = 0,1,\cdots,M-1$$
$$y_j = \sum_{i=0}^{M-1} S'''_{i,j} \quad , j = 0,1,\cdots,N-1 \qquad (6)$$

(b) Determine width from horizontal projection and height from vertical projection:

**Signature Width,** $\Delta w$ :

*for i=1 to M do scan* $x_i$ *to find first position where* $x_i \geq 3$ and *let* $i_{low} = i$ ;

*for i=M downto 1 do scan* $x_i$ *to find first position where* $x_i \geq 3$ *and let* $i_{high} = j$ ;

$$\Delta w = i_{high} - i_{low} \qquad (7a)$$

**Signature height,** $\Delta h$ :

*for j=1 to N do scan* $y_j$ *to find first position where* $y_j \geq 3$ *and let* $j_{low} = j$ ;

*for j=N downto 1 do scan* $y_j$ *to find first position where* $y_j \geq 3$ *and let* $j_{high} = j$ ;

$$\Delta h = j_{high} - j_{low} \qquad (7b)$$

(c) Obtain aspect ratio:

$$\eta = \frac{\Delta w}{\Delta h} \qquad (8)$$

(ii) Slant Angle, $\varphi$:

The angle that the signature images make with the horizontal line is known as the slant angle. It is the angle at which the ratio of horizontal projection to the width projection as the angle is varied becomes maximum.

(a) Find the slant angle, $\varphi$:

$$\varphi = \arg\max_{\varphi}\left(\frac{\sum_{j=0}^{N-1} S'''_{i,j}(\theta)}{\Delta w(\theta)}\right), i = 1,2,\cdots,M\ ; -\theta_1 \le \theta \le \theta_2 \quad (9)$$

*where*:

$\Delta w(\theta) \Rightarrow width\ of\ signature\ image\ (see\ eqn.16a)\ at\ angle\ \theta$

(b) Rotate every pixel of signature image by $\varphi$:

$$\begin{bmatrix} \vec{S'''_x} \\ \vec{S'''_y} \end{bmatrix} = \begin{bmatrix} \cos\varphi & -\sin\varphi \\ \sin\varphi & \cos\varphi \end{bmatrix} \cdot \begin{bmatrix} S'''_x \\ S'''_y \end{bmatrix} \quad (10)$$

(iii) Normalised Area of signature, $A'$:

The normalised area is defined as the ratio of the area occupied by actual signature image to the area of its bounding box. This is can be inferred from eqns(15,16,17):

$$A' = \frac{\sum_{i=i_{low}}^{i_{high}} \sum_{j=0}^{M-1} x_j}{\Delta w.\Delta h} \quad (11)$$

(iv) Centre of Gravity, $(X,Y)$:

The centre of gravity of a signature image can be inferred from eqns (15,16,17) as:

$$X = \frac{\sum_{j=0}^{N-1} y_j.j}{\Delta w.\Delta h} \quad , \quad Y = \frac{\sum_{i=0}^{M-1} x_i.i}{\Delta w.\Delta h} \quad (12)$$

(v) Slope of line joining centres of gravity of two halves of signature, $m$:

(a) Divide signature image within bounding box into two (left, right) halves. The left box is defined by $((i_{low}, i_{high}),(j_{low}, l'))$, and right box by $((i_{low}, i_{high}),(l', j_{high}))$ as inferred from eqns(15,16,17).

$$l' = \frac{j_{high} - j_{low}}{2} \quad (13)$$

(b) Using eqn (21), obtain the centre of gravity (X1,Y1) of the left box; and the centre of gravity (X2,Y2) of the right box.

(c) Calculate slope

$$m = \tan^{-1}\left(\frac{X1 - X2}{Y1 - Y2}\right) \quad (14)$$

(vi) Number of edge points, $\gamma$:

An edge point is a signature pixel having only one neighbour in the 8-neighbour window. A 3 x 3 structuring window with all its element 1's is slided over the the signature box to obtain these edge points.

(vii) Number of cross points, $\chi$:

A cross point is a signature pixel having three neighbours in the 8-neighbour window. A 3 x 3 structuring window with all its element 1's is slided over the signature box to obtain these cross points.

A 12-dimensional feature vector $F = [\eta, \varphi, A', X, Y, X1, Y1, X2, Y2, m, \gamma, \chi]$ is used to characterised each signature.

**Signature Classification**

When a questionable signature is presented to the system, it pre-processed and the 12-elements feature vector extracted. Then, the distance measure between this feature vector of this questionable signature and those feature vector templates are taken using eqn (15):

$$\delta = \arg\min_i \left\| F_{questionable} - F_i \right\|_2 \quad , i = 1,2,\cdots\cdots,K \quad (15)$$

*if* $\delta < T'$ *then* $F_{questionable}$ *recognisedas signatureof* $i-th$ *authentic*

*else impostor*

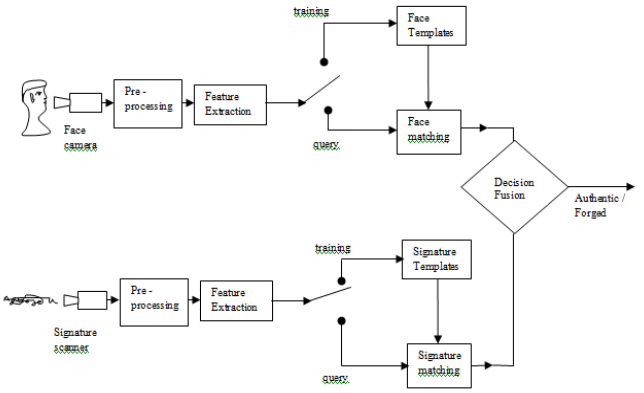



*Fig 2: Face Recognition and Signature Verification System Software Architecture*

## 3.2 FACE RECOGITION BY EIGENFACE ALGORITHM

Face recognition by eigenface algorithm (Ibiyemi and Aliu, 2003; Ashish et al, 2004; Turk and Pentland, 1991) consists of the following sequence:

**Face Pre-processing:**

Given K colour face images, each of size M x N:

(a) Convert each RGB colour image to grey scale:

$$\Gamma_{i,j} = \sum_{l=1}^{3} \begin{bmatrix} 0.299 \\ 0.587 \\ 0.114 \end{bmatrix}^T .G_{i,j,l} \quad , i = 1,2,\cdots,M\ ; \quad j = 1,2,\cdots,N \quad (16)$$

*where*:

$\Gamma_{i,j} \Rightarrow grey\ scale\ image$

$G_{i,j,l} \Rightarrow Colour\ RGB\ image$

(b) Create training image matrix (M.N x K) with each column representing a vectorised image of length, M.N:

$$F = [\Gamma_1, \Gamma_2, \cdots\cdots, \Gamma_K]$$
$$where: \quad \Gamma_i = [x_0, x_1, \cdots\cdots, x_{M.N-1}]^T \qquad (17)$$

(c) Perform illumination normalisation:

$$F' = (F_i - \mu_0).\frac{\sigma_i}{\sigma_0} + \mu_i \quad , i = 1,2,\cdots, K$$

*where*:

$$\mu_i = \frac{1}{M.N}\sum_{j=0}^{M.N-1} x_j \ , \qquad (18)$$

$$\sigma_i = \sqrt{\left(\frac{1}{M.N}\sum_{j=0}^{M.N-1}(x_j - \mu_i)^2\right)}$$

$$\mu_0 \Rightarrow desired\, mean, typically = 100$$
$$\sigma_0 \Rightarrow desired\, standard\, deviation, typically = 100$$

(d) Obtain zero-mean training image matrix:

$$\Phi_i = F_i' - \Psi \qquad , i = 1,2,\cdots, K$$
$$where:$$
$$\Psi = \frac{1}{K}\sum_{i=1}^{K} F_i' \qquad (19)$$
$$A = [\Phi_1, \Phi_2, \cdots, \Phi_K]$$

**Face Feature Extraction:**

(a) Obtain covariance matrix:

$$C = AA^T$$
$$where: \quad C \Rightarrow M.N\ x\ M.N \quad matrix \qquad (20)$$
$$\therefore \ L = A^T.A$$
$$where: \quad L \Rightarrow K\ x\ K\ matrix$$

(b) Calculate eigenvalues and eigenvectors:
Obtaining (M.N) eigenvalues and corresponding (M.N) eigenvectors of length (M.N.) each is computationally intractable even for a modest size image. Hence, better to obtain K eigenvalues and corresponding K eigenvectors of length K each.
Let the eigenvectors of reduced matrix L be

$$v_i \ , i = 1,2,\cdots, K$$

From the eigenvectors of the reduced matrix, the eigenvectors of large matrix C can be obtained:

$$U_i = \sum_{j=1}^{K} v_{i,j}\Phi_j \quad , i = 1,2,\cdots, K \qquad (21)$$

These eigenvectors, Ui , are like the face images hence they are called eigenfaces.
Each of the eigenface has varying significance depending on the magnitude of its eigenvalue. Hence, it suffices to select a subset K' of the K eigenfaces corresponding to K' highest valued eigenvalues as characterising the entire training face images.
These reduced subset K' eigenfaces are stored , in addition to the mean face.

(c) Calculate weight vectors by projecting training face images onto the stored eigenfaces:
The contribution of a stored eigenface to an zero-mean training face image can be calculated as a scalar weight. Therefore, a weight vector of length K' whose elements represent the degree of contribution of the corresponding eigenface to that zero-mean image is obtained by projection:

$$\omega_j = U_j^T.\Phi_j \quad , j = 1,2,\cdots, K'$$
$$\therefore \ \Omega_i = [\omega_1, \omega_2, \cdots\cdots, \omega_{K'}], \qquad (22)$$
$$i = 1,2,\cdots\cdots, K'$$

The calculated $(K'\,x\,K')$ weight matrix is stored as reference templates.

**Recognition of a query face:**
On presentation of a new face image to the system for classification, it is converted to grey scale, and then normalised. Then the zero-mean image is obtained and its weight vector is obtained by projecting it onto the stored eigenfaces.

(a) Calculate weight vector for the new image:

$$\Omega_{new} = U_i.(F_{new}' - \Psi) \quad , i = 1,2,\cdots, K' \qquad (23)$$

(b) Perform classification by matching using Euclidean distance metric:

$$\varepsilon = \arg\min_i \|\Omega_{new} - \Omega_i\|_2 \quad , i = 1,2,\cdots\cdots, K'$$
$$if\ \varepsilon < T\ then\ F_{new}\ recognised\ as\ i-th\ training \qquad (24)$$
$$image\ else\ unknown$$

**Decision Fusion**
The decision fusion is simply based on the logical AND of the two matching results. Hence, for recognition (authentic) classification both modes must have an output of recognition (authentic) otherwise the final result is not recognised (forgery).

## 4. EXPERIMENT AND RESULT

The system was used to capture face images from 100 persons; these images were downloaded to host PC in order to test the developed algorithm for face recognition. Out of these training faces, 40 most significant eigenfaces were stored. The recognition rate was 97% using face recognition mode alone. In case of signature verification, the same 100 persons were used to sign 5 times on A4 paper. Also, 20 of them were used as impostors to give simple, random, and skilled forged signatures. These signatures are then scanned by the in-built signature camera module of the system and downloaded to the PC. The recognition rate was 95%, simple and random forgeries gave FAR of 1%, while skilled forgeries has FAR of 45%. However, when the decision fusion was activated the recognition rate was about 98%. After these tests, 30 most significant eignefaces, and 100 weight vectors were ported to the system flash memory for face, while 100 signature feature vectors were ported to the system flash memory.

## 5. CONCLUSIONS

A portable low-cost embedded system based on dsPIC30F3013 DSC with two digital colour camera has been developed for face recognition and offline signature verification. The recognition results for face recognition and signature verification are satisfactory both on the host PC and on the target embedded system.

## ACKNOWLEDGEMENT

We acknowledge with great appreciation the generous research and development grant received from Federal Government of Nigeria through the STEP-B project to execute this work.

## REFERENCES

Ashish Dhawan, Aditi R. Ganesan, 2004. Handwritten Signature Verification, *ECE533 Project Report ,*pp. 1-15

Brian Harding, Cat Jubinski, 2006. A Standalone Face Recognition Access Control System, *ECE4760 Final Project Report,* pp.1-10

Daramola S., Ibiyemi T.S., 2010a, Novel Feature Extraction Techniques for Offline Signature Verification, *International Journal of Engineering Science and Technology*, vol.12, no.7, pp3137-3143.

Daramola S., Ibiyemi T.S., 2010b. Person Identification System using Static and Dynamic Signal Fusion, *International Journal of Computer Science & Information Security*, vol.6, no.7, pp88-92.

Huang K., Yan H., 1997. Offline Signature Verification based on Geometric Feature Extraction and Neural Network Classification, Pattern *Recognition* 30, pp.9-17.

Ibiyemi T.S., Aliu S.A., 2002. On Computation of Optimum Basis Vector for Face Detection and Recognition, *Abacus: Mathematics Series*, 29(2), pp 144-149

Ibiyemi T.S., Aliu S.A., 2003. Automatic Face Recognition by Computer, *Abacus: Mathematics Series*, vol 30, no. 2B, September, pp180-188

Turk M., Pentland A., 1991. Eigenfaces for Recognition, *Journal of Cognitive Neuroscience*, vol. 3, no.1, pp71-86

# DEVELOPMENT OF IRIS AND FINGERPRINT BIOMETRIC AUTHENTICATED SMART ATM DEVICE & CARD

**T.S. Ibiyemi**

Dept. of Electrical & Electronics Engineering
University of Ilorin, Ilorin, Nigeria
*ibiyemits@yahoo.com*

**S.E. Obaje**

Dept. of Computer Engineering
Federal Polytechnics, Offa, Kwara State, Nigeria
*obajese@yahoo.com*

**J. Badejo**

Dept. of Electrical & Information Engineering
Covenant University, Ota, Ogun State, Nigeria.
*joke.badejo@covenantuniversity.edu.ng*

***ABSTRACT***

*A portable low-cost system that uses iris and fingerprint to authenticate business transaction particularly in banking was developed. A user's Automated Teller Machine (ATM) card contains his/her iris and fingerprint templates in addition to the traditional pin. The developed ATM card has the same level of its data content protection as the existing ATM cards. Towards providing maximum security, both the iris and fingerprint must be valid for any transaction to scale through.*

***Keywords:*** *Authentication, ATM card, dsPIC30F13 controller, Fingerprint, Iris*

## 1. INTRODUCTION

Human iris is believed to provide the most secured biometric for personal identification because it has about six times discriminatory features more than fingerprint which is its distant second. For people to have more confidence in cashless regime, a more secured electronic business transaction mode must be put in place. Hence, a portable low-cost system that uses iris and fingerprint to authenticate business transaction particularly in banking was developed. A user's ATM card contains his/her iris and fingerprint templates in addition to the traditional pin. The developed ATM card has the same level of its data content protection as the existing ATM cards. Towards providing maximum security, both the iris and fingerprint must be valid for any transaction to scale through. The iris camera is usable up to 35 cm to the user.

## 2. SYSTEM HARDWARE ARCHITECTURE

Figure 1 shows the hardware architecture of the developed embedded system. The central processor is a Microchip 16/32 bit dsPIC30F3013 digital signal controller, DSC. The dsPIC30F3013 is a digital signal processor and general purpose microcontroller in one IC. It has on the chip 24 KB of flash program memory, 1KB of non-volatile data EEPROM, 2 KB of RAM, and can operate up to 30 million instructions per second (MIPS),(Microchip, 2005). Interfaced to the DSC are two set of 2 MB flash memory, and two set of 2 MB serial SRAM. One set of 2 MB flash and 2 MB SRAM is for iris templates and data processing, while the other set is for fingerprint template and data processing. Also, an iris camera developed from OV9620 camera module is interfaced to the DSC for capturing eye images at a standoff distance of up to 35 cm. The ov9620 is a colour camera module of 1280 x 1024 pixels with a significant response up to the near infrared. An XFM220 fingerprint sensor module interfaced through its rs232 to the DSC is used for fingerprint data capture. The smart card reader/writer with in-built security access module is also interfaced to the DSC. A global positioning system (GPS), module for providing time and date stamp of any business transaction is provided with this system.

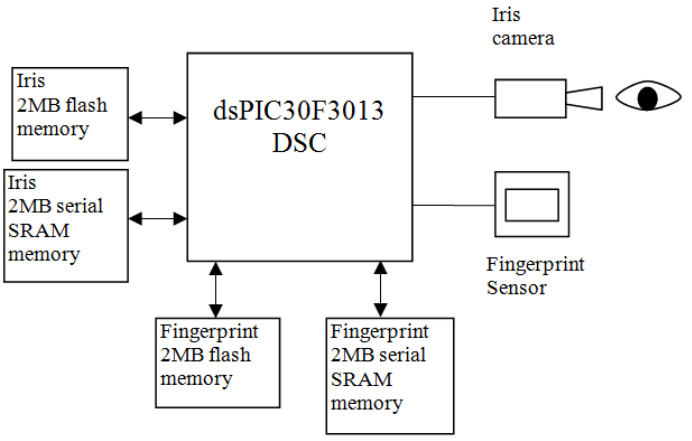



*Fig 1: Hardware Architecture of Iris and Fingerprint Recognition System*

## 3. SYSTEM SOFTWARE ARCHITECTURE

The system software is based on the iris recognition algorithm and fingerprint recognition algorithm described in section 3.1 and section 3.2 respectively. Figure 2 shows the flow diagram of these algorithms. For the training phase, these algorithms were coded in MikroC Pro for dsPIC on Pentium duo core 2.6GHz and 2GB RAM. The training fingerprint images and training eye images are collected using our developed embedded system. The down sampling of the fingerprint and iris images to 320 x 200 pixels was done in software. The iris and fingerprint templates of individual users, and other ancillary data are stored on the smart card. The *hex file* of the developed software in MikroC is then ported to the dsPIC30F3013 DSC via EasydsPIC6 development board.

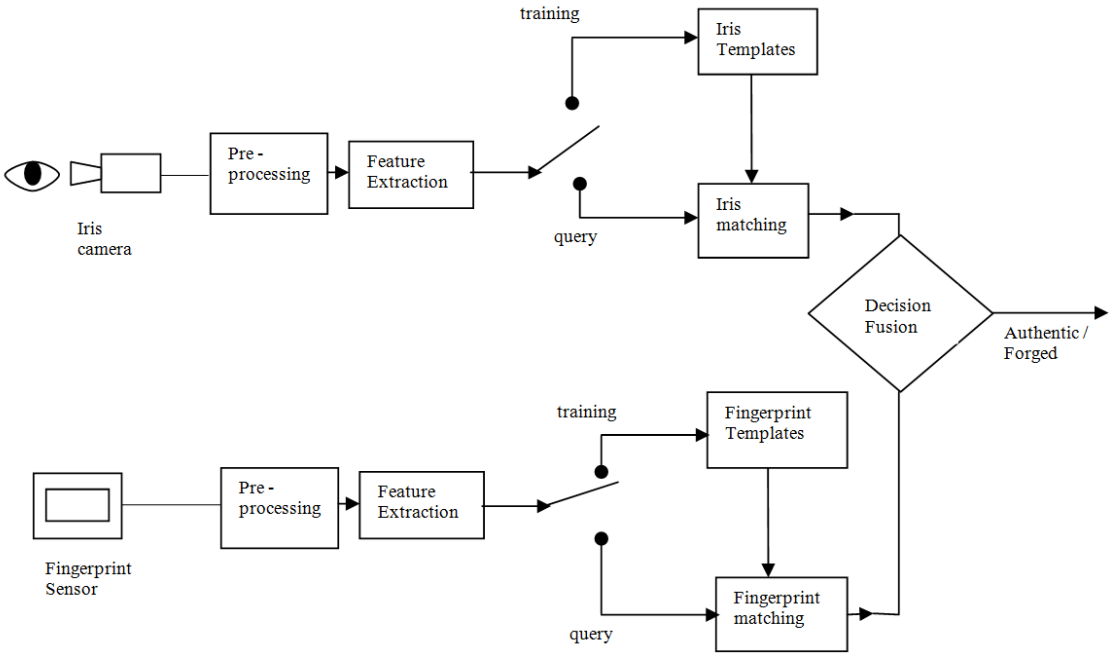



*Fig 2: Software Architecture of Iris Recognition and Fingerprint Recognition System*

### 3.1. IRIS RECOGNITION ALGORITHM

The iris recognition algorithm used in this work is largely based on algorithms described in (Daugman, 2004; Wilde, 1997; Ghassan et al, 2009; Al-Zubi-Nadi, 2007).

*3.1.1. Iris Pre-processing:*

(i) Convert eye image in RGB colour to grey scale:

$$E'_{i,j} = \sum_{l=1}^{3} \begin{bmatrix} 0.299 \\ 0.587 \\ 0.114 \end{bmatrix}^T . E_{i,j,l} \quad , i = 1,2,\cdots,M \; ; \quad j = 1,2,\cdots,N \tag{1}$$

*where*:

$E'_{i,j} \Rightarrow grey\ scale\ image$

$E_{i,j,l} \Rightarrow Colour\ RGB\ image$

(ii) Convolve 3x3 smoothing Gaussian filter window with eye image

$$w(x,y) = \frac{1}{2\pi\sigma^2} e^{-\frac{x^2+y^2}{2\sigma^2}} \quad , -1 \le x,y \le 1 \tag{2a}$$

Obtain the $(mxm)$ discrete kernel for maximum grey intensity of 255, m=3, and ϭ =1:

$$w(i,j) = \frac{255}{\sum_{i=-(m-1)/2}^{(m-1)/2} \sum_{j=-(m-1)/2}^{(m-1)/2} w(i,j)} \left\{ \frac{1}{2\pi\sigma^2} e^{-\left(\frac{i^2+j^2}{2\sigma^2}\right)} \right\}, -(m-1)/2 \le i,j \le (m-1)/2 \tag{2b}$$

The 3 x 3 kernel coefficients are:

$$\therefore \; w(i,j) = \frac{1}{201} \begin{bmatrix} 15 & 25 & 15 \\ 25 & 41 & 25 \\ 15 & 25 & 15 \end{bmatrix} \; ; \; -1 \le i,j \le 1 \tag{2c}$$

Convolving the kernel with the eye image:

$$E''(i,j) = \sum_{k=-1}^{1} \sum_{l=-1}^{1} w'(k,l).E'(i+k,j+l) \tag{2d}$$

(iii) Find centre of pupil $(x_0, y_0)$ by vertical and horizontal projection:

$$x_o = \arg\min_x \sum_{y=0}^{N-1} E''(x,y)$$
$$y_o = \arg\min_y \sum_{x=0}^{M-1} E''(x,y) \tag{3}$$

(iv) Compute image gradient, i.e. edge map, using sobel operator

$$\nabla = \left( \frac{\partial}{\partial x}, \frac{\partial}{\partial y} \right)$$

$\therefore$ *The 3x3 sobel kernel coefficient matrix*:

$$s_v = \begin{bmatrix} -1 & -2 & -1 \\ 0 & 0 & 0 \\ 1 & 2 & 1 \end{bmatrix} \quad , \quad s_h = \begin{bmatrix} -1 & 0 & 1 \\ -2 & 0 & 2 \\ -1 & 0 & 1 \end{bmatrix} \tag{4}$$

*where*: $s_v \Rightarrow vertical\ sobel$ , $s_h \Rightarrow horizontal\ sobel$

*The gradient amplitude*, $s$:

$$s = \sqrt{\left(s_h^2 + s_v^2\right)} \cong |s_h| + |s_v|$$

(v) Obtain papillary boundary by applying circular Hough Transform to the edge map

$$\max\arg_{(x_p,x_p,r)}\left(\left(x_p-x_o\right)^2+\left(y_p-y_o\right)^2=r_p\right) \quad (5)$$

*where*: $(x_o,y_o)\Rightarrow pupil's\ centre,\ r_p\Rightarrow pupil's\ radius$

(vi) Obtain limbic boundary by Daugman's Intergro-Differential Operator, IDO (Daugman, 2004):

$$\max_{(x_o,y_o,r)}\left|G_\sigma(r)*\frac{\partial}{\partial r}\oint\frac{E''(x,y)}{2\pi r}ds\right| \quad (6)$$

*where*:

$$G_\sigma(r)=\frac{1}{\sigma\sqrt{(2\pi)}}e^{\frac{(r-r_0)^2}{\sigma^2}}$$

$(x_o,y_o,r)\Rightarrow centre\ \&\ radius\ of\ searching\ circle\ ,G_\sigma\Rightarrow smoothing\ radial\ gaussian\ filter$

*Discrete IDO*:

$$\max_{(x_o,y_o,n\Delta r)}\left|\frac{1}{\Delta r}\sum_{l=1}^{K}\left\{G_\sigma\left((n-1)\Delta r\right)-G_\sigma\left((n-l-1)\Delta r\right)\sum_{h=1}^{m}E''\left(\left(l\Delta r.\cos(h\Delta\theta)+x_o\right),\left(l\Delta r.\sin(h\Delta\theta+y_o\right)\right)\right\}\right|$$

The segmented iris annular spans $\lfloor r_p, r_i \rfloor$ as obtained in eqn(5 ) and eqn ( 6) respectively.

(vii) Re-map annular iris from Cartesian coordinate to polar coordinate

$$E''\left(x(r,\theta),y(r,\theta)\right)\rightarrow E''(r,\theta)$$

*where*:

$$x(r,\theta)=(1-r)x_p(\theta)+rx_i(\theta) \quad (7)$$
$$y(r,\theta)=(1-r)y_p(\theta)+ry_i(\theta)$$
$$r\Rightarrow[0,1]\ ,\ \theta\Rightarrow[0,2\pi]$$

(viii) Perform enhancement of the unwrapped, i.e. normalised polar, iris image by histogram equalisation:

Let grey image $E''(x,y)$ of intensity range $[L_{\min},L_{\max}]$

Obtain intensity histogram of $E''(x,y)$ :

$$hist(i)\ ,\forall i=0,1,\cdots,L$$
$$hist\left(E''(x,y)\right)=hist\left(E''(x,y)\right)+1\ ,\forall x=0,1,\cdots,N-1;\forall y=0,1,\cdots,M-1$$

*Obtain equalised cumulative frequency:*

$$C_k=\left\{\left(\sum_{j=0}^{k}hist(j)\right).\left(\frac{L}{M.N}\right)\right\}+0.5 \quad (8a)$$

*Re-map original grey image's intensities to equalised image's intensities:*

$$E'''(x,y)=C\left(E''(x,y)\right)\ ,x=0,1,\cdots,N-1,y=0,1,\cdots,M-1 \quad (8b)$$

*3.1.2. Iris Feature Extraction*

Apply 2-D Gabor filter in polar coordinate and Daugman's 2 bit phase quantization encoding:

$$G(r,\theta)=e^{\left(-2\pi jw(\theta-\theta_0)-\frac{(r-r_0)^2}{\alpha^2}-\frac{(\theta-\theta)^2}{\beta^2}\right)} \quad (9)$$

The iris feature encoding is done by quantisation the phase into four quadrants and encoding phase sign in each quadrant by 2 bits

*3.1.3. Iris Matching*

Calculate Hamming distance, HD, between template code and the query code:

$$d=\min\left\{\frac{1}{n}\sum_{j=1}^{n}\left(A_j\oplus B_j\right)\right\} \quad (10)$$

*where*:
$A\Rightarrow template\ code$
$B\Rightarrow query\ code$
$\oplus\Rightarrow logical\ exclusive-OR$

If $(d<T)$ then iris_Recognised otherwise iris_not_Recognised.

### 3.2. FINGERPRINT RECOGNITION ALGORITHM

The fingerprint recognition algorithm used in this work is largely based on algorithms described in (Jain et al, 1997; Chandan et al, 2005; Zhang, 1984; Peter and Mathew, 2012; Maltoni et al, 2003).

*3.2.1. Fingerprint Pre-processing*

(i) Invert the grey scale of each fingerprint image to make ridges foreground and furrows background:

$$F'_{i,j}=255-F_{i,j}\ \ ,i=1,2,\cdots,M\ \ ;j=1,2,\cdots,N \quad (11)$$

(ii) Perform image Normalisation

$$F''(x,y)=\begin{cases}\mu_0+\sqrt{\frac{\sigma_0^2.\left(F'(x,y)-\mu\right)^2}{\sigma^2}}\ ,if\ F'(x,y)\geq\mu\\ \mu_0-\sqrt{\frac{\sigma_0^2.\left(F'(x,y)-\mu\right)^2}{\sigma^2}}\ ,otherwise\end{cases} \quad (12)$$

*where*: $\mu_0=100\Rightarrow desired\ mean;\sigma_0=100\Rightarrow desired\ variance$

(iii) Apply 2-D Gaussian smoothing filter

Obtain 5 x 5 kernel coefficient from eqn (2b) for m=5, σ =1:

$$\therefore\ w(i,j)=\frac{1}{253}\begin{bmatrix}1&3&6&3&1\\3&15&25&15&3\\6&25&41&25&6\\3&15&25&15&3\\1&3&6&3&1\end{bmatrix}\ ;\ -2\leq i,j\leq 2 \quad (13)$$

Convolve 5 x 5 Gaussian kernel with the fingerprint image:

$$F'''(i,j) = \sum_{k=-2}^{2}\sum_{l=-2}^{2} w(k,l).F''(i+k, j+l) \quad (14)$$

(iv) Perform Histogram Equalisation of fingerprint image using eqns (8a&b)

(v) Binarise fingerprint image using mean of 8-neighbour as threshold:

$$f'''(i,j) = \begin{cases} 1 & ,if\ F'''(i,j) \geq \left( \sum_{l=-1}^{1}\sum_{k=-1, i+k\neq 0}^{1} F(i+l, j+k) \right) \\ 0 & ,otherwise \end{cases} \quad (15)$$

(vi) Perform Thinning of binarised fingerprint image based the algorithm in (Zhang, 1984):

*_Thinning_algorithm*
*{*

| | | |
|---|---|---|
| *p9* | *p2* | *p3* |
| *p8* | *p1* | *p4* |
| *p7* | *p6* | *p5* |

*Let A(p)* $\Rightarrow$ *no. of 0→1transitions in sequence p2p3p4p5p6p7p8p9*
*Let B(p)* $\Rightarrow$ *no. of non-zero neighbours of p*
*Repeat*
*(*
*Scan entire image with 3 x 3 window*
*(*
*if* $((2 \leq B(p) \leq 6) \& (A(p)=1) \& (p2 * p4 * p6 = 1) \& (p4 * p6 * p8 = 1))$
*then delete p;*

*Scan entire image with 3 x 3 window*
*(*
*if* $((2 \leq B(p) \leq 6) \& (A(p)=1) \& (p2 * p4 * p8 = 1) \& (p2 * p6 * p8 = 1))$
*then delete p.*
*)*
*} UNTIL ( no more deletion).*

### *3.2.2. Fingerprint Feature Extraction*

(i) Extract Minutia using condition number, $C_N$, of 3 x 3 window & Store them:

$$C_N = 0.5\left( \sum_{i=1}^{8} p_{(i+1) \bmod 8} - p_i \right) \quad (16)$$

$$\therefore\ p = \begin{cases} ridge\ ending; store\ \gamma_j = [t_j, x_j, y_j, \theta_j],\ j = j+1 & ,if\ C_N = 1 \\ ridge & ,if\ C_N = 2 \\ ridge\ bifurcation; \psi_j = [t_j, x_j, y_j, \theta_j],\ j = j+1 & ,if\ C_N = 3 \end{cases}$$

*where:* $p \Rightarrow$ *windowcentre pixel,* $p_1 - p_8 \Rightarrow$ *8neighbours*

$$t = \begin{pmatrix} 0 \Rightarrow ridge\ ending \\ 1 \Rightarrow ridge\ bifurcation \end{pmatrix},\ (x,y) \Rightarrow \text{minutiacoordinate}, \theta \Rightarrow angle\ with\ x-axis$$

(ii) Remove false minutiae using algorithm in (Zhou, 2004)

### *3.2.3. Minutiae Matching & Decision Logic:*

The minutiae alignment and matching algorithm used in our work is largely based on that in (Jain, 1997):

(i) Perform Minutiae Alignment

Given R minutiae template and Q input query minutiae, align the two set of minutiae using geometrical transformation of translation and rotation.

$$Let\ R = \{\gamma_1, \gamma_2, \cdots\cdots, \gamma_M\},\ Q = \{\psi_1, \psi_2, \cdots\cdots, \psi_N\}$$
$$where: \gamma_i = (t_i, x_i, y_i, \theta_i), i = 1,2,\cdots,M;\ \psi_j = (t'_1, x'_1, y'_1, \theta'_1), j = 1,2,\cdots,N \quad (17)$$

Align every minutia in input query fingerprint image with respect to reference minutia:

$$[x''_i\ y''_i\ \theta''_i] = [x'_i - x_r\ \ y'_i - y_r\ \ \theta'_i - \theta_r] . \begin{bmatrix} \cos\Delta\theta & \sin\Delta\theta & 0 \\ -\sin\Delta\theta & \cos\Delta\theta & 0 \\ 0 & 0 & 1 \end{bmatrix} + \begin{bmatrix} \Delta x \\ \Delta y \\ \Delta\theta \end{bmatrix}, i = 1,2,\cdots,N \quad (18)$$

$$where: [x'_i\ y'_i\ \theta'_i] \Rightarrow i-th\ input/query\ \text{minutia}, [x_r\ y_r\ \theta_r] \Rightarrow reference\ \text{minutia}$$

(ii) Perform Minutiae Matching

Firstly, map both aligned query $Q''$ and template R minutiae into polar coordinate, and then concatenate each minutia in ascending of radial angle magnitudes.

$$\begin{bmatrix} r''_i \\ \phi''_i \\ \vartheta''_i \end{bmatrix} = \begin{bmatrix} \sqrt{\{(x''_i - x_r)^2 + (y''_i - y_r)^2\}} \\ \tan^{-1}\left( \frac{y''_i - y_r}{x''_i - x_r} \right) \\ \theta''_i - \theta_r \end{bmatrix} \quad (19)$$

$$where:\ r''_i \Rightarrow aligned\ radius, \phi'' \Rightarrow radial\ angle, \vartheta'' \Rightarrow orientation\ difference$$

$$\therefore\ R_{polar} = \{(r_1, \varphi_1, \vartheta_1), \cdots\cdots\cdots, (r_M, \varphi_M, \vartheta_M)\}$$
$$Q''_{polar} = \{(r''_1, \varphi''_1, \vartheta''_1), \cdots\cdots\cdots, (r''_N, \varphi''_N, \vartheta''_N)\} \quad (20)$$

Now, calculate the edit distance between $R_{polar}$ and $Q''_{polar}$ using dynamic programming, and also calculate the matching score:

$$D_{M,N} = \frac{100.K_{pair}}{\max[N,M]} \quad (21)$$

$$where: K_{pair} \Rightarrow no.\ of\ \text{minutiae within bounding boxes of template}$$

$$if\ D_{M,N} > \tau\ then\ fingerprint\_Recognised otherwise not\_recognised \quad (22)$$

## 4. TESTING

The system was designed, built, and tested. Iris images were captured using the system from 50 persons at 2 irises per person. Hence, 100 iris images were captured. Also, the in-built fingerprint scanner was used to capture fingerprints from index and thumb fingers of left and right hands of 50 persons. The total number of fingerprint images captured was 200. The result of the experiment yielded 93% iris recognition rate; and 96% of fingerprint recognition rate.

## 5. CONCLUSIONS

A low cost portable authentication system based on both iris and fingerprint has been developed. The ATM cards contain user's iris and fingerprint templates in addition to the traditional pin with the same level of data protection as the commonly available ATM cards.

## ACKNOWLEDGEMENT

We acknowledge with great appreciation the generous research and development grant received from Federal Government of Nigeria through the STEP-B project to execute this work.

## REFERENCES

Al-ZubiR.T., and Abu-Al-Nadi D.I., 2007. Automated Personnel Identification System based on Human Iris Analysis, *Pattern Analysis Application*, vol.10, pp147-164

Chandan Sharma, and MihirMukerji, 2005, DSP Implementation of Fingerprint-Based Biometric System, Part iv Project Final Report, Department of Electrical & Computer Engineering, The University of Auckland

Daugman J.G., 2004. How Iris Recognition Works, *IEEE Transactions Circuits System Video Technology*, vol.14, no1, pp21-30

Ghassan J. Mohammed, Hong Bing Rong, Ann A., 2009. A New Localization Algorithm for Iris Recognition, *Information Technology Journal*, vol.8, no.2, pp226-230

Jain K., Hong L., Pankanti S., Bolle R., 1997, Online Fingerprint Verification, IEEE transaction Pattern Analysis & Machine Intelligence, vol.19, no.4, pp302-313

Maltoni D., Maio D., Jain A.K., Prabhakar S., 2003, Handbook of Fingerprint Recognition, Springer, New York

Microchip, 2005.Microchip dsPIC30F3013 Digital Signal Controller Datasheet, *Microchip Technology Inc.*

Peter Greczner, Matthew Rosoff, , Networked Biometric Authentication, http://instruct1.cit.cornell.edu/courses/ee476/FinalProjects/s2008/pag42_msr53/pag42_msr53/index.htm ,url visited 10/2/2012.

Wilde R.P., 1997. Iris Recognition: An Emerging Biometric Technology", *Proceeding IEEE* ,vol 85, no. 9, pp1348-1363

Zhang T.Y., and Suen C.Y., 1984, A Fast Parrallel Algorithm for Thinning Digital Pattern, Communications of ACM, vol.27, no.3, pp236-239

# OPEN SOURCE ENTREPRENEURSHIP IN A CASHLESS SOCIETY

**O. Osunade**
Department of Computer Science,
University of Ibadan, Nigeria.
seyiosunade@gmail.com

***ABSTRACT***

*The global recession that started in 2008 has provided an opportunity for people to start their own business. The cashless initiative in Nigeria is a boost for technology entrepreneurs engaged in open source software. Open source software business has the potential to generate profits. There are few organizations engaged in open source software business in Nigeria. As the country goes to a cashless economy will entrepreneurship based on open source software be encouraged? This paper examines the prospects of open source entrepreneurship in a cashless society. The paper uses the qualitative approach to examine the impact of a cashless society on open source entrepreneurship. The paper concludes that open source software business can succeed in a cashless society if the entrepreneur has computing and business skills.*

***Keywords****: open source, entrepreneurship, cashless society, e-commerce, Nigeria*

## 1. INTRODUCTION

The global recession that started in 2008 has provided an opportunity for people to start their own business. For Information Technology professionals, open source software business is an option to explore. Entrepreneurship is providing services and products to customers that achieve goals or make certain activities more convenient to do. Starting a business that offers open source software and related services for the electronic commerce operations in a cashless society requires both computing and business skills. Adeyemo (2005) looked at the implications of Open Source business models in Nigeria. This paper focuses on the impact of starting an open source software business in a cashless society such as the one proposed by Nigeria. With high levels of unemployment in the country and the cashless society initiative by the Central Bank of Nigeria, open source entrepreneurship is a viable option for technically competent Nigerians to engage in.

The cashless Nigeria promoted by the Central Bank of Nigeria will increase the use of electronic commerce in Nigeria. Electronic commerce will be undertaken by individuals and organizations such as government and banks. With the increased use of electronic commerce for daily financial transactions several software solutions will be required for the myriad of operating systems such as Android, Blackberry OS, Apple iOS, Windows and Linux distributions available. Many large organizations, such as Microsoft Inc. and Apple Inc., rely on third party software developers to develop applications for their operating system and hardware. This crowd sourcing approach ensures that well developed and alternative software is available to users. Most open source software is developed by a crowd of software developers. A list of completed and ongoing opens source software can be found at Freshmeat(2012), Sourceforge(2012) and Oslat (2012). This paper focused on how can a society such as Nigeria use this opportunity to promote entrepreneurship.

## 2. LITERATURE REVIEW

Despite the widespread adoption and utilization of Free and Open Source Software (FOSS) in all sectors of life including education, software engineering and IT sectors, public administrations, and within business circles, there still remain widely held concepts or misconceptions of what FOSS is and what constitutes Open Source Software. The misconceptions have hindered the adoption and have made it difficult for businesses to explain to customers that the software and services they are 'selling' or offering is of good quality and may stand at par or even better than proprietary software. There are also confusions with regards to the terminology when different individuals and researchers use the same term to refer to the same concept.

The general concept behind FOSS is that of improving the quality of access to computer programs (GNU, 2012 and Opensource, 2012a). This includes providing a license that reduces limitations for the developer/user and also making the source code accessible to anyone who wants to obtain it. Binaries or executable (machine readable code) are also made available via the Internet and can be downloaded and used.

This means that FOSS can be shared, it can be studied, and it can be modified and adapted by anyone with the appropriate skills. However, this does not mean that FOSS has no owners. FOSS is protected by exactly the same copyright legislation that limits the possibilities of use of proprietary software. However, through FOSS's use licenses, the rights to use, share, study and modify the software are granted. An example of a free software license (Opensource, 2012b) is the GNU General Public License (GPL) that, on top of granting those freedoms, obliges any derivative works produced to keep the same license, and thus remain free.

It is common to think that most of the software written is paid for through sale of the package. However, the real picture is quite different. Most software is written in-house, under contract, and is never commercialized and sold. On the other hand, most companies that do sell packaged software also obtain a proportion of their revenue from service provision. FOSS-based businesses are able to offer services at lower costs, due to the elimination of license fees. This has lead major players like Sun and IBM to embrace FOSS business strategies, but more importantly, it opens the doors for the creation of small FOSS enterprises.

The lowering of costs, together with the possibilities of open access to knowledge and skills that come with FOSS are key aspects of the creation of small enterprises, which can

harness the full power of technology thanks to the availability of the tools, and the possibility to develop the needed skills. In this respect, the value that comes from FOSS is applicable to several different areas:

(i) Selection/Integration: choosing from the myriad of possible FOSS applications and integrating them into a functional platform.
(ii) Basic substitution/migration: the use of FOSS in the IT infrastructure, frequently in substitution of proprietary software.
(iii) New deployment: the introduction of FOSS for a new project internal to the company (adoption).
(iv) Selling services based on a FOSS Project. Service here can start from support, customization, localization or training.
(v) Selling products that contain FOSS as a significant component

FOSS offers opportunities for a wide range of business models. Each model deriving value from the freedom businesses and individuals have in using, modifying, sharing and redistributing legal copies of the software. One element common to all FOSS business models is that more profit is made around services instead of sales of already developed software products.

At the level of service-based business models there is actually little or no significant difference between FOSS business models and proprietary business models. A proprietary software oriented company may give the same quality maintenance services to a client as that provided by a FOSS company. The main difference lies in the way the company generates revenues, how customers benefit from the company's products and services. FOSS provides access to the source code and the right to modify it, proprietary software does not, and the cost model employed. There are also some differences regarding the core capabilities needed to run the business model. FOSS business models require FOSS skills and some interaction with the FOSS community. But there are no necessary differences between FOSS and proprietary business models regarding the partner network, the markets / customers, the distribution channels, the relationship to customers and the management of these relationships.

According to Daffara(2007) the following types of services can be offered by entrepreneurs interested in Open source software business:

(i) Software Selection: Revenue is made in the software selection business model by charging services associated with helping customers select the most appropriate FOSS application for a given task.
(ii) Software Installation: install FOSS for customers who do not possess sufficient skills in the installation and maintenance of FOSS solutions.
(iii) Software Integration: involves charging customers who want certain components to be integrated into their (new or existing) systems.
(iv) FOSS Training: can take many forms ranging from training for certification to training customers in the use of FOSS solutions.
(v) Maintenance and Support: Users need frequent support when the software malfunctions or performs as unexpected.
(vi) Software / Systems Migration: is based on the deep knowledge of both the starting and end information technology environment. Most migration services are based on software packages that help in automating the migration or on pre-configured "packages" of FOSS that provides complete substitutes of proprietary environments.
(vii) Consultancy: takes many forms: ranging from domain name registration, web design and hosting, installation and configuration of learning management systems, to server maintenance and the supply of hardware with Linux (mostly Ubuntu) installed. FOSS consultancy is rarely a standalone business.
(viii) Software Localization and/or Internalization: software is the process of modifying or changing specific parts of the software so that it meets the needs of local markets or customers' requirements.
(ix) FOSS Development and Customization: leverages the internet and a community of volunteers to develop, customize and deploy software of high quality within a shorter development cycle. The software is assumed to be better in quality, responding to different customer demands overtime.
(x) Technical / Legal Certification: involves technical suitability for a purpose carried out by integrators and external consultants, and may come in two shapes: certification of adherence to an international standard and certification of suitability for a specific environment.

Business is both context and product specific. While one kind of business may work in one region or country, the same business may not prosper in another region. The type of product defining ones business also plays an important part in determining whether the business will succeed or not. Thus, when starting a new business, there are many factors to consider, important decisions to be made, rules and procedures to be followed. In simple terms, there is no golden rule one can follow when starting a business.

Most successful businesses start with a good idea. This idea may be your own or may be drawn from any one of a number of available resources. The following resources have been identified as essential components for building an effective business.

(i) Accounting and Finance: The lifeblood of a business is money and a concrete understanding how the finances keep a business afloat is critical to the success of a business. The roles and responsibility of an accountant are given by Todi (2007).

(ii) Business Plan: A business plan is a document that summarizes the operational and financial objectives of a business and contains the detailed plans and budgets showing how the objectives are to be realized. Stutely (2002) listed the following components which should be incorporated into a business plan:

- Executive Summary
- The Industry
- Market Analysis
- Competitive Analysis
- Marketing Plan
- Management Plan
- Operating Plan
- Financial Plan
- Appendices and Exhibits

(iii) Leadership: is the ability to lead a group of followers effectively, make them and the organization successful, and still maintain valid principles and ideals. Leadership plays a vital role in business. The character and approach of people holding responsibility in any business can make an immense impact on the success of the business (Adair, 1988).

(iv) Organizational Structure: The structure of an organization will determine the manner in which it operates and its performance. Structure allows the responsibilities for different functions and processes to be clearly allocated to different departments and employees. The wrong organization structure will hinder the success of the business. Organizational structures should aim to maximize the efficiency and success of the organization. An effective organizational structure will facilitate working relationships between various sections of the organization. It will retain order and command whilst promoting flexibility and creativity.

## 3. METHODOLOGY

This work is based on observation and discussions with participants at an Open Source Training workshop in Abuja, Nigeria between October 20 and November 4, 2011. There were 25 participants from five West African countries: Ghana, Cameroon, Senegal, Nigeria and Togo. Open source software entrepreneurship was discussed in relation to the social, educational, technical, financial, psychological and environmental make up of the individual.

## 4. RESULTS AND DISCUSSIONS

Table 1 gives the distribution of the participants at the Open Source forum in Abuja.

*Table 1: Participant distribution*

| Occupation | Quantity |
|---|---|
| Business owner | 5 |
| IT Instructors | 14 |
| Researchers | 6 |

*Table 2: Participants by country*

| Country | Quantity |
|---|---|
| Ghana | 4 |
| Cameroon | 4 |
| Senegal | 3 |
| Nigeria | 12 |
| Togo | 2 |

This section provides information about open source entrepreneurship and the impact on a cashless society as discussed.

Technical: Starting a business based on open source software requires specialized training in Information Technology. There is a need for programming skills using object oriented languages such as Java, C++, Perl 5 and scripting languages such as Perl and Python. Participative experience in open source software projects is a valuable asset.

The development of technical skills requires time and practice. It involves hard work and continuous technical skill development.

Education: This is the basis on which open source software entrepreneurship is encouraged. It is assumed that a person starting an open source software business has had formal training in computer science or a related field. The formal and informal training a person is exposed to will determine the level of their productivity.

The formal training up to the tertiary level does not emphasize business or open source software skills. Therefore interested persons have to engage in informal training opportunities to bridge their gap in knowledge.

Financial: There is a need to have mastery over finances if a business venture such as an open source software business is to start, survive and flourish. To most entrepreneurs, getting the start-up capital seems to be a problem. However, handling finances for a business involves getting the capital from various sources, using the capital to produce goods and services, making profit from the capital, paying taxes to government and so on. The educational training of most technical entrepreneurs did not include financial management. An accountant can be hired to provide this service.

Social: This is the ability of the entrepreneur to create connections with humans and the community. The connection may come in various forms such as donations, activity sponsorship, grants and scholarships. Understanding the culture of the customers is equally important. Many technology entrepreneurs are not social.

Socially oriented individuals encounter success as entrepreneurs. The few introverts such as Bill Gates of Microsoft Inc., Steve Jobs of Apple Inc. and Mike Lazaridis of Research In Motion Inc had support from socially oriented sub-ordinates or co-founders.

Psychological: deals with how people behave. People's behaviour under situations such as stress, emotional hurt and risk are a factor in their ability to successful start a business. There is risk associated with starting a business in an uncertain business environment. The reaction to risk determines success. Several ways can be used to plan and manage risks associated with starting a business.

Information technology professionals who are in the best position to start open source software business are usually risk averse. Their training requires all variables to be known before execution, but in real life this is not possible.

Personality traits of the individual have an impact on whether they will start a business or not. Extroverts are generally successful at business ventures while introverts are great at research work.

Environmental: this comprises all aspects of the individual such as religion, training, societal values, practices and regulations. It is the way of life of a group of people. The impact of culture on entrepreneurship in Nigeria can be felt as follows

(i) A graduate of any tertiary institution is expected to get a white-collar job
(ii) Only those who are semi-literate or incompetent own businesses
(iii) Those employed make more money than those who are self-employed
(iv) The benefits of employment far outweigh the advantages of self employment
(v) Self employment is seen as a temporary status until a white-collar job is secured
(vi) Most religion support trading for profit or community good
(vii) Training institutions in Nigeria provide skills required by white collar jobs. A shift is ongoing to provide entrepreneurial training as part of the curriculum.
(viii) The regulations governing business transactions are not well defined in Nigeria

The expectations of the community from a graduate is high, thus pressure is put on the graduate to seek a secured source of income instead of engagement in entrepreneurial business. It takes three to five years for a business to become stable and profitable. The entrepreneur will need support during this time which the community may not be able to provide.

There are many aspects to the business operating environment such as agreements, product specifications, copyright laws, intellectual property rights, payment channels, customer identification, taxation, competitors, import/export regulations and security. In recent times the business environment has gone through a lot of challenges that make being an entrepreneur unattractive. The current business environment has increased the risks associated with starting a business.

## 5. CONCLUSION

Open source entrepreneurship has a role to play in a cashless society. A cashless society will promote electronic commerce. The services offered electronically will support the use of both proprietary and open source software. To successful operate in a cashless society individuals and organizations require technical skills especially computing and business. Organizations offering open source services can prosper in a cashless society with the right use of tools, intellectual protection and strategies.

## ACKNOWLEDGEMENT

The author would like to acknowledge the Open Source Foundation in Nigeria (OSFON) and the ict@innovation FOSS Train-the-Trainers programme on Open Source Software Business Models.

## REFERENCES

GNU, (2012). Philosophy of the GNU Project. Available at: http://www.gnu.org/philosophy/. Accessed January 24, 2012.

Opensource, (2012a). Open Source Definition. Available at: http://www.opensource.org/docs/osd Accessed January 24, 2012.

Opensource, (2012b). Open Source Licenses. Available at: http://www.opensource.org/licenses/alphabetical Accessed January 24, 2012.

Daffara, C. (2007). "Business models in FOSS-based companies" Available at: http://fosstoolkit.iosnasean.net/index.php?title=6._FLOSS-based_business_models . Accessed January 28, 2012.

Todi, B. (2007).Cost Benefit Analysis-whether you should outsource your Bookkeeping to Professional Book Keeper. Available at: http://www.articlesbase.com/business-articles/cost-benefit-analysiswhether-you-shouldoutsource-your-bookkeeping-to-professional-book-keeper-114351.html. Accessed January 28, 2012.

Adair, J. (1988). Effective Leadership. Published by Gower Publishing, United Kingdom. Pages 5 – 7.

Stutely, R. (2002). The Definitive Business Plan. Published by FT Prentice Hall, United Kingdom. ISBN 978-0-273-71096-7.

Freshmeathttp://freshmeat.net/.Accessed January 28, 2012.

Sourceforgehttp://sourceforge.net/.Accessed January 28, 2012.

Osalt: Open source alternatives to commercial software http://www.osalt.com/. Accessed January 28, 2012.

Adeyemo, A.B. (2005). The Open Source Business Model and its Economic Implications for Nigeria and other Third World Economies. Journal of Information Technology Impact, 5(3):121-128

# A FLEXIBLE ENVELOPE SYSTEM FOR TRACKING AND REPORTING OVERSPENDING IN CASHLESS TRANSACTIONS

**Laud Charles Ochei**
Department of Computer Science
University of Port Harcourt
Port Harcourt, Nigeria
*laudcharles@yahoo.com*

**Longe Olumide**
Fulbright SIR Fellow & Research Scholar
Southern University System
Southern University
Baton Rouge
Louisiana, USA.
*longeolumide@fulbrightmail.org*

***ABSTRACT***

*One area of personal, governments, and corporate finance that rightfully gets a lot of attention is budgeting. This is the art of directing how funds should be used. The Central Bank of Nigeria recently proposed that most expenditure be done using a cashless option. The challenge with adopting the cashless options for transactions is the susceptibility to overspending. Studies have shown that it is very easy to spend more than what your budget allows when you are not counting out the actual cash and seeing the hard earned money leave your hands. Merely controlling how to use cash is not a budget tool, there is the need to use flexible budgeting systems that allow citizens to track expenditures, and get report on transactions that may lead to overspending. In this paper, we propose a flexible envelope system for tracking and reporting overspending in cashless transactions. This proposed system used a three-prong approach which incorporates-(1) creating pretend account envelopes; (2) creating special checking account envelopes for charging items; and (3) regular checking of running balance of each envelope. An algorithmic framework is presented for the flexible envelope system which can be integrated within any application designed for personal budgeting as well as for governments and organizations.*

***Keywords****: envelope, budget, tracking, SOA, overspending, cashless*

## 1. INTRODUCTION

Budgets are a necessary part of modern life- especially for any person or group of persons that have financial goals and if there is a desire to balance your income with your spending.

Years ago, households and companies, and governments were limited to spending only the physical money that they had. Without physical cash in the hand, it was nearly impossible to purchase anything. There was no requirement to keep a written or electronic record of inflow or outflow.

Today, we have a harder time keeping track of our money because cash is no longer required for most transactions, and many of us are finding it difficult to use cash anymore (Foreman, 2012). This is commonly referred to as cashless society.

A cashless society is a culture where no one uses cash, all purchases being made are by credit cards, charge cards, cheques, or direct transfers from one account to another through mobile banking and other electronic means. The cashless society envisioned refers to the widespread application of computer technology in the financial system (NSACC, 2012).

It is common to see how quickly spending can pile up with credit card. Swiping plastic is an incredibly easy and painless way to buy stuff.

The problem many people have with cashless options for transactions is overspending. It is very easy to spend more than what your budget allows when you are not counting out the actual cash and seeing the hard earned money leave your hands. The "I will pay it later" is much easier than saving money for the expensive purchase, and most of the time, sometimes comes up that prevents us from paying it completely when "later" actually arrives. One report suggests that people spend ten to twenty percent more money when using a credit card (or other similar options) versus cash (Stew, 2012).

Financial planners have long encouraged people to avoid credit-card purchases as a way to save money. This is because several studies in the past have suggested that less transparent payment forms(such as credit cards) tend to be treated like(play) money and are hence more easily spent (or parted with)," the researchers argue (LiveScience, 2011).

A flexible budget system is the only real way to keep track, and prevent overspending in the cashless transactions.

In this paper we modified the conventional envelope budgeting system so as to accommodate today's cashless transactions and also track and report possible transactions that may lead to overspending.

## 2. LITERATURE REVIEW

In this section we will look at the background of the cashless policy, the benefits, and the fears of Nigerians as regards its implementation.

## 2.1 ADVANTAGES OF THE CASHLESS POLICY IN NIGERIA

The cashless policy was expected to commence on January 1, 2012. The Central Bank of Nigeria, CBN, has reeled out final operational guidelines (which can be obtained from the CBN website) for the implementation of the cashless policy. Kingsley Omose in an article published by Elombah.com has also provided practical tips on the implementation of the cashless policy by the CBN (Omose, 2011).

The Managing Director/CEO of eTranzact International Limited, Mr. Valentine Obi said that cashless transactions were viable and more secured mode of payment in any economy (NSACC, 2011).

This latest development, according to the apex financial regulatory authority is coming on the heels of increasing dominance of cash in the economy with its implication for cost of cash management to the banking industry, security, money laundering, among others.

"About two years ago, a World Bank study revealed that about $10 billion cash transactions that move just between Nigeria, Ghana and Cote de Ivoire shows no clue about how it comes and how it goes. The transactions were not recorded or reported anywhere in our system. So government can't even plan based on that. Cash based economy encourages money laundering activities.

The benefits of a cashless society to banks and merchants include larger customer coverage, reduction in cost of operations, international products and services promotion and branding, increase in customer satisfaction and personalized relationship with customers, and easier documentation and transaction tracking. To the government, it aids adequate budgeting and taxation, improves regulatory services, improves administrative processes, and reduces cost of currency administration and management.

To the customer, it aids convenience, as it is available 24 hours a day and seven days of the week. It also helps reduce transfer costs and processing fees; supports multiple payment options; and also facilitates immediate notification of all transactions on customer's account platform (Global Press Institute, 2011).

In the wider society, effective implementation of the policy would curb corruption in all forms of transactions. The expert also expressed optimism that Nigeria would truly move on progressively as a cashless society (NSACC, 2011).

Each year, nearly 3 million Americans are victims of crimes in which criminals target cash, according to extrapolated statistics from the U.S. Bureau of Justice Statistics. All over the world, cab drivers, convenience-store clerks, bank tellers, and others who deal almost exclusively in cash are accosted daily and often murdered, simply because they possess currency, and the impact of these crimes resonates throughout society (Warwick, 2004).

Making cash electronic has the potential of making workplaces and crime-ridden neighborhoods safer, reducing prison populations, and freeing up emergency rooms. It could bring down insurance rates, cut public outlays for law enforcement and courts, and much more. If drug crimes and tax evasion, both of which are conducted almost exclusively in cash, are included in the calculations, the fiscal relief could run as high as a trillion or more dollars each year(Warwick, 2004).

In spite of the numerous advantages highlighted above, many people in Nigeria agree that there is need to educate people on the policy and evaluate its effects during the pilot run. So far, many Nigerians say they are still wary of the new policy, citing concerns over the current deficiencies in the banking sector, such as ATM malfunctions and poor Internet services (Global Press Institute, 2011).

## 2.2 OVERSPENDING IN CASHLESSPOLICY

Most of the transactions are done with cashless options and there is potential to overspend. It is a fact that most of us are beginning to move away from cash for everyday spending; the convenience of debit and credit cards is very tempting. Some cards actually offer rewards or cash back that makes the use of cash even less appealing. The problem with this convenience is that you can begin to forget the true value of the money you are spending and end up having trouble staying within your limits. This is what leads to overspending (Vohwinkle, 2011).

Most of us still rely on keeping enough cash on hand or carefully balance your checkbook each day, the act of spending money meant you had to do a little planning and some simple math. Now, all you have to do is swipe your debit card like you would a credit card and the funds are electronically whisked out of your account. When you are not physically handing someone money or a check for a purchase, it can almost feel as if you are not spending money at all.

## 2.3 BUDGETING SYSTEM

One area of personal, governments, and corporate finance that rightfully gets a lot of attention is budgeting, the art of directing how your money should be used.

A budget (from old French bougette, purse) is a financial plan and a list of all planned expenses and revenues. It is a plan for saving, borrowing and spending (Wikipedia, 2012). In fact, budgeting in its general sense is the act of quantifying objectives in financial terms. An article published by Accountnextdoor.com explores the functions of budgeting in a modern and forward looking business in a simple and non-technical manner (Accountantnextdoor.com, 2011).

There is a direct relationship between effective budget implementation and national development; complete budgeting protocol entails effective planning, monitoring, and implementation of recurrent and capital proposals. With a population of about 150m, ineffective budget monitoring and implementation still remains the biggest challenge to Nigeria's economic and socio-infrastructural rejuvenation. Budgeting culture in Nigeria mostly begins and end with planning alone (Gwegwe, 2010).

It is even more worrisome that most of our expenditures (in government and private sectors) are now made using cashless options. The issue therefore is how to track our cashless expenditures and still know how much balance have left in the budget.

Although, there are several budget management tools, most of these tolls are designed specifically for a particular organization, group for people or purpose.

There are several electronic payment solutions and budget management tools within and outside the country. An example is the eTA, a comprehensive budget management tool developed for the National Institute of Health (NIH), a component of the U.S. Department of Health and Human Services. This is a user-friendly, web-based system covering key parts of the extramural business process related to grant and financial management (eTA, 2012).

In Nigeria, several electronic payment solutions such as CashEnvoy and eTranzact have emerged in last few years. While CashEnvoy is basically a web payment platform (Global Press Institute, 2011), eTranzact is a multi-channel electronic payment system that facilitates real time settlement of financial transaction using Internet SMS, WAP, Voice XML and bank outlets (NSACC, 2011).

Merely controlling how to use cash is not a budget tool, we need to use a proper budgeting system that will allow us to track our expenditures, and also track and report transaction that may lead to overspending.

In order to accommodate today's nearly cashless society, a number of budgeting systems have been introduced, but many of them use after the fact reconciliation methods (Smith, 2012).

There are several ways to budget; these include line item budget, envelope budget, percentage budget, cash budget, capital budget, event budget and category budget. One of the easiest budgeting systems is the envelope system, an "active" process that works by assigning income to various virtual "containers." (Kulicki, 2012) In this paper we seek to make it more flexible in order to accommodate the cashless nature of today's transactions so that it will be an effective tool in tracking and reporting suspicious transactions that may lead to fraud and overspending.

## 2.4 THE CASHLESS POLICY VERSUS ENVELOPE BUDGETING

The envelope system relies on a series of envelopes, hence its name, to budget and each envelope contains a fixed amount of money for that expense. An example would be an envelope for groceries, where all grocery expenditures would come from that envelope. If an envelope is depleted, the funds must come from another envelope in the system.

One of the biggest advantages of the envelope system is that it is a tool that helps to check and prevent overspending. It restricts how much you can spend from both an individual category perspective (each envelope) and a monthly total perspective (all the envelopes). When an envelope runs out, you can only pull funds from another envelope, which limits how much you can spend each month.

Empirical studies shows that when people do transactions using a cashless options such as credits cards, Visa card, western union, ATM cards, they tend to spend more because it is difficult to track their expenses on a regular basis.

In this paper we propose to develop an algorithm that can be integrated in any budgeting application for tracking and reporting suspicious transactions that may lead to overspending.

This algorithm will make the envelope system more flexible because it includes components that address the shortcomings of the traditional envelope system while still retaining its advantages for use in cashless transactions.

For example, the major drawback of the envelope budgeting is that you have less information about your spending. You know you spent N500 on "feeding" last month. Assuming that you want to cut back, it will be difficult since you did not track your spending, by default. You need to know how much you spend on restaurants, beverages, drinks etc. We will address this problem by making sure that once an amount has been assigned to an envelope, any amount deducted from that envelope is assign a unique ID to ensure proper monitoring and tracking of the expenditure. In our implementation, the database that supports this system allows us to handle as many envelopes that we want.

From implementation standpoint, our flexible envelope system will be anchored on three major components to track and report overspending- (1) use of a checking account, (2) use of a pretend envelope, and (3) use of a running balance

## 3 THE PROPOSED SYSTEM

We looked at this flexible envelope system in two directions: an SOA-based system and a conventional web-based system.

### 3.1 SOA-BASED SYSTEM

In this direction we looked at the flexible envelope system as a service-oriented architecture based system. Service Oriented Architectures (SOA) are a way of developing distributed systems where the components of these systems are stand-alone services (or web services) (Sommerville, 2007).

SOA is a flexible set of design principles used during the phases of systems development and integration in computing. A system based on a SOA will package functionality as a suite of interoperable services that can be used within multiple separate systems from several business domains. Figure 1 illustrates how web services are used.

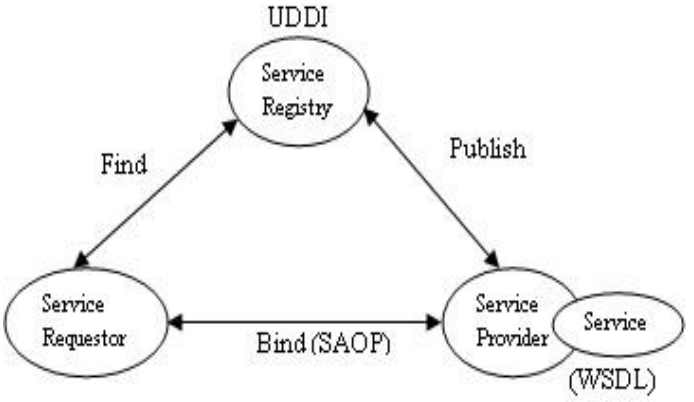



*Figure 1: The conceptual architecture of a service-oriented architecture (Sommerville, 2007)*

This flexible envelope system will make it easy for people to track their spending and prevent overspending. As a result the system will be interoperable and flexible. Services that

target other features that will improve the system can still be added- tracking overspending, computing balance, creating and charging items to a checking account, can be easily implemented in the system and they are flexible to be used by other authorized services or systems.

In this paper, an architecture which can be later developed into a fully functional system is presented. The proposed system is basically a layered architecture. The figure 2 shows the conceptual diagram of the system as a set of fundamental services for tracking and reporting overspending in Cashless transactions. The services in the internal structure are organized in a set of four (4) layers which consist of - the User Interface layer, Budget services layer, Overspending Tracking Services layer, and Repository Services layer.

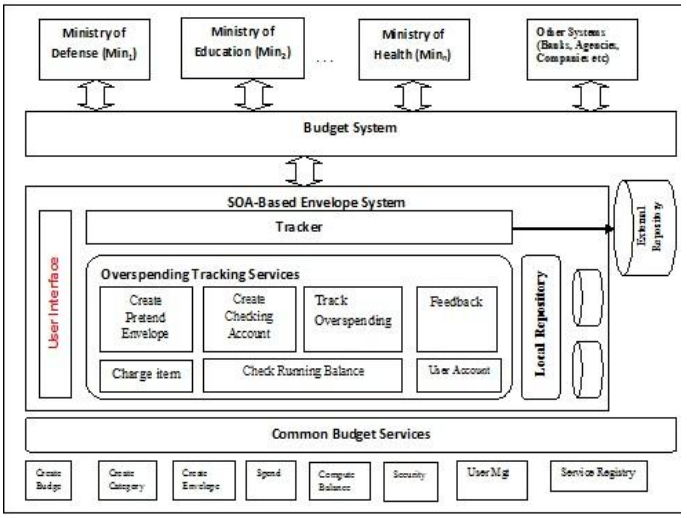



*Figure 2: Conceptual SOA-based Envelope System Architecture*

The process of designing an SOA-based system for tracking and reporting overspending in cashless transactions starts from the point that any functionality that the system has, should be implemented as a service. The whole system itself also should be considered as a service, realizing the global idea that it can be plugged to any type of system which would like to use some of its functionalities. These systems will also use the system as a service. The system will have both an external and internal structure. The Internal structure is the flexible SOA-based envelope system itself while the external structure controls other components that interact with the SOA-based envelope system.

The overspending tracking services layer will contain a set of services that work together to support the control and track overspending in cashless transactions. The group of common budget services (outside the internal structure) is a set of services that may be found in any budget system or any other system that has budgeting functionality. The Repository services layer (local and external) contains the various data sources that provide the resources that are being accessed. The Tracker service acts as an adviser. It also advises and coordinates the operation of other services and also helps to search for content either in the local or external repository. The User Interface layer provides a flexible platform for connecting with the overspending tracking services. The modules of the overspending tracking service are charge item, create checking account, track overspending, check running balance and feedback provision (for personal, private and public organizations).

This architecture will provide a good foundation for a system that needs services for use in tracking and reporting overspending. This architecture will make sharing and exchanging of services that will prevent overspending easier. As a result the system will be interoperable and flexible. Other services can be easily implemented in the system and they are flexible to be used by other authorized services or systems.

### 3.2 CONVENTIONAL WEB-BASED SYSTEM

In this direction we look at the flexible envelope system as traditional three-tier web-based application architecture. In this paper, we used discovery prototyping as an alternative to system modeling as a way of representing the system that we want to design. Prototyping is used to build the inputs and output that will help in constructing the underlying database and the programs for inputting and outputting data to and from the database (Whitten et al, 2004). Figure 3 represents a context data flow diagram used to document the scope of the system.

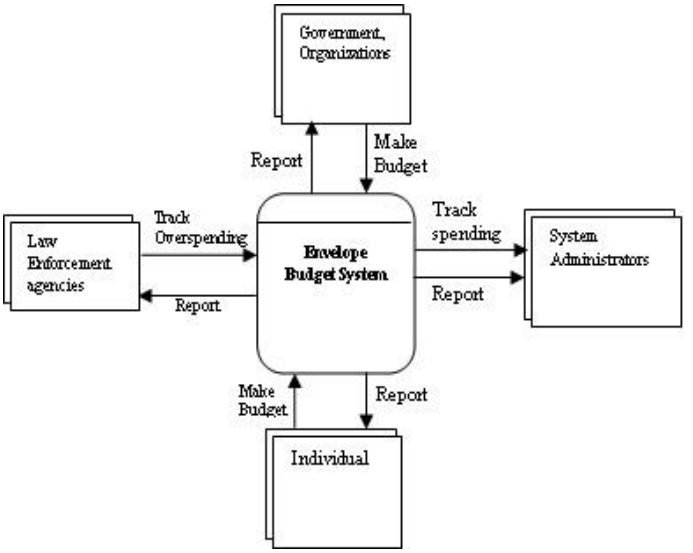



*Figure3:. Context Data Flow diagram*

Figure 3 is a context data flow diagram that shows how the flexible envelope system interact with several components such as individuals, governments, governments/organizations and law enforcements agencies, to create budget, view reports and track overspending. We also developed an algorithm described below and a flowchart (figure 4) which captures other functionalities of the system for tracking and reporting overspending and other fraudulent activities in cashless transactions.

**Algorithm**

(i) Start
(ii) Make Budget
(iii) Create Category
(iv) Create envelope

(v) Enter spending details

(vi) Check running balance(RunningBal) for the envelope

(vii) If (**RunningBal**< 0)

**Halt Spending and Notify Administrator**

Chose spending option

If option =1 then

Goto step 5

Else

Create checking account

Charge item to checking account

(viii) Else If (**RunningBal**>= 0)

Chose spending option

If option =1 then

Spend from the envelope

Else

Create checking account

Charge item to checking account

Spend

(ix) Compute balance

(x) Check budget expiration

(xi) If budget has expired ( **BudgetEnddate > CurrentDate)**

Compute balance for each Envelope

Transfer all balance in each envelope to savings account

(xii) Else If budget has not expired GOTO Step5

(xiii) Compute Budget Difference

(xiv) End

Figure 4 shows the flowchart of the process of tracking and reporting overspending.

### 3.3 TECHNIQUE FOR TRACKING OVERSPENDING

The system checks overspending by computing what we call the running of each envelope once the spending details have been entered into the system.

Assuming a user intends to spend N700 on item1 which falls under an evelope1. Envelope1 has N500 balance. The running balance which is -200 is less than zero (that is 500-700).

When this happens, the system halts spending on that particular envelope whose running balance is less than zero, and then notifies the administrator or the authorities about an attempt to over spend. Thereafter, the system presents two options to the user to proceed with the transaction. We will explain with a simple example.

When using the first option, the user has to review the spending details by bringing down the amount to spend on item1 or re-enter spending details for a fresh item whose running balance will be less than zero. In using the second option, the user has to charge an item to a special checking account. This is done by creating a unique ID for a checking account and a charged item. This accountID is tied to a specific chargeditemID. The checking account maintains the actual amount of the item to charge, the current account balance of the account and the envelopeID from which the item was charged from. The item is then charged from each envelope in the budget to the checking account until the

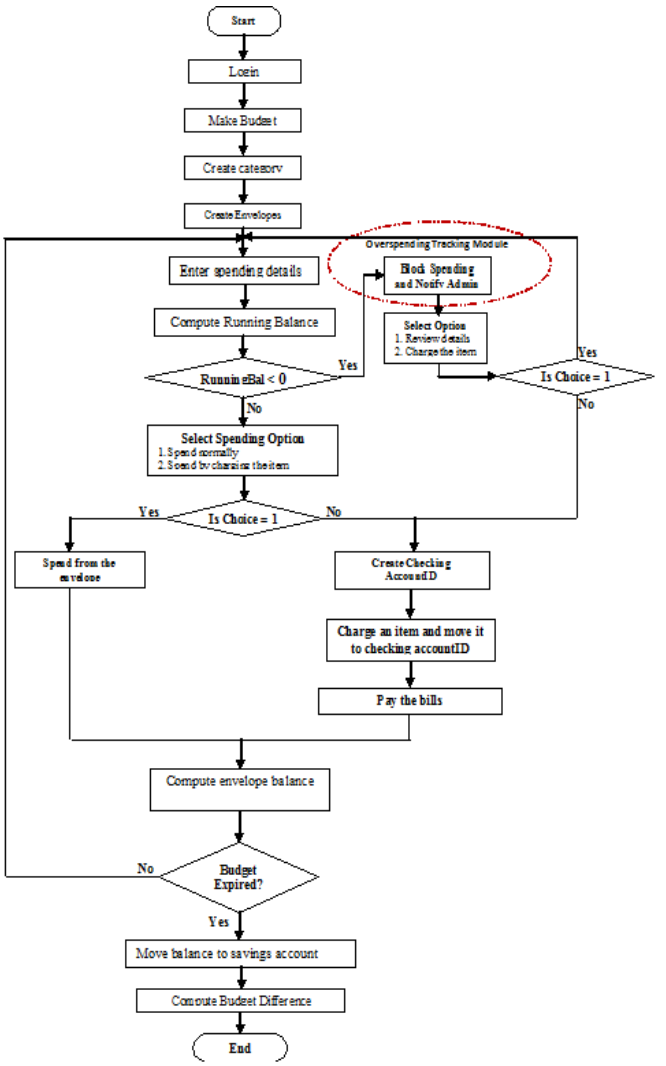



*Figure 4: Flowchart for controlling and tracking overspending*

Accountbalance is greater than or equal to ActualAmt. Once this is done, item can now be spent in the normal way. It should also be noted that this is the second option ordinarily which a user can choose from if he/she decides to charge the item to a special checking account.

### 3.4 DATABASE DESIGN

Microsoft Access 2007 is used to create the database for this application. The relationships between the tables of the database (EnvelopeSystem.mdb) are shown in Figure 5. The basic table is – Budget, Category, PretendEnvelope,CheckignAccount, ChargedItem, Spend, RunningBalance. All other tables are either temporary or supportive in nature.

## 4.0 IMPLEMENTATION AND RESULT

We implemented the Flexible Envelope System (FeS)– using the following tools and technologies:

(i) Operating system – Windows 7

(ii) Web Server – ASP.NET Development Server

(iii) Web Browser – Mozilla Firefox (for testing the application during development)

(iv) Server and Client scripting language – Visual C# 2010
(v) Database Management System – Microsoft Access 2007
(vi) Database Access method – ActiveX Data Object (ADO)
(vii) Development tool – Microsoft Visual Studio 2010(the main development tool is Visual Web Developer 2010)

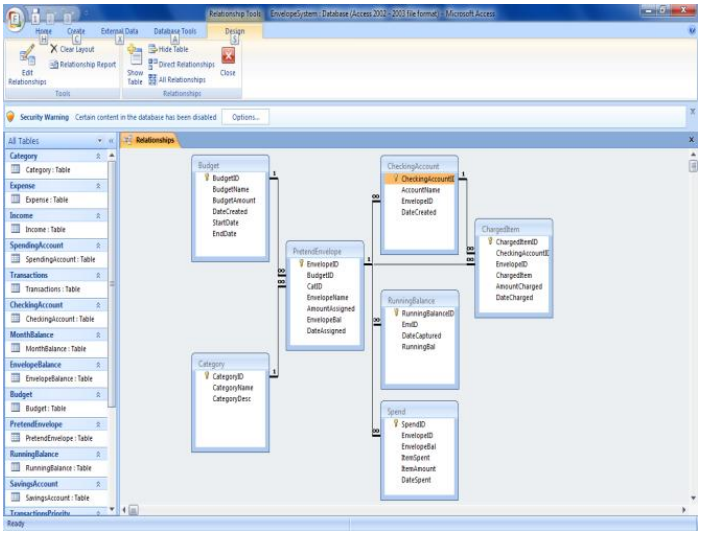


*Figure 5: Relationships between tables of the EnvelopeSystem.mdb database*

### 4.1 DESCRIPTION OF THE FLEXIBLE ENVELOPE SYSTEM (FES)

The home page is accessed when the user first browses to the application. The home page has four major tasks:

(i) Checks whether a session variable is available to indicate a UserID
(ii) If the UserID exists, looks up information from the database and displays the page in personalized mode.
(iii) If no UserID exists, present options to look up the UserID or create a new one
(iv) Allows the entry of UserID and then answers a security question to obtain a password reminder

A session variable is a global variable that is accessible by any page in the current Web directory. By setting a session variable in the login script to indicate that the visitor has logged in all pages can check this variable to determine whether or not to permit access to a page (Adams, 2000).Figure 6 shows the screenshot of the home page.

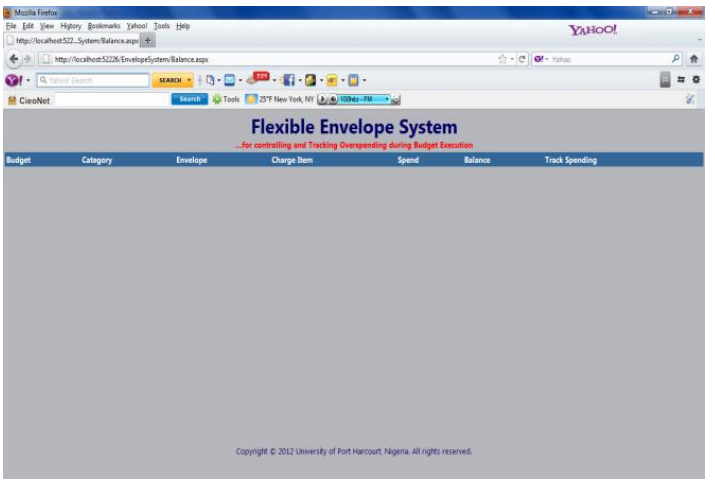



*Figure 6: The Home page of FeS*

There are five basic modules in the design. These include: Budget, Envelope, Charge item, Spend, Balance and Track spending.

(v) Creating the budget – this entails creating the budget. In creating a budget, you supply certain details as shown in Figure 7.

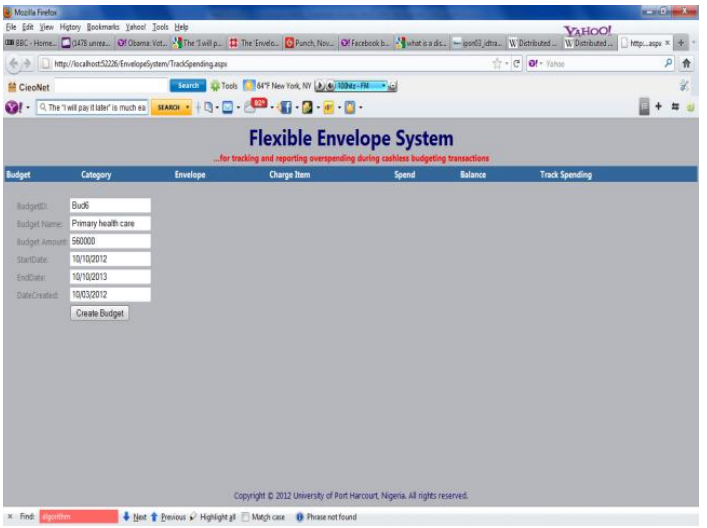



*Figure 7: Creating a budget in FeS*

(vi) Creating Envelope- this entails creating an envelope from the different budget categories that exist. One of the envelopes to be created is the checking account envelope for charging items. This is one of the features that we have introduced to make the envelope system to handle cashless transactions.
(vii) Tracking Spending-this entails selecting one the several parameters available for use in tracking overspending. It is possible to use the system to track spending by date, envelope, charged item etc.

### 4.2 RESULTS

We created five budgets, five categories, and ten envelopes. Thereafter we made 20 different transactions

(expenditures) at random targeting different envelopes. To examine the effectiveness of our system we generated a report at regular intervals (monthly) and at the expiration of the budget duration (i.e., the end of the financial year). Specifically, we checked and compared the running balance for each envelope and the budget against the initial amount assigned to the envelopes and the entire budget.

Simulation results show that for each budget (and the individual envelopes), the total running balance plus the total expenditure equals the total amount that was initially assigned to the each budget (each envelopes).

We also examined the reports and messages sent to notify the administrator of any potential transaction that may lead to overspending. The expenditures for different budgets can be collected overtime and these data can be examined and the spending patterns studied carefully to further give an insight into those areas that are vulnerable to overspending and possible fraud. Thereafter the system can be modified to check and identify such pattern/traits and report accordingly anytime they appear.

## 5.0 CONCLUSION

This Flexible Envelope System has been tested at the level of the design and it was found to be satisfactory. This system can be used by individuals, organizations, and governments can use the system to control and track expenditure.

Application of this system will make it easier to automatically track transactions due to the fact that you can know where money was going, how much was left, and how long it needed to last. Most governments and corporations will be very successful at making smart and sound decisions when they know how much is left to spend.

The single most serious challenge for implementing the flexible Envelope system is convincing the organizations and governments to subject their budgets to this system for scrutiny to see if it meets the standards set. A good legislation is also required to ensure that all budgets are subjected to scrutiny on this system and the results presented to the public or at least the stakeholders of the business for consideration.

## REFERENCES

Accountantnextdoor.com(2010): Budgeting: What are the functions of budgeting? Investments and Business Accountants. Retrieved on January 4, 2012 from http://www.accountantnextdoor.com/budgeting-what-are-the-functions-of-budgeting/

Adams, David R(2006): ASP.NET 2.0 Tutorial. Retrieved on January 30, 2008 at http://msconline.maconstate.edu/tutorials/ASPNET20/default.htm

eTA(2012): Electronic Tracking and Analysis (eTA). Office of Extramural Research at the National Institutes of Health (NIH), U.S. Department of Health and Human Services. Retrieved on January 4, 2012 from http://era.nih.gov/nih_and_grantor_agencies/award/eRA_eTA.cfm

Foreman, G. (2012): The 'Envelope System' In a Cashless Society. AllThingsFrugal.com. Retrieved on January 9, 2012 from http://www.allthingsfrugal.com/f.envelope.htm

Warwick D. (2004): Toward a Cashless Society. The Futurist, July-August 2004 Vol. 38, No. 4

Global Press Institute(2011): Nigerians Debate Pros and Cons of New Cashless Policy. Retrieved on January 4, 2012 from http://www.globalpressinstitute.org/global-news/africa/nigeria/nigerians-debate-pros-and-cons-new-cashless-policy?page=2

Gwegwe, K(2010): Improved Budget Implementation: Key To Nigeria's Recovery. FocusNigeria.com. Retrieved on January 4, 2012 from http://www.focusnigeria.com/budget-implementation.htm

Kulicki, W. (2011): What Type of Budget Do You Use? Fiscal Fizzle. Retrieved on January 9, 2012 from http://www.fiscalfizzle.com/2011/04/types-of-budgets/

Livescience(2008): Study: Credit Card cause more spending . Retrieved on January 4, 2012 from http://www.livescience.com/2849-study-credit-cards-spending.html

NSACC (2011): Imperatives of advancing a cashless Nigeria. Nigerian South African chamber of commerce. Retrieved on January 23, 2012 from http://nsacc.org.ng/imperatives-of-advancing-a-cashless-nigeria/

Omose, K(2011): Practical Tips on the Cashless Policy. Elombah News. Retrieved on January 4, 2012 from http://www.elombah.com/index.php?option=com_content&view=article&id=9246:practical-tips-on-the-cashless-policy&catid=25:politics&Itemid=92

Smith S. (2012): Envelope Budgeting in a Cashless Society.Crown Financial Ministries.Retrieved in April 12, 2012 from http://www. crown.org/conference/NCS2012/

Sommerville, Ian(2007): Software Engineering(Eight Edition).Pearson Education Limited, Harlow, England

USAID(2005): USAID/Nigeria Budget Process Support Project. Technical Assistance Project Funded by United States Agency for International Development Contract # PCE-I-00-00-00015-0, Task Order # 6. Retrieved on January 4, 2012 from http://pdf.usaid.gov/pdf_docs/PDACF588.pdf

Wang, J(2012): Brief Look at Five Budgeting Systems. Bargaineering.com. Retrieved on January 9, 2012 from http://www.bargaineering.com/articles/brief-look-at-five-budgeting-systems.htm.

Vohwinkle, J(2011): Try Using Cash to Keep Spending Under Control. The Convenience of Cards Can be Costly but Cash Can Help. About.com Guide. Retrieved on January 24, 2012 from http://financialplan.about.com/od/budgetingyourmoney/a/usecash.htm

Whitten, Bentley, and Dittman(2004): Systems Analysis and Design(Fifth Edition). Irwin/McGrawHill companies Inc. New York. USA.

Wikipedia (2012): Budget. Wikimedia Foundation Inc. Retrieved on January 4, 2012 from http://en.wikipedia.org/wiki/Budget

# RETAIL ELECTRONIC BANKING QUALITY (EBQ) IN NIGERIA: A PERFORMANCE EVALUATION

**Olayinka David-West**
Lagos Business School, Pan-African University
ydavid-west@lbs.edu.ng

***ABSTRACT***

*The introduction of electronic banking services is one of the initiatives propelling the shift into a cashless economy. However, whilst the adoption of information and communications technologies (ICTs) is prevalent, they are subject to service failures and customer disappointments that jeopardise the effectiveness of Nigeria's cashless initiatives. This paper evaluates consumer perceptions of electronic banking performance using quality as a proxy defined through a 10-dimensional and 35-item scale, EBQUAL. A survey of bank customers comprising of electronic banking users in Lagos and Borno States was conducted to measure electronic banking quality (EBQ) across EBQUAL dimensions – acceptability, accessibility, competence, convenience, reliability, responsiveness, security/privacy, access to support, availability of support, and usability. Using multiple criteria decision analysis (MCDA) techniques, an industry performance score of 56% was derived. The results show that whilst electronic banking services can be improved, the EBQUAL dimensions and scale items can guide electronic banking providers and regulators in the design and development of improvement mechanisms.*

***Keywords:*** *electronic banking, evaluation, quality, MCDA, Nigeria*

## 1. INTRODUCTION

The commoditisation of computers and availability of high-speed networks has altered the manner in which business services are delivered, hence altering the service encounter and service delivery process. Using self-service technologies (SSTs), Internet-based tools like websites, and mobile communications networks, organisations are utilising electronic methods to aid service delivery and augment traditional methods. The introduction of technology, whilst reducing the interaction between employees and customers, adds new complexities to service management and service quality as these complexities are evidenced by new services interactions (customer-technology, firm-technology and employee-technology) that need to be taken into consideration (Parasuraman, 2000a; Parasuraman, 2000b). In addition, the active role of the customer in the creation of the service presumes customers have prerequisite technology knowledge and skills.

The service benefits availed through the deployment of information and communication technology (ICT) has been widely adopted by banks and extended to customer domains using SSTs such as automated teller machines (ATMs), point of sale (POS) terminals, Internet-accessible bank accounts, etc. These implementations have extended banking operational hours and reduced the security risks associated with holding cash. In spite of these advantages, electronic banking services are plagued with operational problems including ATM disbursement errors, electronic fraud, and slow recovery and problem resolution processes. These challenges combined with the occasional forfeiture of funds have made customers cautious in their adoption of e-banking services. To foster adoption, banks introduced monetary penalties for low-valued services such as over the counter (teller) cash withdrawals that can be fulfilled by ATMs. To enhance the perception of e-banking services, the Central Bank of Nigeria (CBN), published additional operational guidelines and mandatory initiatives to curb extant operational challenges and enhance service quality. These include call centres, installation of cameras at ATMs, replacement of magnetic stripe cards for chip-based cards, and the adoption of payment card industry data security standards (PCIDSS). Furthermore, cautionary security mechanisms such as ATM screens, pin-pad screens, etc. have been implemented to augment security. Whilst these initiatives specifically target certain challenges, improve service delivery, and quality; they are unsupported by empirical consumer analysis akin to consumer studies. In spite of these extant challenges, the CBNs bid to reduce cash management costs in favour of electronic transactions guarantees increased transaction volumes amidst hypothetical problem solutions. This paper presents the results of a consumer evaluation of electronic banking quality (EBQ) using constructs specifically formulated to local challenges experienced in an era of growing electronic transactions.

Quality, "the lifeblood that brings increased patronage, competitive advantage, and long-term profitability" (Clow and Vorhies, 1993), has been a priority for business managers; drawing significance from various disciplines including marketing, operations, and human behaviour. Service quality or the overall quality of the services industry or service-based processes, is "the degree of discrepancy between customers' service perceptions and expectations" (Zeithaml and Parasuraman, 2004). The evaluation of service quality not only offers a construct for the assessment of the consumer gap, but insights into service improvement initiatives. Though it can be argued that comparable ICTs are deployed in developed and developing economies and studies instigated in Western societies are applicable in other contexts; discrepancies in societal, cultural, and environmental norms and the socio-technical nature of ICT systems should not be underestimated. These differences, observed in the few service quality studies conducted in developing countries, provides insurmountable evidence that cultural perspectives impact the conceptualisation of service quality. As such, the adoption of quality dimensions based on the developed countries context

is problematic and the alteration of research instruments to the context has been proposed (Angur et al., 1999; Greenland et al., 2006; Imrie et al., 2002; Raajpoot, 2004). This study seeks to measure consumer perceptions of electronic banking quality (EBQ) using a 10-dimensional and 35-item scale called EBQUAL (David-West, 2012) comprising of dimensions - acceptability, accessibility, competence, convenience, reliability, responsiveness, security/privacy, access to support, availability of support, and usability. The EBQ analysis employs multiple criteria decision analysis (MCDA) techniques where an option is chosen from a set of alternatives characterised by multiple, conflicting criteria (Stewart, 1992; Xu and Yang, 2001). The remainder of this paper is set out as follows. Section 2 provides a literature review identifying extant dimensions of quality and measurement frameworks originating from developing and developed countries prior to introducing the EBQUAL scale. Section 3 presents the method used to address the research question, and Section 4 outlines the results of the research. Section 5 discusses the results and implications for future research prior to the presentation of conclusions.

## 2. LITERATURE REVIEW

### 2.1 ELECTRONIC BANKING

Prior to the Internet explosion that extended the reach of services outside the organisation using ICTs, banking services were delivered by traditional brick and mortar structures and intra-organisational technology applications to reduce operational costs and increase revenues (Furst et al., 2002). However, attempts to enhance customer convenience (Furst et al., 2002) in this information intense industry (Economist Intelligence Unit and KPMG Professional Services, 2000) resulted in the adoption of electronic strategies and systems. SSTs extend the application of ICTs beyond back office automation to the delivery of banking services using electronic communication networks complemented by access devices. SSTs comprise any technology interface that enables a customer to produce and consume services without direct assistance from firm employees (Meuter et al., 2000) and have been available to banking since the installation of the first ATM in 1970. The commercialisation of the Internet and the significant growth in Internet users (Miniwatts Marketing Group, 2010) expanded the domain of SSTs to include the Internet, an emerging business platform. In the context of financial services, e-business is defined as "*anywhere/anytime banking and brokerage*" (Nemzow, 2000). However, the narrow scope of e-business in banking (electronic banking) is challenged by Enders et al. (2006) who suggest that banks need to offer more services (outside banking) to qualify as an e-business, a view supported by Beynon-Davies (2004) and Boyes and Stone (2003) in their classification of e-business opportunities in banking by product, channel, risk and markets. Therefore, e-business in the banking industry goes beyond electronic banking and includes the various technology-related transformation initiatives deployed to elevate the bank into an e-enterprise (Daniel and Wilson, 2003; Earl, 2000; Enders et al., 2006) through transformation initiatives cutting across the enterprise and its customers, employees, and suppliers or partners and enhancing market, intra-organisation, and inter-organisation relationships respectively.

### 2.2 ELECTRONIC SERVICE QUALITY EVALUATION

Electronic service quality or e-service quality (ESQ) refers to quality of service in electronic environments such as those facilitated through the Internet, high-speed networks and electronic channels/devices. The relative novelty of this domain, employing technology in service delivery, has resulted in a lag between technological advancements and academia. Attempts to bridge the knowledge gap in service quality literature has predominantly focused on website quality (Barnes and Vidgen, 2002; Collier and Bienstock, 2006; Cristobal et al., 2007; Liu and Arnett, 2000; Loiacono et al., 2000; Madu and Madu, 2001; Santos, 2003; Van Riel et al., 2003; Webb and Webb, 2004; Wolfinbarger and Gilly, 2003). However, the multi-product and multi-channel nature of electronic banking systems warrants an extension of the analytic scope of electronic systems beyond websites and web-based transactions (Rust and Kannan, 2003; Zeithaml et al., 2002). Although constructs for the general evaluation of electronic services are evolving, (Cox and Dale, 2001; Dabholkar, 1996; Parasuraman et al., 2005; Zeithaml et al., 2000), these do not eliminate calls for a multi-channel conceptualisation of service quality (Sousa and Voss, 2006).

*i. Electronic Service Quality Measures*

Service quality evaluation measures have been dominated by the 5-dimensional RATER (reliability, assurance, tangibles, empathy, and responsiveness) scale known as SERVQUAL (Parasuraman et al., 1988). In the electronic domain, the exchange of traditional SERVQUAL attributes, empathy and tangibles, for information and technology-relevant dimensions that take the remote self-service nature of these transactions into consideration has resulted in a new set of dimensions such as interactivity, navigability, speed, design, information quality, security, and trust. The variability identified in the measurement of service quality across industries, channels (traditional and electronic), and countries is also prevalent in electronic service (ESQ) and banking (EBQ) quality studies. However, although the measurement of traditional service quality has been well established by SERVQUAL, equivalent measurements in the electronic space are emerging, albeit mostly focusing on e-commerce (retail) and web-based activity, with relatively few generic measures of e-service quality. Whilst some researchers have risen to this challenge (Broderick and Vachirapornpuk, 2002; Jun and Cai, 2001; Parasuraman et al., 2005; Yang et al., 2004), the comparative pace of ICT development vis-à-vis the generation of scholarly research still leaves a gap in the knowledge of the phenomenon where like SERVQUAL, contextual differences in the dimensions can be assumed (Robledo, 2001).

*ii. Electronic Banking Service Quality Measures*

In banking, variability in measurement dimensions is evidence of a lack of consensus in the measurement of bank service quality (BSQ) and the applicability of SERVQUAL, which

has resulted in the development of alternative scales more suited to the industry. As such, BSQ constructs that accommodate human-service delivery elements (Aldlaigan and Buttle, 2002; Avkiran, 1994; Johnston, 1995) omitted by SERVQUAL have emerged. The behavioural SQ dimension in the Aldlaigan and Buttle's SYSTRA-SQ scale (1996), staff conduct and communication from Avkiran (1994), and attentiveness/helpfulness, care, communication, competence, and courtesy from Johnston (1995) represent the human-service elements. Other unique dimensions include the service portfolio representing the range of services offered (Bahia and Nantel, 2000), and organisational social image (social responsibility) (Sureshchandar et al., 2003). The increased use and emphasis of technology in the provision of banking services through SSTs and electronic channels has also led to the examination of service quality determinants. However, differences in delivery channels/technologies ranging from Internet/online banking (Broderick and Vachirapornpuk, 2002; Joseph et al., 1999; Jun and Cai, 2001; Yang et al., 2004) to portals (Bauer et al., 2005) and channels like the telephone and ATMs, have resulted in the identification of a diverse set of dimensions to date. In assessing the impact of automated service quality, Al-Hawari and Ward (2006) identified quality attributes of each automated service (product). Montoya-Weiss et al. (2003) in their study used a relational and multichannel approach to formulate measures of service quality. A summary of extant EBQ attributes is illustrated in Table 1.

*Table 1: Summary of bank service quality constructs*

| Author(s) | Dimensions |
|---|---|
| Al-Hawari and Ward (2006) | ATM – five items, telephone banking – six items; Internet banking – seven items. |
| Bauer et al. (2005) | Security & trust, Basic services quality, Cross-buying services quality, Added values, transaction support, Responsiveness |
| Broderick and Vachirapornpuk (2002) | Customer expectations, Image & reputation of the service organisation, Aspects of the service setting, Actual service encounter, Customer participation |
| Joseph et al. (1999) | Convenience/accuracy, Feedback/compliant management, Efficiency, Queue management, Accessibility, Customisation |
| Jun and Cai (2001) | Customer service quality: Reliability, Responsiveness, Competence, Courtesy, Credibility, Access, Communication, Understanding the customer, Collaboration, Continuous improvement; Banking service product quality: Product variety/diverse features; Online systems quality: Content, Accuracy, Ease of use, Timeliness, Aesthetics, Security |
| Kassim (2005) | Internet/Telephone/SMS, Personnel assistance, Instructions, ATM machines, Functionality of ATM machines |
| Montoya-Weiss et al. (2003) | Website Design Factors: Navigation structure, Information content, Graphic style; Customer Evaluations: Service quality – online channel and alternative channel, Risk perception |
| Phillips Consulting (2001a; 2001b) | Aesthetics, technical aspects, website content, e-financial services, customer experience, performance |
| Woldie et al. (2008) | Reliability, assurance, responsiveness |
| Yang et al. (2004) | Reliability, Responsiveness, Competence, Ease of use, Security Product Portfolio |

### 2.3 SERVICE QUALITY IN DEVELOPING COUNTRIES

Although tenets of service quality have also been extended to electronic retail (Zeithaml et al., 2000), electronic channels (Al-Hawari and Ward, 2006; Loiacono et al., 2000), and Internet banking (Broderick and Vachirapornpuk, 2002), the duplicity of measures due to channel and/or service differences has contributed to the diverse range of electronic service constructs evolved in more advanced economies. However, the converse persists as a double-edged sword in developing economies, especially African countries such as Nigeria that are not only underserved in research outputs (Boateng et al., 2009; Greenland et al., 2006; Sureshchandar et al., 2003), but where adoption of these electronic environments is being embraced by businesses, albeit with low subscription rates. In sum, evidence corroborating the evolving nature of developing country research in the electronic domain presented by Boateng et al. (2008; 2009) is validated by limited adoption (Aghaunor and Fotoh, 2006; Akinci et al., 2004; Okunoye et al., 2007; Olatokun and Igbinedion, 2009) and evaluation (Andoh-Baidoo et al., 2007; Bello, 2005; Woldie et al., 2008) studies published. The documented experiences from developing countries studies also emphasise the impact of environmental (e.g. legal systems), infrastructural (e.g. power and telecommunications), and societal (e.g. societal adoption and acceptance of technology) systems on evaluation measures.

#### *2.3.1. The EBQUAL Scale*

EBQUAL (David-West, 2012) is a 10-dimensional and 35-item scale representing consumer perceptions of EBQ in Nigeria. EBQUAL, developed for the sole purpose of evaluating consumer perceptions of electronic banking quality, evolved after a mixed methods study comprising of exploratory qualitative studies and scale development processes. Due to the novelty of electronic banking in Nigeria, EBQUAL uses a 7-point uni-polar scale with a neutral midpoint and agreement and likelihood responses ranging from strongly disagree to strongly agree and very unlikely to very likely respectively.

## 3. METHOD

Survey research techniques that support the collection and analysis of large sets of quantitative data collected from multiple subjects are appropriate for the evaluation of consumer perceptions of EBQ. Survey research is common in social science disciplines such as marketing, organisational theory (Hinkin, 1995) and information systems (Grover and Lee, 1993; Pinsonneault, 1993). Survey research methods have also been applied in the development of consumer measurement constructs of technology readiness (Parasuraman, 2000b) and electronic/technology service quality (Bauer et al., 2005; Parasuraman et al., 2005; Zhang and Prybutok, 2005). Even though statistical analyses methods are common to survey research, multiple criteria decision analysis (MCDA) techniques, facilitated by a Windows application, Intelligent Decision Systems Multiple Criteria Assessor (IDS), used to score EBQ.

### 3.1. SAMPLING

The sample population comprised of debit card holders (bank customers issued with debit cards) and users of electronic banking channels like ATMs and POS terminals and Internet-enabled devices to conduct financial and non-financial transactions such as funds transfers/purchases and enquiries. To avoid bias in customer selection, bank assistance and permissions were not sought in the acquisition of respondents. Thus, with the assistance of three enumerators, purposive sampling techniques were employed in the administration of 900 paper surveys. The surveys were distributed for self-administration in two Nigerian states: Lagos and Borno. Unlike urban Lagos, Borno provides a distinct contrast with respect to access and quality of telecommunications, a prerequisite for any electronic banking activity. The survey was administered between the months of October and December 2010 using street intercept techniques combined with drop-off and pick up procedures within business locations (office or educational institutions), shopping centres, and places of worship were used in Lagos. In Borno, on the other hand, the survey was administered to undergraduate students of mixed gender, ethnicity and ages in their third and fourth years of study at the department of Accountancy, University of Maiduguri. The surveys were administered in a classroom setting in which they were completed and returned to facilitate instrument return and retrieval.

### 3.2 RESEARCH PROCESS

The seven-step research process employed in the MCDA analysis of EBQ is discussed in the subsequent paragraphs.

*Model Problem*: This multi-step activity transforms the EBQ evaluation into a multiple-criteria decision problem by defining: 1) options to be evaluated (alternatives); 2) values against which the evaluation will take place (criteria); 3) key stakeholders; and 4) internal and external uncertainties (Belton and Stewart, 2002).

*Build Attribute Hierarchy*: The EBQ attribute hierarchy is a three-tier representation of the EBQUAL scale. The first level represents the overall score; the second level, criteria (constructs/dimensions); and the third level attributes. The attribute hierarchy is then specified into an IDS-project file. Using the IDS attribute definition dialog, node attributes (level 3) were created and labelled using equivalent survey statements. Second level criteria were created and labelled as EBQUAL dimensions. This was followed by the assignment of data ranges to the attributes and dimensions. Node-level attributes were defined using the 7-point survey scale whilst a 5-point scale corresponding to performance grades of poor, adequate, good, very good, and excellent was used for first- and second-level attributes. An inbuilt IDS mechanism to convert scale grades, synonymous with mapping the 7-point grades defining the bottom-level attributes to the second-level 5-point grades were specified using either rule- or utility-based methods that allocate grades within a value space of [0,1], where 1 represents the most favourable outcome and 0 the least (IDS Limited, 2005).

*Capture Individual Responses (Data)*: The form-based interface of IDS was used to capture data from survey responses. Data acquired from individual surveys were equivalent to decision alternatives and attributes to survey questions. Input assessments for each attribute permitted the entry of belief degrees for one or more grades. The belief degree is a subjective probability associated with the strength that the assessment judgement is supported and should total 1 or less. IDS processes attributes where the belief degree is less than 1 indicating that there is missing information and the effects of the missing information is analysed and revealed in outcomes generated (IDS Limited, 2005). Responses were captured by bank and later aggregated for industry analysis resulting in 23 IDS files, corresponding to the banks.

*Assign Weights*: Assigning relative importance weights to attributes is a feature supported by IDS to ensure importance ascribed to attributes are taken into consideration during the scoring process. The weights used in this study were obtained from the average importance scores within the survey.

*Aggregate Responses*: The IDS modelling feature was used to create a group alternative entry representative of all the alternatives within that bank group. Each group aggregate was subsequently added to a new IDS file with the alternatives being bank aggregate scores.

*Report Results*: An overview of the decision model and summary report that includes alternative rankings based on utility scores and performance profile distribution is the main IDS output. In addition, graphical representations are generated per alternative and/or attribute depending on the level of analysis desired.

*Sensitivity Analysis*: IDS permits the use of sensitivity analysis techniques in the evaluation of performance variations based on changes in weights and input data. Various sensitivity analyses were conducted to assess the impacts of various scenarios on the scores and ranks generated.

## 4. RESULTS AND DISCUSSIONS

The study population comprised of 739 respondents from Lagos and Borno States of which 32 respondents completed only the demographic sections failing to respond to any of the survey questions. As such, these were eliminated from the IDS analysis that was conducted with 707 responses; however, the

survey instruments were retained for future reference. The survey respondents varied in age and educational qualifications. Male respondents were in the majority with a representation of 68.5%, female respondents 29.9% and unknown of 1.6%. Although twenty-two banks were named, the distribution of responses by bank varied from 1 (lowest) to 135 (highest); with 81 unspecified.

### 4.1. INDUSTRY EBQ PERFORMANCE

The IDS evaluation of the 707 EBQ responses resulted in an aggregate score of 56.41% (Table 2). The convenience dimension reported the best performance scores (71%) and usability the poorest (41%). The performance of the convenience dimension can be associated with the general benefits derived from electronic banking when compared with traditional banking services that are evident in access 24/7/365. The sizeable investments in the provision of electronic channels may also explain the performance of the accessibility dimension (68%). The grade distribution shown in Figure 1 illustrate 13.03% of EBQ was adjudged poor, 19.20% average, 15.20% good, 29.17% very good, 20.87% excellent, and 2.53% unknown. These results shows that even with an average EBQ score of 56.41%, about one third of overall grades (32.23%) are below average indicating the capacity for performance improvements.

*Table 2: EBQ Performance Scores by Dimension*

| Dimension | Weight | |
|---|---|---|
| | Zero | Importance |
| Security/trust | 0.6458 | 0.6458 |
| Convenience | 0.7088 | 0.7069 |
| Usability | 0.4091 | 0.4091 |
| Accessibility | 0.6824 | 0.6824 |
| Availability | 0.5188 | 0.5188 |
| Reliability | 0.5533 | 0.5533 |
| Competence | 0.5229 | 0.5229 |
| Support Access | 0.5305 | 0.5305 |
| Acceptance | 0.4655 | 0.4655 |
| Responsiveness | 0.5469 | 0.5469 |
| Industry performance | 0.5641 | 0.5640 |

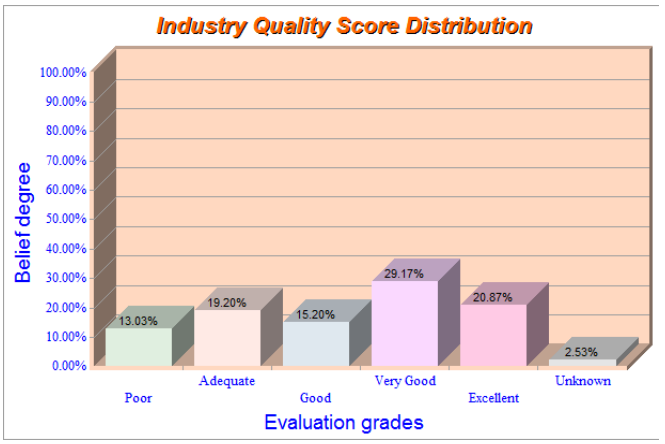



*Figure 1: EBQ Score Distribution (IDS-generated)*

#### 4.1.1. *Impact of Uncertainties Weights*

Using the average importance scores of all 707 responses analysed by dimension as weights in the MCDA model, a slightly varied electronic banking performance score of 56.38% is computed. Compared to the performance score of 56.41% using the zero weight value of 1.0 per dimension, the importance-weight score differences illustrated in Table 2 are somewhat negligible (-0.0001 or 0.01%). While the exact cause of this insignificance is unknown, it may be attributed to the immature development of expectations in electronic environments (Parasuraman et al., 2005; Zeithaml et al., 2000) and the elimination of importance averages (weights) in the analysis of EBQ performance. The decomposition of the zero weight and importance weight grades demonstrate that whilst 50% of the respondents perceive EBQ as above average (very good and excellent), 33% (poor and adequate) perceive the quality as below average. This view of evaluation grades provides a detailed view of how the final score was composed and serves to helps banks better understand the sentiment of consumers globally and across dimensions.

#### 4.1.2. *Sensitivity Analyses*

The sensitivity analyses features of IDS can aid in what-if scenario analysis that can identify gaps or improvement areas. The IDS application supports sensitivity analyses by evaluating weight and data changes. Whilst the descriptions of the analyses conducted in the formation of improvement strategies are inexhaustible, examples of the application of sensitivity analyses to weights, policy and benchmarking problems.

*Weight Sensitivity:* Similar to the importance weight scores, the application of importance weights on rank performance have no impact.

*Data Sensitivity:* Evaluated using the attribute, "merchants prefer cash to e-payments", that indicates the reluctance of merchants to electronic payment transactions as an example. This is a current policy challenge being addressed by the CBN through restrictions in cash withdrawal limits in a bid to promote electronic transactions through acceptance by merchants (Central Bank of Nigeria, 2011). Evaluating the possible impact of this policy using IDS is possible through data sensitivity analysis where the impact of modifications to the belief degree using the embedded data editor immediately visualise the effect of the change. Using the data sensitivity dialog to alter the industry belief degree altered the attribute score from 37% to 80% and the overall industry score to from 56.41% to 58.83% indicating that the implementation of policy change and increased merchant acceptance of electronic payments will positively impact electronic banking performance.

## 5. LIMITATIONS, FUTURE RESEARCH AND CONCLUSION

Given the population of the Nigeria, the sample employed may be considered a limitation, but may also be an opportunity for further research. Additional further research studies that



can emanate from this include the statistical analysis of the survey results, analysis by location, and bank EBQ performance benchmarking.

With an average industry performance score of 56%, where weights or missing values (uncertainties) had little impact and scores showing more weaknesses than strengths, it is evident that the electronic banking industry is in need of improvement. The IDS analysis also showed similar performance scores across banks, representing a lack of differentiation in the delivery of electronic banking services. Thus, it can be concluded that in its present state, electronic banking services cannot be deemed strategic and do not offer competitive advantage. The analytical prowess of IDS is demonstrated in its evaluation of uncertainties, identification of strengths and weaknesses, sensitivity analyses, and numerical and pictorial outputs that have served as techniques in the formulation of improvement strategies. In summary, the EBQUAL scale offers banks in emerging markets such as Nigeria an assessment tool and the ability to measure electronic banking performance towards the improvement of cashless services in banking. In addition, the IDS workbench provides electronic banking service providers the opportunity to conduct multi-tier analysis of EBQ performance results for the design of appropriate and effective improvement strategies.

**REFERENCES**

Aghaunor, L. & Fotoh, X., 2006. Factors Affecting Ecommerce Adoption in Nigerian Banks, *Jonkoping International Business School*.

Akinci, S., Aksoy, S. & Atilgan-Inan, E. 2004. Adoption of Internet banking among sophisticated consumer segments in an advanced developing country. *International Journal of Bank Marketing,* 22**,** pp.212-232.

Al-Hawari, M. & Ward, T. 2006. The effect of automated service quality on Australian banks' financial performance and the mediating role of customer satisfaction. *Marketing Intelligence & Planning,* 24**,** pp.127-147.

Aldlaigan, A. & Buttle, F. 2002. SYSTRA-SQ: a new measure of bank service quality. *International Journal of Service Industry Management,* 13**,** pp.362-381.

Andoh-Baidoo, F., Osatuyi, B., Muhammadou, K. & Aidoo, E. 2007. An Assessment of Electronic Banking Initiatives in Nigeria. *In:* Americas Conference on Information Systems (AMCIS), 2007 Keystone, Colorado.

Angur, M., Nataraajan, R. & Jahera Jr, J. 1999. Service quality in the banking industry: an assessment in a developing economy. *International Journal of Bank Marketing,* 17**,** pp.116-125.

Avkiran, N. 1994. Developing an instrument to measure customer service quality in branch banking. *International Journal of Bank Marketing,* 12**,** pp.10-18.

Bahia, K. & Nantel, J. 2000. A reliable and valid measurement scale for perceived service quality of banks. *International Journal of Bank Marketing,* 18**,** pp.84-91.

Barnes, S. & Vidgen, R. 2002. An Integrative Approach to the assessment of e-commerce quality. *Journal of Electronic Commerce Research,* 3**,** pp.114-127.

Bauer, H. H., Hammerschmidt, M. & Falk, T. 2005. Measuring the quality of e-banking portals. *International Journal of Bank Marketing,* 23**,** pp.153-175.

Bello, A., 2005. The Impact of E-banking on Customer Satisfaction in Nigeria. mpra.ub.uni-muenchen.de. Available at: http://mpra.ub.uni-muenchen.de/23200/1/The_Impact_of_E-banking_on_Customer_Satisfaction_in_Nigeria.pdf [Accessed November 21, 2010].

Belton, V. & Stewart, T.J., 2002. *Multiple Criteria Decision Analysis: An Integrated Approach*, Dordrecht: Kluwer Academic Publishers.

Beynon-Davies, P. 2004. *E-Business,* Basingstoke, Palgrave Macmillan.

Boateng, R., Hinson, R., Heeks, R. & Molla, A. 2008. E-commerce in Least Developing Countries: Summary Evidence and Implications. *Journal of African Business,* 9**,** pp.257-285.

Boateng, R., Molla, A. & Heeks, R., 2009. E-Commerce in Developing Economies: A Review of Theoretical Frameworks. In K. Rouibah, O. E. M. Khalil, & A. E. Hassanien, eds. *Emerging Markets and E-Commerce in Developing Countries*. IGI Global.

Boyes, G. & Stone, M. 2003. E-business opportunities in financial services. *Journal of Financial Services Marketing,* 8**,** pp.176-189.

Broderick, A. & Vachirapornpuk, S. 2002. Service quality in Internet banking: the importance of customer role. *Marketing Intelligence & Planning,* 20**,** pp.327-335.

Buttle, F. 1996. SERVQUAL: Review, critique, research agenda. *European Journal of Marketing,* 30**,** pp.8-32.

Central Bank of Nigeria 2011. Penalty for Non-Compliance with CBN Circulars and Guidelines on ATM Operations in Nigeria. *In:* Banking and Payments Department (ed.). Abuja: Central Bank of Nigeria.

Clow, K. & Vorhies, D. 1993. Building a competitive advantage for service firms: measurement of consumer expectations of service quality. *Journal of Services Marketing,* 7**,** pp.22-32.

Collier, J. & Bienstock, C. 2006. Measuring Service Quality in E-Retailing. *Journal of Service Research,* 8**,** pp.260-275.

Cox, J. & Dale, B. 2001. Service quality and e-commerce: an exploratory analysis. *Managing Service Quality,* 11**,** pp.121-31.

Cristobal, E., Flavián, C. & Guinaliú, M. 2007. Perceived e-service quality (PeSQ). *Managing Service Quality,* 17**,** pp.317-340.

Dabholkar, P. 1996. Consumer evaluations of new technology-based self-service options: An investigation of alternative models of service quality. *International Journal of Research in Marketing,* 13**,** pp.29-51.

Daniel, E. M. & Wilson, H. 2003. The role of dynamic capabilities in e-business transformation *European Journal of Information Systems,* 12**,** pp.282-296

David-West, O. 2012. *An Assessment of Electronic Banking Performance in Retail Banking.* DBA, University of Manchester.

Earl, M. 2000. Evolving the E-Business. *Business Strategy Review,* Vol. 11**,** pp.33 - 38.

Economist Intelligence Unit & Kpmg Professional Services 2000. The e-business Value Chain: Winning strategies in seven global industries. The Economist.

Enders, A., Jelassi, T. & Harald, B. 2006. From E-Banking to E-Business at Nordea Bank. *MIS Quarterly Executive,* Vol. 5**,** pp.31-42.

Furst, K., Lang, W. & Nolle, D. 2002. Internet Banking. *Journal of Financial Services Research,* Vol. 22**,** pp.95-117.

Greenland, S., Coshall, J. & Combe, I. 2006. Evaluating service quality and consumer satisfaction in emerging markets. *International Journal of Consumer Studies,* 30**,** pp.582-590.

Grover, V. & Lee, C., 1993. Analyzing methodological rigor of MIS survey research from 1980-1989. *Information & Management*, pp.305–317.

Hinkin, T. 1995. A Review of Scale Development Practices in the Study of Organizations. *Journal of Management,* 21**,** pp.967-988.

Ids Limited 2005. IDS Multicriteria Assessor Manual.

Imrie, B., Cadogan, J. & Mcnaughton, R. 2002. The service quality construct on a global stage. *Managing Service Quality,* 12**,** pp.10-18.

Johnston, R. 1995. The determinants of service quality: satisfiers and dissatisfiers. *International Journal of Service Industry Management,* 6**,** pp.53-71.

Joseph, M., Mcclure, C. & Joseph, B. 1999. Service quality in the banking sector: the impact of technology on service delivery. *International Journal of Bank Marketing,* 17**,** pp.182-191.

Jun, M. & Cai, S. 2001. The key determinants of Internet banking service quality: a content analysis. *Marketing,* 19**,** pp.276-291.

Kassim, N., 2005. E-banking service quality: gaps in the Qatari banking industry. Journal of Internet Banking and Commerce, 10(2). Available at: http://www.arraydev.com/commerce/JIBC/2005-08/KassimTry.asp [Accessed August 28, 2010].

Liu, C. & Arnett, K. 2000. Exploring the factors associated with Web site success in the context of electronic commerce. *Information & Management,* 38**,** pp.23-33.

Loiacono, E., Watson, R. & Goodhue, D. 2000. WebQual: A Measure of Website Quality. *Working Paper.*

Madu, C. & Madu, A. 2001. Dimensions of e-quality. *International Journal of Quality & Reliability Management,* 19**,** pp.246-258.

Meuter, M., Ostrom, A., Roundtree, R. & Bitner, M. 2000. Self-Service Technologies: Understanding Customer Satisfaction with Technology-Based Service Encounters. *The Journal of Marketing,* 64**,** pp.50-64.

Miniwatts Marketing Group. 2010. *World Internet Usage and Population Statistics* [Online]. Available: http://www.internetworldstats.com/stats.htm [Accessed 31 March 2011].

Nemzow, M., 2000. The E-Business Agenda. Journal of Internet Banking and Commerce, Vol. 5(Iss. 1). Available at: http://www.arraydev.com/commerce/JIBC/0001-02.htm [Accessed August 28, 2010].

Montoya-Weiss, M., Voss, G. & Grewal, D. 2003. Determinants of Online Channel Use and Overall Satisfaction With a relational, Multichannel Service Provider. *Journal of the Academy of Marketing Science,* 31**,** pp.448-458.

Okunoye, A., Bada, A. & Frolick, M. 2007. IT Innovations and E-Service Delivery: An Exploratory Study. *In:* Proceedings from the 9th International Conference on Social Implications of Computers in Developing Countries, Jul 7 2007 São Paulo, Brazil. pp.1-8.

Olatokun, W. & Igbinedion, L. 2009. The Adoption of Automatic Teller Machines in Nigeria: An Application of the Theory of Diffusion of Innovation. *Issues in Informing Science and Information Technology,* 6**,** pp.373-393.

Parasuraman, A. 2000a. Superior Customer Service and Marketing Excellence: Two Sides of the Same Success Coin. *Scienza & Business, Roma***,** pp.23-30.

Parasuraman, A. 2000b. Technology Readiness Index (TRI): A Multiple-Item Scale to Measure Readiness to Embrace New Technologies. *Journal of Service Research,* 2**,** pp.307-320.

Parasuraman, A., Zeithaml, V. & Berry, L. 1988. SERVQUAL: A Multiple-Item Scale For Measuring Consumer Perception. *Journal of Retailing,* 64**,** pp.12-40.

Parasuraman, A., Zeithaml, V. & Malhotra, A. 2005. E-S-QUAL: A Multiple-Item Scale for Assessing Electronic Service Quality. *Journal of Service Research,* 7**,** pp.213-233.

Phillips Consulting Limited, 2001a. Website Effectiveness: Financial Institutions Wakeup. Available at: http://s105583270.websitehome.co.uk/ratings/articles/pdf/articlead.PDF [Accessed August 28, 2010].

Phillips Consulting Limited, 2001b. Website Effectiveness: The Case of Nigerian Banks. Available at: http://s105583270.websitehome.co.uk/ratings/articles/pdf/synopsis1.pdf [Accessed August 28, 2010].

Pinsonneault, A., 1993. Survey research methodology in management information systems: an assessment. *Journal of Management Information Systems*, pp.75–105.

Raajpoot, N., 2004. Reconceptualizing service encounter quality in a non-western context. *Journal of Service Research*, 7(2), pp.181–201.

Robledo, M. 2001. Measuring and managing service quality: integrating customer expectations. *Managing Service Quality,* 11**,** pp.22-31.

Rust, R. & Kannan, P. 2003. E-Service: A New Paradigm For Business in the Electronic Environment. *Communications of the ACM,* 46**,** pp.36-42.

Santos, J. 2003. E-service quality: a model of virtual service quality dimensions. *Managing Service Quality,* 13**,** pp.233-246.

Sousa, R. & Voss, C. 2006. Service Quality in Multichannel Services Employing Virtual Channels. *Journal of Service Research,* 8**,** pp.356-371.

Stewart, T. 1992. A critical survey on the status of multiple criteria decision making theory and practice. *Omega,* 20**,** pp.569-586.

Sureshchandar, G., Rajendran, C. & Anantharaman, R. 2003. Customer perceptions of service quality in the banking sector of a developing economy: a critical analysis. *International Journal of Bank Marketing,* 21**,** pp.233-242.



Van Riel, A., Semeijn, J. & Janssen, W. 2003. E-service quality expectations: a case study. *Total Quality Management & Business Excellence,* 14**,** pp.437-450.

Webb, H. & Webb, L. 2004. SiteQual: an integrated measure of Web site quality. *The Journal of Enterprise Information Management,* 17**,** pp.430-440.

Woldie, A., Hinson, R., Iddrisu, H. & Boateng, R. 2008. Internet banking: an initial look at Ghanaian bank consumer perceptions. *Banks and Bank Systems International Research Journal Volume 3, Issue 3, 2008 Special Issue on Small Business Finance and Banking Services of Emerging and Developing Countries***,** pp.35-46.

Wolfinbarger, M. & Gilly, M. 2003. eTailQ: dimensionalizing, measuring and predicting etail quality. *Journal of Retailing,* 79**,** pp.183-198.

Xu, D. L. & Yang, J. B. 2001. Introduction to multi-criteria decision making and the evidential reasoning approach. *Manchester School of Management*.

Yang, Z., Jin, M. & Peterson, R. 2004. Measuring customer perceived online service quality. *International Journal of Operations & Production Management,* 24**,** pp.1149-1171.

Zeithaml, V.A., Parasuraman, A. & Malhotra, A., 2000. *A Conceptual Framework for Understanding E-service Quality: Implications for Future Research and Managerial Practice*, Cambridge, Marketing Science Institute.

Zeithaml, V., Parasuraman, A. & Malhotra, A. 2002. Service Quality Delivery through Web Sites: A Critical Review of Extant Knowledge. *Journal of the Academy of Marketing Science,* 30**,** pp.362-375.

Zeithaml, V. A. & Parasuraman, A. 2004. *Service Quality,* Cambridge, Marketing Science Institute.

Zhang, X. & Prybutok, V. 2005. A Consumer Perspective of E-Service Quality. *Engineering Management, IEEE Transactions on,* 52**,** pp.461-477.

**APPENDIX 1**

1. Banks protect e-banking systems from illegal use.
2. Banks protect customers information from intruders.
3. Bank employees can be trusted.
4. Banks detect fraudulent e-banking system activities.
5. Banks validate e-banking transactions before processing.
6. Banks advise customers of new e-banking developments.
7. E-banking system operations are slow.
8. E-banking system operations are irregular.
9. E-banking services are active within minutes of sign-up.
10. E-banking systems are easy to use.
11. E-banking systems meet customers needs.
12. E-banking systems are good value for money.
13. Customers can contact any branch for e-banking issues.
14. Customers can contact the bank at any time.
15. Banks advise customers of e-banking system failures.
16. E-banking systems are out of reach after banking hours.
17. E-banking devices are difficult to find.
18. ATMs never have cash.
19. Banks provide on-line tutorials for new e-banking users.
20. Banks provide printed help for new e-banking users.
21. Merchants prefer cash to e-payments.
22. Customers are uncomfortable with e-banking technologies.
23. Bank staff have little knowledge of e-banking terms and conditions.
24. Bank staff have insufficient knowledge to solve e-banking problems.
25. Bank staff insufficient knowledge to innovate new e-banking systems.

When there is an e-banking problem...

26. I am ignorant of what to do.
27. I am ignorant of who to contact.
28. I have difficulty contacting the bank.

When I complain, bank staff are...

29. Unbelieving.
30. Impolite.
31. Apologetic.
32. Helpful.
33. Hostile.
34. Sympathetic.
35. Slow to process complaints.

## Section 2

## Security and Law Enforcement; e-Government; and Call Centre Issues

# A MODEL OF A PRAGMATIC SECURE E-PAYMENT SYSTEM

**E. E. Odokuma**
Biotic Technology & Consulting Services,
Port Harcourt, Rivers State
*elizzyodoks@yahoo.com, 2*

**G. M. M. Obi**
International Business Systems,
12 Moleye St, Alagomeji Sabo Yaba.
*gmm.obi@consultant.com*

***ABSTRACT***

*The traditional e-payment system is modeled as the interaction of the five principal entities: the client, the merchant, the issuer, acquirer and the payment system service provider, all singletons, operating in an environment where the security considerations are based on the Fortress Model. In this paper, we present a formal model in which each of the principal entities is possibly not a singleton, and the set includes new entrants such as intermediaries/mediators as well as e-payment enhancing mechanisms. Moreover the security considerations are based on the contemporary paradigm of survivability. This work is in response to developments and trends in the e-payment landscape where new aspects such as: business mediator, network smart card and mobile devices, multiparty and connectivity scenarios, and the multiplicity of entities as dictated by aggregation of demand and aggregation of supply have emerged, and the assumptions on which the extant security considerations are based are no longer valid in the contemporary environment of an e-payment system.*

*Key Words: e-payment, demand/supply aggregation, fortress, survivability.*

## 1. INTRODUCTION

Electronic payment systems (e-payments) have attracted a lot of research interest over the years, more so since e-commerce made its debut. The literature is replete with proposed solutions to the issue of formal pragmatic secure e-payment models for e-payment systems. In these attempts an e-payment system is modeled as the interaction of the five principal entities, all singletons: the client, the merchant, the issuer, acquirer and the payment system service provider (Carbonell et al, 2007). This is however limiting, given developments and trends where new aspects have emerged, such as: business mediator, network smart card and mobile devices, multiparty and connectivity scenarios, and the multiplicity of entities, induced by the need for demand and supply aggregations, all of which now create new scenarios and circumstances for which new survivable secure solutions are needed. This work presents a formal model which provides a basis for protocol designers and system implementers to create, implement, and analyze survivable and more practical and realistic e-payment systems, thus enabling a fuller description of the principal entities involved, the inter entity interactions and the attendant flow of transactions among and between them.

The rest of the paper is organized as follows: Section 2 presents a brief description of the traditional generic e-payment system. This is followed in Section 3 by developments in the e-payment landscape and related works. In Section 4 is presented the proposed e-payment model. Some applications are presented in Section 5, and the conclusion in Section 6.

## 2. THE TRADITION E-PAYMENT MODEL

The traditional e-payment model is presented in several works for example (Kou, 2003; Kungpisdan, 2005; Obi, 2011b; Tsiakis and Stheohanidews, 2005) as consisting of five principal inter-related interacting entities.

(i) **Client (CL): The e**ntity who seeks to buy goods or to be rendered services.

(ii) **Merchant (MT):** The **e**ntity who delivers the goods or renders the services to the client, when payment shall have been made by the client.

(iii) **Issuer (IR):** The financial organization that issues the valid electronic payment instrument (for example, credit/debit card, account and others). The issuer transfers funds from the client's account to the financial organization of the merchant in payment for the related goods or services.

(iv) **Acquirer (AQ):** The financial organization of the merchant. The acquirer verifies the validity of the deposited payment made by the issuer and on being satisfied inform the payment system provider who in turn inform the merchant.

(v) **Payment system provider (PP):** The entity which performs payment interactions on behalf of **IR** and **AQ** on the one hand, and on behalf of **CL**and **MT**on the private financial network side, on the other. The **PP** receives the request of payment authorization from the merchants and communicates with the issuer or,depending on the e-payment instrument**,** with the client for some information (account, password, etc.). If this payment authorization request is successful, the PP informs the merchant and, on the merchants concurrence, the acquirer.

The principal flow of messages in the payment process is:

(vi) Payment ordering: PO is the interaction between CLand MT, where CLrequests to purchase goods from, or use the services of, MT. The required information (amount of purchases, issuer identification by payment instruments, etc.) is sent to MT by CL,

(vii) Authorization request is the interaction by which MT requests a payment authorization from the issuer of the client and waits for a response. The payment authorization process is handled through a PP. This is done by either:

(a) Off-line client authentication: Where the PP checks the client information, received from merchants, without resorting to an online client authentication. In this approach, the merchant receives all the private information of client, forwards it to the PP and the PP connects to the issuer bank.

(b) Online client authentication: Where the PP checks the client information, which is received from merchants, by means of an online authentication mechanism (PIN, password, certificates, etc.). To achieve this, the PP establishes an authentication channel with the client.

(viii) Authorization response: Where the PP sends the response (successful or unsuccessful depending on issuer decision) of the authentication process to the merchants. If it is successful, the response is sent to the acquirer, in order to conclude the purchase.

(ix) Payment clearing: An interaction between **IR** and **AQ** concludes the payment process, the goal being to transfer the requested amount from the account of the client to that of the merchant. Normally, this type of transaction is performed under a private banking network, once the acquirer has received a successful authorization response. The interaction ends when AQforwards the payment receipt to MTthrough a PP.

In figure 1 the arrows represent the directions of these transactions.

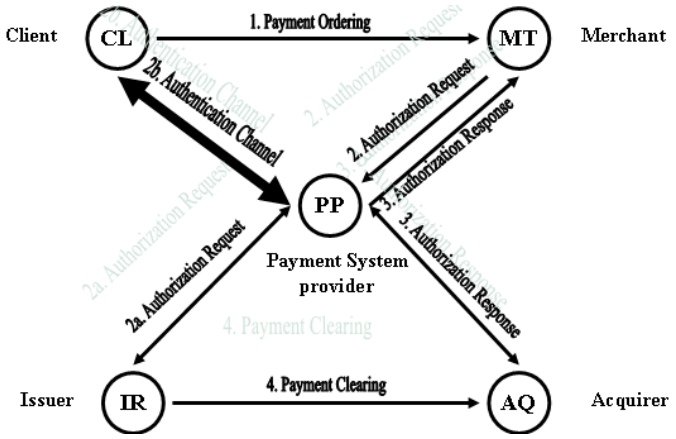



*Figure 1: flow of messages in the traditional e-payment system (adapted from Carbonelli et al, 2007)*

## 3. DEVELOPMENTS AND RELATED WORK

In the aforementioned model each of the five principal entities is assumed to be a singleton (consist of a single element) – one client buying from one merchant with there being one issuer, one acquirer and one payment system provider. The security considerations are focused on the transactions, and are based on the fortress model which emphasizes protecting the system from unauthorized users.

However, in reality there are now more elements in the set of principal entities. Examples of some of these are given next.

### a. Mediators/Intermediaries

There are now mediators or intermediaries, or clients' agents who source the goods and negotiate on behalf of the clients (Bhargava and Choudhary, 2004; Dikaiakos, 2004; Esparza et al, 2006; Giaglis et al, 2002) thus providing many value adding functions that cannot be easily substituted or 'internalized' through direct supplier-buyer dealings. In some works the payment process, the intermediary/mediator is usually considered as an entity that secures the payment transaction, i.e. it is associated with the PP while in others works it is represented, as an entity capable of, among other functionalities, of reducing the customer operations (Bhargava and Choudhary, 2004), simplifying the amount of transactions (Urien, 2000), providing a centralized connection with the PP (Chari et al, 2001), among others. In all the cases, it is represented as an entity with value added services to the client and merchants.

### b. E-Payment Enhancing Mechanisms

Also coming into the e-payment picture are enhancing mechanisms. The several efforts made to transform the smart card into a device open to network interconnectivity have yielded a number of such e-payment enhancing devices which are considered as fully functional Internet nodes in accordance, whenever possible, with established standards. Examples of such mechanisms are the Network Smart Cards (NSC's) which feature in several studies such as (Postel, 1981; Rees and Honeyman, 2000; Porter, 2001; Giaglis et al, 2002; IST, 2003; Ali et al, 2004;; Lu and Ali, 2004; Ali et al, 2005; Esparza et al, 2006; Rappa, 2006; Torres et al, 2006; and Torres et al, 2007; Tellez and Sierra Cámara, 2007; Obi, 2011b).. There are thus mechanisms now that are able to provide services or access Internet resources making use of protocol stacks in the same way as any other node on the network. Indeed, apart from its having been proposed that the network smart card be used in security solutions, the mechanism has been able to establish secure direct communication with remote Internet servers, (Ali et al, 2004; Lu and Ali, 2004), thus demonstrating usability in online transactions.

On a related note, the remote authentication protocol architecture for network smart cards described in (Torres et al,

2006), aims at offering a global authentication process with maximum security assurance. Thus the NSCs and other mechanisms of the like, which are referred to in this work as e-payment enhancing mechanisms, are powerful devices for use as secure mechanisms to authenticate the client.

**c. Connectivity**

In recent years protocols designed for mobile payment systems, an aspect of e-payment, are based on a scenario where all entities are directly interconnected. This scenario (formally called "Full connectivity scenario" (Chari et al, 2001)) offers advantages to protocol designers because it allows them to simplify the design and development of payment protocols without losing security guarantees. Nevertheless, this scenario does not consider situations in which one of the principal entities may not be able to communicate directly with another for some reason, e.g. lack of Internet access, restrictions of handheld device, or geographic. New connectivity scenarios have therefore emerged, and these have been classified (Chari et al, 2001) as:

(i) **Disconnected:** CL and MT are disconnected from the PPand directly communicate with each other using a local link.
(ii) **Server-Centric:** The PP is connected to both CL and MT but they are not directly connected with each other.
(iii) **Client-Centric**: CLis connected to both MT and the PPbut they are not directly connected with each other.
(iv) **Kiosk-Centric**: MTis connected to both CLand the PPbut they are not directly connected with each other.
(v) **Full-Connectivity:** All the entities are directly connected to one another.

Connectivity is one of the more important determinants of the design of further security solutions for electronic payment, especially in mobile contexts. This concept implies in many cases new message flows and new secure mechanisms to protect the traditional payment transactions.

**d. Multiplicity of involved entities**

Multiparty scenarios in electronic commerce (Tellez and Sierra Cámara, 2007; Torres et al, 2006) are already well-known. Applications such as virtual mall or market place, commercial search agentdescribe a commerce scenario of multi-purchase, where one customer could interact with several merchants simultaneously (supply aggregation) – one client obtaining products from several merchants.

In other business models, such as demand aggregation, there appear scenarios where several customers need to form a partnership in order to increase their bargaining power and obtain discounts; in that way, this multiple customers could interact with one merchant or with many merchants, simultaneously.

From the foregoing, traditional topologies such as (one-to-many, ring, mesh, many-to-many) now need to be considered in the payment model, and also, need to be integrated with the others previous aspects in order to represent real applications.

The principal entities of client, merchant, PP, issuer and acquirer has to be extended to address the practical reality: the possibility of the clients, merchants, intermediaries/mediators, e-payment enhancing mechanisms, payment system providers, issuers and acquirers all being sets with more than one element and not singletons as hitherto modeled, with the exception of the mediator or intermediary sets which may contain zero or more elements; zero when no mediators are involved, in the case when the client does the negotiations personally, and more, otherwise. Thus, while the mediator set could be empty in the case when the clients opt to do their buying by themselves, the client and merchant's sets are non-empty.

As expected, there are a number of differences between this extension and the traditional model outside the increase in the cardinality of the principal entities. For example the devices, tokens and media are all considered as sets too, and while the number of connectivity scenarios in the traditional model is eight (8) (Charis et al, 2001), they are thirty-two (32) in the extended version (Obi, 2011), thereby exacerbating the survivability concerns.

## 4. THE PROPOSED E-PAYMENT MODEL

The proposed formal model is presented hereunder. Recalling that the e-payment system (**EPS**) is a collection of interacting interrelated entities, it can be described as:

$$\mathbf{EPS=\xi(PE, PC, PT, GL, RQ, SV)} \quad 1.0$$

where$\xi$ is a binary map that returns the result of the interactions of the system's entities. It returns the value 1 if the payment transaction is successful i.e. if all interactions, survivability, trust, and performance issues relating to the payment in question are the prescribed ones, and 0 otherwise. The variables are as follows:

**PE** is the set of principal entities;

**PC** is the set of payment channels. The channels through which the payment under consideration is carried out;

**PT** is the set of payment transactions;

**GL** is the set of goals – of the principal entities and of the systems itself;

**RQ** is the set of requirements – of the principal entities, the system, statutory, trust and performance;

**SV** is the set of survivability measures.

These are now described formally. In what follows the cardinality of a set **A** will be denoted by $|\mathbf{A}|$.

**a. The Principal Entities**

**PE** is the set of the extended principal entities:

$$\mathbf{PE=\{CL, MT, IR, AQ, PP, IM, EM\}} \quad \mathbf{1.1}$$

where**CL** is the set of clients,

$$\mathbf{CL=\{}CL_1, CL_2, \ldots, CL_{|\mathbf{CL}|}\mathbf{\}} \quad \mathbf{1.1.1}$$

**MT** is the set of merchants,

$$\mathbf{MT=\{}MT_1, MT_2, \ldots, MT_{|\mathbf{MT}|}\mathbf{\}} \quad \mathbf{1.1.2}$$

**IR** is the set of issuers,

$$\mathbf{IR=\{}IR_1, IR_2, \ldots, IR_{|\mathbf{IR}|}\mathbf{\}} \quad \mathbf{1.1.3}$$

**AQ** is the set of acquirers,
**AQ={**$AQ_1, AQ_2, \ldots, AQ_{1|AQ|}$**}** **1.1.4**
**PP** is the set of payment system providers,
**PP={**$PP_1, PP_2, \ldots, PP_{|PP|}$**}** **1.1.5**
**IM** is the set of intermediaries/mediators,
**IM={**$IM_1, IM_2, \ldots, IM_{|IM|}$**}** **1.1.6**
**EM** is the set of Payment enhancing mechanisms,
**EM={**$EM_1, EM_2, \ldots, EM_{|EM|}$**}** **1.1.7**

**b. Channels of Payment**

**PC** is the set of channels of payment
**PC={PE, DV, TK, MD, CN}** **1.2**
where**DV** is the set of devices,
**DV={PE,** $DV_1, DV_2, \ldots, DV_{|MD|}$**}** **1.2.1**
**TK** is the set of payment tokens,
**TK={PE,** $TK_1, TK_2, \ldots, TK_{|TK|}$**}** **1.2.2**
**MD** is the set of media,
**MD={PE,** $MD_1, MD_2, \ldots, MD_{|MD|}$**}1.2.3**
**CN** is the set of connectivity scenarios,
**CN={PE,** $CN_1, CN_2, \ldots, CN_{|CN|}$**}1.2.4**

This can be described as: the principal entities **PE** interacting using the devises **DV** and the tokens **TK,** over the media **MD** on the connectivity scenarios **CN**, to effectuate the related payment transactions. Here the devices could be, for example, Pc's, handheld e.g handsets and PDA's, the tokens e-cash or one form of card or the other, the medium online PC, fixed or wireless network, and the connectivity scenarios one or more of the 32 that have been identified,(Obi, 2011).

**c. Payment Transactions**

**PT** is the set of transactions, each transaction being composed of processes, which are in turn composed of protocols and documentations.

$PT=\{PE, TT, PC\}$ 1.3

where TT is the set containing sets of processes

$TT=\{TT_1, TT_2, \ldots, TT_{|TT|}\}$ 1.3.1

$TT_i$ is a set of processes each of which is made up of protocols and documentations.

$$\mathbf{TT_i}=\left\{\mathbf{Pd_{i,j}}\right\}_{\mathbf{j=1,2,\cdots,|TT_i|}} \quad 1.3.2$$

$Pd_{i,j}$ being the process j in $TT_i$, and

$$\mathbf{Pd_{i,j}}=\left\{\mathbf{PL_{i.j,k}},\mathbf{DC_{i,j,k,\ell}}\right\}_{\mathbf{k=1,2,\cdots,\left|PL_{i,j}\right|}},$$

$$\ell=\mathbf{1,2,\cdots,\left|DC_{i,j,k}\right|} \quad 1.3.3$$

with PLi, j, k being the protocol k in the process $\mathbf{Pd_{i,\ j}}$ and $\mathbf{DC_{i,\ j,\ k,\ l}}$being the documentation l in the protocol $\mathbf{PL_{i,\ j,\ k}}$

In the case under consideration the transactions are: payment ordering, withdrawal, deposit, or payment clearing. So, setting

$\mathbf{TT_1}$=payment ordering, $\mathbf{TT_2}$=withdrawal, $\mathbf{TT_3}$=deposit, and $\mathbf{TT_4}$=payment clearing, there would be two processes in $\mathbf{TT_1}$ namely: the process wherein the client sends a request to the merchant for the purchase of goods or the use of the services of the merchant, and that wherein the merchant responds to the request of the client. The documentations relating to these are easily discernable. The flow of messages arising from the extension of the principal entities is as shown in figure 2. The plain arrows indicating direct connection while dotted arrows are indicative of the connections being direct or indirect.

**d. The Goals Relating to the Payment**

**GL** is the set of goals. This consists of the goals of the engaging parties (clients, merchants, payment system providers, issuers, acquirers, and intermediaries/mediators), the goals of the messages and of course those of the system. Thus,

$GL=\{GL_1, GL_2, \ldots, GL_{|GL|}\}$ 1.4

where is the set of goals for each engaging party or entity $GL_i$

$GL_i=\{GL_{i,j}\}_{j=1, 2, \ldots, |GLi|}$ 1.4.1

For example, if $GL_1$ relates to CL, $GL_2$ to MT, $GL_3$ to IR, $GL_4$ to AQ, $GL_5$ to PP, $GL_6$ to MD, $GL_7$ to the system, and $GL_8$ to the set of messages, then $GL_1=\{GL_{1,j}\}_{j=1, 2, \ldots, |GL1|}$ is the set of goals of the clients, while $GL_5=\{GL_{5,j}\}_{j=1, 2, \ldots, |GL5|}$ is the set of goals of the payment system providers.

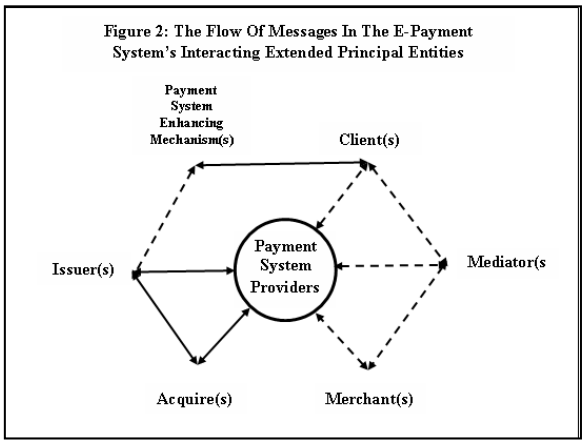


Figure 2: The Flow Of Messages In The E-Payment System's Interacting Extended Principal Entities

**e. The Payment Requirements**

**RQ** is the set of requirements. This consists of the requirements of the engaging parties (clients, merchants, payment system providers, issuers, acquirers, and intermediaries/mediators), the system and of course, regulatory and statutory requirements.

**RQ={**$\mathbf{RQ_1, RQ_2, \ldots, RQ_{|RQ|}}$**}** **1.5**

where**$\mathbf{RQ_i}$**is the set of goals for each engaging party or entity **$\mathbf{GL_i}$**.

**$\mathbf{RQ_i=\{RQ_{i,j}\}_{j=1, 2, \ldots, |RQi|}}$** **1.5.1**

For example, if **$\mathbf{RQ_1}$** relates to **CL**, **$\mathbf{RQ_2}$** to **MT, $\mathbf{RQ_3}$** to **IR, $\mathbf{RQ_4}$** to **AQ, $\mathbf{RQ_5}$** to **PP, $\mathbf{RQ_6}$** to **MD, $\mathbf{RQ_7}$** to the system**,** and **$\mathbf{RQ_8}$**tothe set of regulatory and statutory agencies**,** then **$\mathbf{RQ_1=\{RQ_{1,j}\}_{j=1, 2, \ldots, |RQ1|}}$** is the set of requirements of the clients, while **$\mathbf{RQ_5=\{RQ_{5,j}\}_{j=1, 2, \ldots, |RQ5|}}$** is the set of requirements of the payment system providers.

Still on requirements, the trust relationships as well as security and performance are very important in e-payment and deserve some expatiation.

*i. Trust In An E-Payment System*

Let **$\mathbf{RQ_t}$**for some $0<t\leq|\mathbf{RQ}|$, be the set of such relationships. In the traditional e-payment model there are

five (5) interacting entities, so there are $3^5$-1=242 such relationships while in the model involving intermediaries, there are $242.\prod_{n_i \neq o}(3^{n_i}-1)$ , i=1, 2, …, 6, where $n_1$=|**CL|,** $n_2$=|**IM|,** $n_3$=|**ME|,** $n_4$=|**PP|,** $n_5$=|**IR|,** and$n_6$=|**AQ|.** In the general model under consideration the trust relationships are given by: $\mathbf{RQ_t(a, b)}$ with **a, b**∈{**CL, MT, IM, IR, AQ**}, $\mathbf{RQ_t}$(**CL, EM**), $\mathbf{RQ_t}$(**EM, CL**), $\mathbf{RQ_t}$(**EM, IR**), $\mathbf{RQ_t}$(**IR, EM**), where $\mathbf{RQ_t(a, b)}$ indicates that the set of entities **a** "trust" **b** meaning that **a** trusts that **b** performs its tasks and/or acts as prescribed that it should. The formal definition of "trust" adopted is that contained in(Obi, 2011a).

**f. Survivability (Security) Conditions**

Let **RQ** for some 0<s≤|**RQ**| be the set of survivability conditions that an e-payment system should satisfy. These are critical for the e-payment system, Stallings (2006). Survivability is the capability of a system to continue to support mission critical processes despite attacks, failures or accidents (Lipson and Fisher, 1999). This security paradigm is considered rather than the extant FORTESS security paradigm because it is now known that the assumptions on which the latter paradigm is based are no longer valid in the contemporary environment of the Internet and other unbounded networks and systems. Composed of a combination of legacy and emerging technologies, the e-payment environment, broadly viewed, is heterogeneous and multi-layered (specifically, 3-layered). At the top is the 'application/service' layer, which uses network services for end system processes and provides interface to the user. In the middle is the 'traffic layer', which provides routing and congestion control for connections across the network. It consists of the networking environment such as circuit-switching, packet-switching (TCP/IP), ATM, and virtual private networks (for special services). Finally, there is the bottom layer, the "transmission layer", which typically consists of a mixed technology infrastructure containing fiber and non-fiber wire based systems as well as wireless components (microwave, cellular, satellite, etc.). Thus, an e-payment service may traverse several interconnected networks with different physical layer and network layer components.

Therefore the e-payment security should cover not only one layer – the transaction layer, but the other layers as well, i.e. address survivability to provide measures that minimize the impact of untoward incidents. This is dealt with extensively in (Dawudu and Obi, 2011 )

Thus, the e-payment system survivability is modeled as follows:

$\mathbf{RQ_s = \{PE, RC, RS, RV, AD\}}$ **1.6**

where**RC** is the set of incident integrated and coordinated recognition measures,

**RC={CA, CT, CP, CD}** **1.6.1**

where**CA, CT, CP, and CD** are the sets of recognition measures at the application, traffic and physical layers, respectively

**RS** is the set of incident integrated and coordinated resistance measures

**RS={SA, ST, SP, SD}** **1.6.2**

where**SA, ST, SP, and SD** are the sets of resistance measures at the application, traffic and physical layers, respectively.

**RV** is the set of incident integrated and coordinated recovery measures

**RV={VA, VT, VP, VD}** **1.6.3**

where**VA, VT, VP, and VD** are the sets of recovery measures at the application, traffic and physical layers, respectively.

**RA** is the set of incident integrated and coordinated measures for system adaptation to incidents

**RA={AA, AT, AP, AD}** **1.6.4**

where**AA, AT, AP, and AD** are the sets of measures for system adaptation to incidents at the application, traffic and physical layers, respectively

This engenders the authentication, privacy, integrity, authorization and the non-repudiation of transactions as well as the robustness of the system during, and its restoration after untoward incidents.

**g. Performance Requirements**

The proposed model of the transaction performance of an e-payment system is given by:

$\mathbf{RQ_p(PR, BW, RL, CP, MS, DU)}$ 1.7

For some 1≤**p**<|**RQ|, w**here

**PR**=(**PE**, **PC, PT)** is the processing capability at a set of channels **PC** used by a set of entities **PE** in performing a set of payment transactions **PT**

**BW**=(**PE**, **PC, 1, PT)** is the available resources (e.g. bandwidth) of a set of channels **PC** used by a set of entities **PE** during the performance of a set of payment transactions **PT**

**RL**=(**PE**, **PC, 2, PT)** is the reliability of a set of channels **PC** used by a set of entities **PE** in performing a set of payment transactions **PT**

**CP**=(**PE**, **PC, 3, PT)** is the total computation at a set of channels **PC** used by a set of entities **PE** in performing a set of payment transactions **PT**

**MS**=(**PE**, 1, **PT)** is the number of messages passed among a set of entities **PE** in performing a set of payment transactions **PT**

**DU**=(**PE**, 2**, PT)** is the duration to complete a set of channels payment transactions by a set of entities **PE**.

## 5. APPLICATIONS

**a. The traditional e-Payment**

It is easy to see that the proposed model addresses the traditional model, as in this case, the set of principal entities, **PE,** is composed of the singletons of client, merchant, issuer, acquirer, and payment system provider, and the null sets of the intermediary and e-payment mechanisms. The requirements, trust, security and performance issues are as usual. The model however, makes possible considerations of more payment connectivity options than the traditional eight (8). Here as many as thirty-two (32) options are possible Obi (2011b). The security component is more realistic in that it is predicated on the contemporary paradigm which address the

e-payment system as a layered entity that it is rather than focusing on "protection" and hence on layer-violating counter-measures.

**b. New scenarios**

The following new scenarios, among others, not addressed by the traditional model when the set of principal entities is composed of elements that are not necessarily singletons, are all possible applying the proposed model. Let:

CL, be the set **CL** with one element and $CL^+$ the set **CL** with more than one element, similarly for the sets **MT, IR, AQ, PP, IM,** and **EM.** Let $\mathbf{IM^0}$, $\mathbf{EM^0}$be the respective sets with 0 elements, i.e. the respective empty sets. Finally let $b_1b_2b_3b_4b_5$ with $b_i$ =0 or 1, i =1, 2, ..5, be a bit vector. Then e-payment scenarios can be considered, whose principal elements are given by:

**PE**={$PE_1$, $PE_2$, $PE_3$, $PE_4$, $PE_5$, $PE_6$, $PE_7$} and with connectivity scenarios $b_1b_2b_3b_4b_5$,

where,

$PE_1$ = CL or $CL^+$,

$PE_2$ = MT or $MT^+$,

$PE_3$ = IR or $IR^+$

$PE_4$ = AQ or $AQ^+$,

$PE_5$ = PP or $PP^+$

$PE_6$ = $IM^0$, IM or $IM^+$,

$PE_7$ = $EM^0$, EM or $EM^+$

The traditional model is obtained when **PE** = {CL, MT, IR, AQ, PP, $IM^0$, $EM^0$} with any of the connectivity scenario $b_1b_2b_3$.

## 6. CONCLUSION

The traditional e-payment model with five entities: the client, the merchant, the issuer, acquirer, the payment system service provider, and layer violating security measures has been found not to be realistic given the developments and trends in e-payment systems and their environments. An extended e-payment model, which in addition to the entities in the traditional model, include new and emerging trends such as intermediaries/mediators, e-payment enhancing mechanisms, and the flow of transactions among and between them, and security conditions respecting the layered nature of the system has been presented. The traditional model assumes that each of its five entities consist of a single element; one client buying from one merchant with one issuer, one acquirer and one payment system provider. The extended model however takes cognizance of the fact that some of its entities may have plural multiplicity (consist of. more than one element). Devices, tokens, media and connectivity scenarios are all considered as sets in the set of channels of payment in the extended model. It also took into accountchanges in the systems' security landscape and connectivity scenarios. This work thus presents a formal model which provides a basis for protocol designers and system implementers to create, implement, and analyze survivable and more practical and realistic e-payment systems.

## REFERENCES

Ali, A., Lu, K., Montgomery, M., 2004. Secure Network Card. Implementation of a Standard Network Stack in a Smart Card. In: *Proc. of 4th IFIP Smart Card Research and Advanced Application Conference, CARDIS.*Toulouse, France. Kluwer Academic Publishers, Dordrecht, pp 193-208.

Ali, A., Lu, K., Montgomery, M., 2005. Network Smart Card: A New Paradigm of Secure Online Transactions. In: *Proc. of Security and Privacy in the Age of Ubiquitous Computing, IFIP TC11, 20th International Conference on Information Security.* Chiba, Japan, pp.267~280

Bhargava, H., Choudhary, V., 2004. Economics of an Information Intermediary with Aggregation Benefits.*Information Systems Research* 15(1), pp 22–36.

Carbonell, M., Sierra, J., Torres, J., Izquierdo, A., 2007.Security analysis of a new multi-party payment protocol with intermediary service. In: *DEXA Workshops*, pp. 698–702

Chari, S., Kermani, P., Smith, S., Tassiulas, L., 2001. Security Issues in MCommerce: An Usage-Based Taxonomy. In: *Proceedings of E-Commerce Agents*, pp. 264–282.

Dawudu D, Obi G. M. M., 2011. Survivability in e-Payment Systems: A Holistic Approach to e-Payment Security, Preprint

Dikaiakos, M., 2004.Intermediary infrastructures for the World Wide Web.*Computer Networks* 45(4), 421–447.

Esparza, O., Muñoz, J., Soriano, M., Forné, J., 2006. Secure brokerage mechanisms for mobile electronic commerce. *Computer Communications* 29(12), 2308–2321

Giaglis, G., Klein, S., O'Keefe, R., 2002. The role of intermediaries in electronic marketplaces: developing a contingency model. *Information Systems Journal* 12(3), 231.

IST, 2003.Roadmap for European Research on Smartcard related Technologies-RESET, *Final Roadmap, v.5*.IST-2001-39046.

Kou, W., 2003.*Payment technologies for e-commerce*.Springer, Heidelberg.

Kungpisdan, S., 2005.*Modeling, design, and analysis of Secure Mobile Payment Systems*., Thesis for Doctor of Philosophy, Faculty of Information Technology, Monash University. *http://beast.csse.monash.edu.au/~srini/theses/keng.pdf,* Accessed Oct 17, 2011.

Lipson, H.F., Fisher, D.A., 1999. Survivability- A new Technical and Business Perspective on Security, In *Proc. Of the New Security Paradigm Workshop, IEEE Computer Society press,* pp 33-39.

Lu, H.K., Ali, A., 2004. *Prevent On-line Identity Theft - Using Network Smart Cards for Secure On-line Transactions*. Zhang, K., Zheng, Y. (eds.) ISC. LNCS, vol. 3225.Springer, Heidelberg, pp 342-353.

Obi Gabriel M.M., 2011a. A Formal Trust Model in Autonomic Computing, Preprint

Obi Gabriel M.M., 2011b. An Extended e-Payment Usage Connectivity Taxonomy, Preprint

Porter, M., 2001.Strategy and the Internet.*Harvard Business Review*, 63–78.

Postel, J., 1981. Transmission Control Protocol.IETF RFC 079.

Rappa, M., 2006. Business models on the web. Managing the digital enterprise.*http://digitalenterprise.org/models/models.html* Accessed 17th December, 2011

Rees, J., Honeyman, P., 2000. Webcard: a Java Card web server. In*: Proc. of 4th IFIP Smart Card Research and Advanced Application Conference, CARDIS*. Bristol, U.K, pp 197-207.

Stallings, W., 2006.*Cryptography and network security: Principles and Practices*, ch. 16-20. Prentice Hall, Englewood Cliffs.

Tellez Isaac, J., Sierra Cámara, J.M., 2007. Anonymous Payment in a Client Centric Model for Digital Ecosystems. In: *Proceedings of IEEE International Digital Ecosystems and Technologies (DEST),* Australia, pp 422-427.

Tellez, J., Sierra, J.M., Izquierdo, A., Torres, J., 2006. Anonymous Payment in a Kiosk Centric Model using Digital signature scheme with message recovery and Low Computational Power Devices.*Journal of Theorical and Applied Electronic Commerce Research* 1(2), 1–11.

Torres, J., Izquierdo, A., Sierra, J.M., Ribagorda, A., 2006. Towards self-authenticable smart cards.*Computer Communications* 29(15), 2781–2787.

Torres, J., Izquierdo, A., Sierra, J.M., 2007. Advances in network smart cards authentication.*Computer Networks* 51(9), 2249–2261.

Tsiakis, T., Stheohanidews, G., 2005.The concept of security and trust in electronic payments.*Computer & Security* 24(1), 10–15.

Urien, P., 2000 Internet card, a smart card as a true Internet node. *Computer Communications* 23(17), 1655–1666.

# USERS' PASSWORD SELECTION AND MANAGEMENT METHODS: IMPLICATIONS FOR NIGERIA'S CASHLESS SOCIETY

**A. S. Sodiya**
Dept of Computer Science,
Federal University of Agriculture, Abeokuta
sodiyaas@unaab.edu.ng

***S. Agholor**
Dept of Computer Science,
Federal College of Education, Abeokuta
sunday_agholor@yahoo.com
sunday.agholor@gmail.com

***ABSTRACT***

*The Central Bank of Nigeria (CBN) commenced the cashless policy on April 1, 2012 using Lagos State as a pilot scheme. There was general criticism of the policy because of the activities of the cyber-criminals and general inadequate protection of customers' accounts and transactions. Since the password is a major security system that drives the cashless society, there is the urgent need to examine the readiness of Nigerians in terms of password selection and management methods. Twenty four thousand (24,000) Lagos State residents that carry out online banking transactions were used for this study. A pre-tested questionnaire was administered to capture the attitudes of the customers in terms of password selection and management. The empirical results reveal alarming negative password practices. The implication of having negative password practices is that there is the urgent need to educate all Nigerians on password best practices in order to have a cashless society with minimal cyber-crimes.*

***Keywords**: Cashless, Cyber-criminals, Password, Security*

## 1. INTRODUCTION

A cashless society is a society that minimizes the use of cash by providing alternative channels for making payments. According to Edet (2008) a cashless society involves the settlement of financial transactions electronically with the use of electronic gadgets such as Automatic Teller Machines (ATMs), Point-of-Sales terminals (PoS), Global System for Mobile Communications (GSM) phones, Valu-cards etc. The concept of cashless society has been implemented in many countries especially in the developed countries where its citizens are inclined to the use of technology. Nigeria, as a developing country with the ambition of becoming one of the 20 largest economies in 2020 cannot afford to stay behind the trend.

Authentication is the process of identifying an individual, usually based on a username and password. Traditionally, authentication procedures are divided into two stages: identification, which is the process of capturing users' identities; and authentication, which is the process of verifying the supplied identities. According to Hayashi and Jason (2011), Alkhalifah and Skinner (2010) and Perkovic et al (2009) the traditional authentication method is the simplest and most commonly used by majority of the users and systems. It has been reported that 86% of U.S. companies use password authentication (InformationWeek, 2007) and, according to a Deloitte Security Survey (2007), 53% of surveyed organizations rely solely on password-based authentication for end-user Internet transactions. In the U.K., four-fifths of surveyed companies use passwords as the only authentication method (DTI survey, 2006). Since organizations widely adopt and heavily depend on password authentication methods, the issue of password management is critical to Nigeria cashless economy. Passwords and Personal Identification Numbers (PINs) are common traditional authentication methods (Rabkin, 2008). In this article, passwords and PINs are collectively referred to passwords.

The wide condemnation and criticism that followed the CBN announcement of implementing cashless society calls for a second look on how users select, use and manage their passwords. The cry is not unconnected with increasing number of cases of identity theft. Identity theft involves stealing money or getting other benefits by pretending to be someone else (Divyans, 2009). According to Butler (2005), the increasing number of cases of identity theft has resulted in a lot of more emphasis being placed on advising users on the selection and use of passwords. The question now arises as to whether users adopt international best practices in selecting, using and managing passwords. The purpose of this research is to evaluate the practices of Nigerians in creating, managing and using passwords for accessing bank online accounts.

The rest of this paper is organized as follows: Section 2 presents Literature Review. Research methodology is discussed in Section 3. Analysis and discussion of results are presented in Section 4. Finally, recommendations, conclusion and future work were discussed in section 5.

## 2. RELATED WORKS

As one of the most common authentication methods, passwords help to secure information by granting access only to authorized parties. To be effective, passwords should be strong, secret, and memorable. While password strength can be enforced by automated information technology policies, users frequently jeopardize secrecy to improve memorability (Zhang et al, 2009). The password memorability problem is exacerbated by the number of different passwords a user is required to remember.

There have been several studies on investigating password usage, including people's selection of passwords (Gehringer, 2002), strength and memorability of user chosen passwords (Yan et al, 2004; Kuo et al, 2006 and Florencio et al,

2007) and the number of passwords and accounts users have (Gaw and Felten, 2006; and Florencio and Herley, 2007). Inglesant and Sasse (2010) investigated password usage in companies and Shay et al (2010) investigated the effects of password policies on users' practices.

To prevent themselves from having to remember a variety of different complex passwords, many users make use of the same password for different applications and services. Unfortunately, this increases the risk of an attacker stealing users' digital identities, as the password could be stored in applications and potentially be accessible to others (Wessels and Steenkamp, 2007). Password authentication therefore appears to involve a trade-off. Some passwords are very easy to remember, but also very easy to guess with dictionary searches or by obtaining the personal information of a user. In contrast, some passwords are very secure against guessing, but difficult to remember (Yan et al, 2004).

Although, a vast number of research studies have been done on what good password practices entails, a limited number of studies on how users employ and remember passwords could be identified. It is much safer to use a password on the Internet than securing stand alone computers with passwords. This is because when every possible key is being tested on a personal stand alone computer with the actual cipher text, it is a much quicker process to guess the password than when the testing is being done remotely. Most Web sites will also shut down an account if there are too many incorrect password attempts in a row. That is why criminals have turned to stealing passwords, for example, through phishing (Schneier, 2004).

Password-protected accounts are very common and are widely used for a variety of on-line applications, including instant messaging, personal and business e-mail, and on-line banking and retail accounts. Good passwords generally involve a combination of uppercase and lowercase letters at least six to eight characters long, with numbers or special keyboard characters imbedded in the middle (Andrews, 2002; Armstrong, 2002). Aside from poor password construction, bad practices in password applications include things such as using the same password repeatedly (Zhang et al, 2009; Dhamija and Perrig, 2000), writing down passwords (Zhang et al, 2009).

Riley (2006) conducted a study among undergraduate and graduate-level college students from Wichita State University in Kansas, USA, to assess what practices users employ to create and store passwords for on-line accounts. The majority of the participants reported password-generation practices that are simplistic and a security risk. Particular practices reported included using lowercase letters, numbers or digits, personally meaningful words and numbers. These findings are supported by similar research by Vu et al (2003), who found that even with the application of password guidelines, users tended to revert to the simplest possible strategies. In her findings, Riley (2006) reported that nearly 60% of the respondents did not vary the complexity of their passwords to match the nature of the site, and 53% indicated that they never change their password if they were not required to do so. These practices were most likely encouraged by the fact that users maintained multiple accounts (average 8.5) and had difficulty recalling too many unique passwords.

Yan et al(2004) highlighted the problems of selecting good passwords caused by a lack of proper advice to users on how to decide on a password, as well as the system-level enforcement that should complement the password-selection process. Their research consisted of an experiment involving 400 first-year students at Cambridge University. The experiment compared the effects of giving three alternative forms of advice about password selection, and measuring the effect that this advice had on the security and memorability of passwords. In their research, they confirmed that users had difficulty remembering random passwords. Passwords based on mnemonic phrases are harder for an attacker to guess than naively selected passwords. A mnemonic phrase involves choosing a password by using the first letters of a phrase or sentence.

However, they found that random passwords were not better than those based on mnemonic phrases, nor were passwords based on mnemonic phrases harder to remember than naively selected passwords. They advised that users should be instructed to choose mnemonic-based passwords, as these are just as memorable as naively selected passwords, while being just as hard to guess as randomly chosen ones. Length of passwords does matter as stated by Florencio and Herley (2010) and users should be forced to select passwords of eight characters or more. They also recommend that users should be told to choose passwords that contain numbers and special characters as well as letters.

Compliance with these rules is a critical issue. In systems where users can place only themselves at risk, it may be prudent to leave them to select and change their passwords themselves. In systems where a user's negligence can impact on other users too, consideration should be given to enforcing password quality through system mechanisms. Many of the shortcomings of password-authentication systems arise from human memory limitations. Human memory for sequences is temporally limited, with a short-term capacity of around seven, plus or minus two items. In addition, when humans do remember a sequence of items, those items must be familiar chunks such as words or familiar symbols. Finally, human memory thrives on redundancy and is much better at remembering information encoded in multiple ways (Yan et al2004).

In a survey conducted by Brown et al (2004) to evaluate the generation and use of passwords, it was found that students in their study had an average of 8.18 password uses. These included the use of passwords to access Internet accounts, as well as for ATM access, cell phone access, etc. The most common items requiring passwords were (in order of frequency) e-mail, voice mail, ATM, access to mainframe and the Internet. With 4.45 different passwords to cover these functions, the average password had 1.84 applications. Two thirds of the passwords were designed around the respondents' personal characteristics, with most of the remainder relating to relatives, friends or lovers. Proper names and birthdays were the primary information used in constructing passwords, accounting for about half of all password constructions. Almost all respondents reused

passwords, and about two thirds of password uses were duplications.

In order to serve as an effective authentication method, passwords must be strong, secret, and memorable (Wiedenbeck et al, 2005; Bellovin, 2006). 'Strong' passwords are those that are difficult for others to guess; 'secret' passwords are hard for others to locate and obtain; and 'memorable' passwords are those that users can easily remember. As a knowledge-based authentication mechanism, passwords depend on human memory. Yet, the increasing complexity and quantity of passwords make it nearly impossible for users to remember all of their passwords. Hence, users trade security for memorability. The effectiveness of password authentication can be jeopardized by end-users' mispractice, which is an inevitable consequence of human memory limitations.

Mispractice, including choosing weak passwords, writing passwords down, and using a common password for multiple accounts, has been widely reported in a variety of security surveys (Zhang et al, 2009). User-created passwords are usually neither strong nor secret (Warkentin et al, 2004; Wiedenbeck et al., 2005; Vu et al, 2007). In fact, the top 10 passwords used on the Internet are all weak passwords (PC Magazine, 2007). When IT-enforced policies require users to choose strong passwords, users often write their passwords on a Post-it note stuck to the monitor, thereby compromising secrecy and defeating the purpose of having a password. 66% of managers have observed employees writing passwords down on paper at work (RSA, 2006). Furthermore, a recent Kaspersky security survey found that more than 50% of respondents use only one to four passwords, suggesting that password reuse is a common practice (PCPRO, 2007).

Despite the drawbacks, passwords are likely to remain the dominant authentication technology (Wiedenbeck et al., 2005). While alternative authentication methods exist such as public key encryption, one-time logon tokens and biometric authentication, each would require widespread adoption of a variety of standards and hardware devices. Hence, the issues of reliability, privacy, and cost prevent these methods from being widely deployed. According to the 2007 Computer Security Institute (CSI) survey, only 18% of companies use biometric technologies and 35% use smart card/one-time tokens. On the other hand, 51% of companies use traditional password-based authentication. Furthermore, many other security-oriented technologies incorporate passwords to some extent, and, therefore, using them does not eliminate the issues related to memorability.

The research, as discussed in this section, highlights the issues around the use of passwords in accessing protected information. Given the sensitivity of the information that the users gain access to by supplying a valid password such as banking details, one might expect users to consciously create very secure passwords. As was discussed in this section, this has not proven to be the case, with many studies concluding that users consistently use very simplistic, easily predictable practices when constructing and using passwords. Such predictable and systematic practices are easier for the user to remember, but they sacrifice the security that passwords are intended to provide.

## 3. METHODOLOGY

The methodology used in carrying out this study is presented below.

### 3.1. POPULATION

This work is limited to Lagos State residents who carry out online banking transactions. This is because Lagos State was selected by CBN for the pilot scheme of the cashless policy which commenced on April 1, 2012.

### 3.2. SAMPLE SIZE

The study is supposed to cover all residents of Lagos State who carry out online banking transactions but due to difficulty in reaching out to them on individual basis, the researchers made use of the branches of the banks in the twenty (20) Local Government Areas (LGAs). One thousand two hundred (1,200) questionnaires were randomly distributed to the banks in each of the 20 LGAs. This brings the total number of questionnaire administered to 24,000 (twenty-four thousand) out of which a total of 20,025 (twenty thousand and twenty-five) were returned. The response rate of 83.44% was considered sufficient enough to draw meaningful conclusions.

### 3.3. RESEARCH INSTRUMENT

The research instrument used for this study is the questionnaire. The questionnaire was developed on the basis of the good password practices identified from the literature study to assess the current practices employed by users when they select and use passwords to access information. The questionnaire focused on identifying the password practices employed in accessing on-line accounts or information that requires users to identify themselves by providing valid passwords. When the questionnaire was designed, a number of questions were compiled to identify how users currently use passwords (e.g. the number of accounts they use that require passwords, whether they use the same password for more than one account and whether they change their passwords on a regular basis). A number of questions were also designed to identify how users currently choose or select their passwords.

### 3.4. VALIDATION OF RESEARCH INSTRUMENT

The questionnaire was distributed to experts for validation. They were requested to consider the questionnaire in terms of logic, clarity and intelligibility. Minor corrections were made on the basis of their feedback.

### 3.5. RELIABILITY OF RESEARCH INSTRUMENT

The test-retest method was used to test the reliability of the questionnaire. Scores from the two sets of questionnaire were subjected to a simple correlational analysis where a correlation coefficient of 0.92 was obtained thus signifying a reliable questionnaire.

## 4. ANALYSIS AND RESULTS

Table 1 shows that out of 20,025 respondents, 61.33% are male while 38.67% are female.

*Table 1: Demographic Analysis of the total respondents*

| Sex | No. of Respondents | Percentage of respondents |
|---|---|---|
| Male | 12282 | 61.33% |
| Female | 7743 | 38.67% |
| Total | 20025 | 100.00% |

Further analyses were divided into two major groups:

(vi) Those that have one online account, referred to as *Single Online Account* as shown in 4.1; and

(vii) Those that have more than one online account, referred to as *Multiple Online Accounts* as shown in 4.2.

### 4.1. SINGLE ONLINE ACCOUNT ANALYSIS

Out of 20,025 respondents, a total of 7,209 respondents representing 36.00% indicated that they operate one online account. Detail analyses of this group of one online account are presented in Tables 2 to 7.

Table 2 shows that out of 7,209 respondents that operate one online account, 70.37% are male while 29.63% are female.

*Table 2: Demographic Analysis of Single Online Account holders*

| Sex | No. of Respondents | Percentage of respondents |
|---|---|---|
| Male | 5073 | 70.37% |
| Female | 2136 | 29.63% |
| Total | 7209 | 100.00% |

*Table 3: Character Length of Password*

| Character Length | No. of Respondents | Percentage of Respondents |
|---|---|---|
| 1 – 6 | 4005 | 55.56 |
| 7 – 8 | 801 | 11.11 |
| 9 – 10 | 1602 | 22.22 |
| 11 – 12 | 534 | 7.41 |
| Above 12 | 267 | 3.70 |
| Total | 7209 | 100.00% |

Table 4 shows that 88.90% of single online account holders do not change their password once created while 7.40% that manage to change theirs, construct closely related password.

### 4.2. MULTIPLE ONLINE ACCOUNTS ANALYSIS

Out of 20,025 respondents, a total of 12,816 respondents representing 64.00% indicated that they operate more than one online account. Detail analyses of this group of multiple online accounts are presented in Tables 8 to 13.

*Table 4: Pattern of Changing the Single Password for the Single Online Account*

| Methods | No. of Respondents | Percentage |
|---|---|---|
| Do not change Password | 6408 | 88.90 |
| I change the password but construct closely related | 534 | 7.40 |
| I change but construct entirely different password | 267 | 3.70 |
| Total | 7209 | 100.00 |

*Table 5: Password Storage Techniques*

| Sn | Password Storage | YES | % | NO | % |
|---|---|---|---|---|---|
| 1 | Commit it to my memory | 6408 | 88.89 | 801 | 11.11 |
| 2 | Write it down somewhere (e.g. Post-it, diary etc) | 1068 | 14.81 | 6141 | 85.19 |
| 3 | Online password managers (e.g. Gator eWallet, PasswordSafe.com) | 0 | 0.00 | 7209 | 100.0 |
| 4 | Software password managers (e.g. Password Agent, Password Tracker) | 0 | 0.00 | 7209 | 100.0 |

*Table 6: Password Management Techniques*

| Duration before Changing Password | No. of Respondents | Percentage |
|---|---|---|
| 2 – 3 weeks | 267 | 3.70 |
| 1 month | 267 | 3.70 |
| 2 – 3 months | 0 | 0.00 |
| 4 – 6 months | 267 | 3.70 |
| I never change my password once created | 6408 | 88.90 |
| Total | 7209 | 100.00% |

Table 8 shows that out of 12,816 respondents that operate more than one online account, 56.25% are male while 43.75% are female.

### 4.3. DISCUSSION OF RESULTS

#### *4.3.1. Password Construction Methods for Multiple Online Accounts*

The poor practice most frequently cited in the literature is using the same password for more than one secure online account. The results depicted in Table 10 display the responses for those respondents with two or more accounts requiring passwords. Of the respondents, 18.75% indicated that they used the same password to access other accounts while 25.00% used closely related password to access each account.

This reinforces the findings of Moshfeghian and Ryu (2012), Zhang et al (2009), Wessels and Steenkamp (2007), Gaw and Felten (2006), Dhamija and Perrig (2000) that end-users make use of similar passwords to access multiple online accounts.

### *4.3.2. Character Length of Password*

One of the most basic requirements of good password practice is that the password should consist of at least eight characters or considerably more (DeBolt, 2012; Yan et al,2004).With this in mind, respondents were asked to indicate the length of the password used to access their account. Of the respondents, 55.56% used passwords that are between 1 to 6 characters long for those with more than one account while 54.16% used passwords that are between 1 to 6 characters long for those operating one account as shown in tables 3 and 9 respectively.

*Table 7: Password Selection Practices*

| Sn | Password Selection Practices | YES | % | NO | % |
|---|---|---|---|---|---|
| | Weak Password Practices | - | - | - | - |
| 1 | Lowercase letters only | 2937 | 40.74 | 4272 | 59.26 |
| 2 | Personally meaningful words (e.g. pets, street addresses etc) | 1602 | 22.22 | 5607 | 77.78 |
| 3 | Personally meaningful numbers (e.g. birthdates, phone numbers etc) | 1068 | 14.81 | 6141 | 85.19 |
| 4 | A Standard word in ANY dictionary | 534 | 7.41 | 6675 | 92.59 |
| 5 | Names of friends, relatives, children, spouse | 0 | 0.00 | 7209 | 100.0 |
| 6 | Same character three or more times only (e.g. aaa or AAAA or 1111 or ???? etc) | 0 | 0.00 | 7209 | 100.0 |
| 7 | Geographical locations | 0 | 0.00 | 7209 | 100.0 |
| 8 | Simple sequence of characters only (e.g. 12345, qwerty) | 267 | 3.70 | 6942 | 96.30 |
| 9 | Names of famous people | 0 | 0.00 | 7209 | 100.0 |
| 10 | My name/surname | 534 | 7.41 | 6675 | 92.59 |
| 11 | Relate password to the web site you are on | 0 | 0.00 | 7209 | 100.0 |
| 12 | Login name, i.e., password is the same as username | 0 | 0.00 | 7209 | 100.0 |
| | Medium Password Practices | - | - | - | - |
| 13 | Numbers or digits only (e.g. 152) | 1335 | 15.52 | 5874 | 81.48 |
| 14 | Standard words, but in reversed order only (e.g. cat becomes 'tac') | 0 | 0.00 | 7209 | 100.0 |
| 15 | Uppercase letters only | 0 | 0.00 | 7209 | 100.0 |
| | Strong Password Practices | - | - | - | - |
| 16 | Numbers and special characters in place of letters (e.g. m@Tr!x) | 267 | 3.70 | 6942 | 96.30 |
| 17 | Special characters only (e.g. ^%,$) | 267 | 3.70 | 6942 | 96.30 |
| 18 | Capitalized word with numbers | 0 | 0.00 | 7209 | 100.0 |
| 19 | Uppercase and lowercase letters mixed up with numbers | 267 | 3.70 | 6942 | 96.30 |
| 20 | Mnemonic phrases arranged in a mixture of uppercase, lowercase and numbers | 0 | 0.00 | 7209 | 100.0 |
| 21 | Spaces | 0 | 0.00 | 7209 | 100.0 |

*Table 8: Demographic Analysis of Multiple Online Account holders*

| Sex | No. of Respondents | Percentage of respondents |
|---|---|---|
| Male | 7209 | 56.25 |
| Female | 5607 | 43.75 |
| Total | 12816 | 100.00% |

*Table 9: Character Length of Password*

| Character Length | No. of Respondents | Percentage of Respondents |
|---|---|---|
| 1 – 6 | 6942 | 54.16 |
| 7 – 8 | 2937 | 22.92 |
| 9 – 10 | 1335 | 10.42 |
| 11 – 12 | 1335 | 10.42 |
| Above 12 | 267 | 2.08 |
| Total | 12816 | 100.00% |

*Table 10: Password Construction Methods for multiple online accounts*

| Methods | No. of Respondents | Percentage |
|---|---|---|
| I use the same password | 2403 | 18.75 |
| I construct closely related password for each account | 3204 | 25.00 |
| I construct entirely different password for each account | 7209 | 56.25 |
| Total | 12816 | 100.00% |

*Table 11: Password Storage Techniques*

| Sn | Password Storage | YES | % | NO | % |
|---|---|---|---|---|---|
| 1 | Commit it to my memory | 11748 | 91.67 | 1068 | 8.33 |
| 2 | Write it down somewhere (e.g. Post-it, diary etc) | 3738 | 29.17 | 9078 | 70.83 |
| 3 | Online password managers (e.g. Gator eWallet, PasswordSafe.com) | 267 | 2.08 | 12549 | 97.92 |
| 4 | Software password managers (e.g. Password Agent, Password Tracker) | 1335 | 10.42 | 11481 | 89.58 |

*Table 12: Password Management Techniques*

| Duration before Changing Password | No. of Respondents | Percentage |
|---|---|---|
| 2 – 3 weeks | 0 | 0.00 |
| 1 month | 267 | 2.08 |
| 2 – 3 months | 267 | 2.08 |
| 4 – 6 months | 534 | 4.17 |
| I never change my password once created | 10947 | 85.42 |
| Others (Occasional, when prompted to do so etc) | 801 | 6.25 |
| Total | 12816 | 100.00% |

The average number of characters per password for single account and multiple accounts was 7.31 with a standard deviation of 2.27 and 7.15 with a standard deviation of 2.14 respectively. This is in line with the findings of Wessels and Steenkamp (2007), who reported an average number of characters per password to be 6.87 with a standard deviation of 2.27.

### *4.3.3. Password Storage Techniques*

Another "bad habit" noted in the password literature is writing down passwords. In response to being asked whether they wrote down their passwords, tables 5 and 11 depict the results of the respondents. From table 5, (single account users) 14.81% answered positively while in table 11 (multiple account users) 29.17% answered positively. This confirms the findings of Zhang et al (2009).

### *4.3.4. Password Management Techniques*

A further control measure advocated in the literature review is that passwords should be changed regularly. The literature does not always agree on the specific period, but that it should be changed is a general recommendation. The respondents were asked how long they normally kept their passwords unchanged. Tables 6 and 12 display the results of this question as 88.90% and 85.42% respectively, never changed their passwords. It appears that the discipline to regularly change passwords is lacking with 6.25% doing so only when prompted do so (table 12). Our findings supported that of Wessels and Steenkamp (2007) and Riley (2006) who reported that 68% and 52.7% of the respondents respectively do not change their passwords. It also confirms the finding of Jabbour et al (2011).

*Table 13: Password Selection Practices*

| Sn | Password Selection Practices | YES | % | NO | % |
|---|---|---|---|---|---|
| | Weak Password Practices | - | - | - | - |
| 1 | Lowercase letters only | 6408 | 50.00 | 6408 | 50.00 |
| 2 | Personally meaningful words (e.g. pets, street addresses etc) | 6141 | 47.92 | 6675 | 52.08 |
| 3 | Personally meaningful numbers (e.g. birthdates, phone numbers etc) | 8831 | 68.91 | 3985 | 31.09 |
| 4 | A Standard word in ANY dictionary | 801 | 6.25 | 12015 | 93.75 |
| 5 | Names of friends, relatives, children, spouse | 1869 | 14.58 | 10947 | 85.42 |
| 6 | Same character three or more times only (e.g. aaa or AAAA or 1111 or ???? etc) | 534 | 4.17 | 12282 | 95.83 |
| 7 | Geographical locations | 1335 | 10.42 | 11481 | 89.58 |
| 8 | Simple sequence of characters only (e.g. 12345, qwerty) | 2403 | 18.75 | 10413 | 81.25 |
| 9 | Names of famous people | 534 | 4.17 | 12282 | 95.83 |
| 10 | My name/surname | 1869 | 14.58 | 10947 | 85.42 |
| 11 | Relate password to the web site you are on | 267 | 2.08 | 12549 | 97.92 |
| 12 | Login name, i.e., password is the same as username | 801 | 6.25 | 12015 | 93.75 |
| | Medium Password Practices | - | - | - | - |
| 13 | Numbers or digits only (e.g. 152) | 1068 | 8.33 | 11748 | 91.67 |
| 14 | Standard words, but in reversed order only (e.g. cat becomes 'tac') | 534 | 4.17 | 12282 | 95.83 |
| 15 | Uppercase letters only | 0 | 0.00 | 12816 | 100.0 |
| | Strong Password Practices | - | - | - | - |
| 16 | Numbers and special characters in place of letters (e.g. m@Tr!x) | 801 | 6.25 | 12015 | 93.75 |
| 17 | Special characters only (e.g. ^%,$) | 0 | 0.00 | 12816 | 100.0 |
| 18 | Capitalized word with numbers | 267 | 2.08 | 12549 | 97.92 |
| 19 | Uppercase and lowercase letters mixed up with numbers | 1602 | 12.50 | 11214 | 87.50 |
| 20 | Mnemonic phrases arranged in a mixture of uppercase, lowercase and numbers | 534 | 4.17 | 12282 | 95.83 |
| 21 | Spaces | 0 | 0.00 | 12816 | 100.0 |

*4.3.5. Password Selection Practices*

The respondents were provided with a list of 22 possible practices that they could follow when constructing a password. They were asked to indicate which of the 22 possibilities they used when constructing a password. Respondents were able to select all the applicable possibilities, resulting in the total being more than the number of respondents. Tables 7 and 13 are the summary of the results that are sorted on the basis of the strength of the particular password practice. The result of this survey reinforces the expectation that passwords are chosen so that they can be easily remembered (e.g. Personally meaningful numbers (68.91% as seen in table 13)), and not necessarily on the basis of what is recommended as good and secure practice. 7.4% (table 7) and 14.58% (table 13) of the respondents used their own names as passwords which compared favourably to 15% reported by Brown et al (2004). This finding shows that users' do not adhere to good password practices such as those put forward by Adelaide University (2012).

### 4.4. IMPLICATIONS FOR NIGERIA'S CASHLESS SOCIETY

(i) The implication of using the same password for more than one secure online account is that should the one password be compromised, the entire accounts will be in jeopardy. Transactions will be carried out in all the accounts with ease in a cashless society. For those that are closely related, cracking one will serve as a clue to others.

(ii) The findings also reveal that the number of characters per password and that of character length where more than half of the respondents have their passwords between 1 to 6 fall below the international best practices and thus will have negative effect on the cashless society.

(iii) With 29.17% of respondents indicating that they wrote down their passwords in order to remember them ( table 11), it calls for great concern as we march into cashless society. Writing down password implies that the password has been compromised. The implication of this for our cashless economy is that it will boost the activities of cyber-criminals.

(iv) Since the discipline to regularly change the password is lacking, it means that if the password is compromised, the account could be accessed for considerable periods of time. Again, this is not good for our cashless economy.

(v) The practice of using personally meaningful numbers, ones own name etc as passwords is a serious mispractice that if not discouraged, will jeopardize the cashless policy of CBN.

## 5. RECOMMENDATIONS, CONCLUSION AND FUTURE WORK

### 5.1. RECOMMENDATIONS

The findings of this survey highlight the password problems that bank customers in Nigeria are likely to face should the CBN goes ahead to implement the cashless policy. To reduce the problems, the following recommendations are suggested.

(a) CBN or government should establish an Agency that will be charged with the following functions:

(i) continued assessment/evaluation of the cashless policy with a view for improvement;

(ii) conduct regular research on the efficiency of the policy and make recommendations to government;

(iii) continuing education of all stakeholders as this is essential in order to maximally ensure security of customers' accounts;

(iv) ensure that independent security experts perform a security health check on banks and other financial institutions' IT infrastructure and PoS/ATM devices, and continuous security monitoring to cope with the dynamic nature of the online world; and

(v) develop ground rules and ensure that financial institutions attain Payment Card Industry Data Security Standards (PCI-DSS) certification.

(b) Since the current design of Password Selection Mechanism (PSM) does not help the user choose a good password, we recommend the feedback augmented PSM such as the progress bar that dynamically reflects the quality of the password, with a textual indicator that is updated at thresholds.

(c) Information managers should not rely solely on users to employ good password practices, but actively seek other means to enforce users to adhere to minimum best password practices such as forced changes of passwords on a regular basis, minimum length of passwords, disallowing the re-use of old passwords etc.

(d) Users should be made to be aware of the dangers of improper password management.

### 5.2. Conclusion and Future Work

This survey indicates that a typical Lagos State resident creates an average of 3.35 passwords. The majority of participants in this survey most commonly reported password generation practices that are simplistic and therefore very insecure. Particular practices reported include using lowercase letters, personally meaningful words and numbers, etc (tables 7 and 13). This includes birthdays, anniversary dates, telephone numbers, identity numbers, personal names, etc. that could be easily guessed with a basic knowledge of the

respondent's interests. The data collected in this study answer some questions but raise others for future research. The recommendations serve as potential starting point for future research.

## ACKNOWLEDGEMENTS

This work was supported in part by Tertiary Education Trust Fund (TETFund), Abuja Nigeria (formerly called ETF) and TWAS-AAS-MICROSOFT. Any opinions, findings, conclusions or recommendations expressed in this paper are those of the authors and do not necessarily reflect the views of TETFund or TWAS-AAS-MICROSOFT or both.

## REFERENCES

Adelaide University., 2012. Password Policies Guide from www.adelaide.edu.au/... Date visited 25/05/12

Alkhalifah, A. and Skinner, G. D., 2010. Enhanced Knowledge Based Authentication Using Iterative Session Parameters, *In World Academy of Science, Engineering and Technology*, pp 293 – 299.

Andrews, L. W., 2002. Passwords Reveal your Personality, *In Psychology Today*, Vol. 35, pp 12 – 20.

Armstrong, L., 2002. And the Password is …#%?&! Business Week from www.businessweek.com/magazine/content/o2 Date visited 23/01/12

Bellovin, S., 2006. Unconventional Wisdom, *In IEEE Security & Privacy*, Vol. 14, No. 1, pp 88-95.

Brown, A.S. et al, 2004. Generating and Remembering Passwords, *In Applied Psychology* Vol. 18, No. 6, pp 41-52.

Butler, R., 2005. Avoid the hook in the Phisherman's bait, *In Accountancy SA*, pp 16-22.

CSI., 2007. The 12th Annual Computer Crime & security survey from www.i.cmpnet.com/v2 Date visited 23/01/12

DeBolt, D., 2012. Password Best Pracctices from www.totaldefense.com/blogs/... Date visited 25/05/12

Deloitte Security Survey., 2007. The 2007 Technology, Media and Telecommunications Security Survey, from www.deloitte.com/dtt/cda/dx/content/dtt_tmt_security survey2007.pdf Date visited 18/03/11

Dhamija, R. and Perrig, A., 2000. Using Images for Authentication, *Proceedings of the 9th USENIX Security Symposium*.Denver, Colorado, USA pp. 137- 150.

Divyans, M., 2009. Secure Password Entry Scheme in ATM Network which is Resistant to Peeping Attacks, *In International Journal of Engineering and Technology*, Vol 1 No. 2, pp 142 – 155.

DTI Survey., 2006. DTI Information security breaches survey from www.pwc.co.uk/pdf/ Pwc_dti_fullsurveyresults06.pdf Date visited 12/01/11

Edet, O., 2008. Electronic in Banking industries and its effects, *In International Journal of Investment and Finance*, Vol 3, pp 62-70.

Florencio, D. and Herley, C., 2010. Where Do Security Policies Come From? Proceedings of SOUPS. Redmond, WA, USA, pp. 1-14

Florencio, D. and Herley, C., 2007. A Large-Scale Study of Web Password Habits.*Proceedings of 16th International Conference on WWW*. USA, pp. 120-129.

Florencio, D. et al, 2007. Do Strong Web Passwords Accomplish Anything? *Proceedings of USENIX Hot Topics in Security*. USA, pp. 97-107.

Gaw, S. and Felten, E. W., 2006. Password Management Strategies for Online Accounts.*Proceedings of the 4th Symposium On Usable Privacy & Security, (SOUPS)*. Pittsburgh, PA, USA, pp. 1-12.

Gehringer, E. F (2002) Choosing Passwords: Security and Human Factors.*Proceedings of International Symposium on Technology and Society (ISTAS).*USA, pp. 39-59.

Hayashi, E. and Jason, I. H., 2006. A Diary of Password Usage in Daily Life, Technical Report No. 5000, Carnegie Mellon University, USA, pp. 1- 5.

Inglesant, P. and Sasse, M. A. 2010. The True Cost of Usable Password Policies: Password Use in the Wild, *Proceedings of association for Computer Machinery (ACM) Conference on Human-Computer Interaction (CHI).* USA, pp. 56-70.

Information Week., 2007. InformationWeek/Acceture Global information security survey from www.informationweek.com/whitepaper/security/privacy Date visited 22/03/12

Jabbour, R. et al. 2011. Better Passwords Get with the Beat. *In International Journal of Internet Technology and Secured Transactions,* pp. 20-28

Kuo, C., 2006. Human Selection of Mnemonic Phrase-based Passwords.*Proceedings of SOUPS* .Pittsburgh, USA, pp. 22-34.

Moshfeghian, S. and Ryu, V. S., 2012. Your Password is Invalid: Improving website Password Practices. In Science Daily from www.sciencedaily.com/release/ 2012/01/… Date visited 25/05/12

PC Magazine., 2007. 10 most common passwords, from www.pcmag.com/article2/02817 Date visited 23/01/12

PCPRO., 2007. Password re-use opens door to ID theft, from www.pcpro.co.uk/news Date visited 23/01/12

Perkovic, T. et al, 2009. Shoulder-Surfing Safe Login a Partially Observable Attacker Model, Technical Paper, FESB University of split, pp. 1 – 8

Rabkin, A., 2008. Personal Knowledge Questions for fallback Authentication: Security questions in the era of Facebook, *Proceedings of SOUPS*. USA, pp. 139-148.

Riley, S., 2006. Password Security: What users know and what they actually do. *Usability News* Vol. 8, No. 1 from www.psychology.wichita.edu/sur/usabilitynews/81/passwords.html Date visited 20/08/11

RSA., 2006. RSA Security Research shows volume of business passwords overwhelming end users and hindering IT security efforts, from www.rsa.com/press_release Date visited 23/01/12

Schneier, B., 2004. Customers, passwords and websites, *In IEEE Security & Privacy*, from www.schneier.com/essay-048.html Date visited 20/08/11

Shay, R. et al, 2010 Encountering Stronger Password Requirements: User attitudes and Behaviours. *Proceedings of SOUPS*. Canada, pp. 123-133.

Vu, K.P.L. et al, 2003. Imposing password Restrictions for multiple accounts: impact on generation and recall of passwords.*Proceedings of the 47th annual meeting of the Human Factors & Ergonomics Society*. Santa Monica, pp. 234-244.

Vu, K.P.L. et al, 2007. Improving password Security and memorability to protect personal and organizational information, *In International Journal of Human-Computer Studies*, Vol. 65, pp 744 – 757.

Warkentin, M. et al, 2004. Introducing the Check-off Password System (COPS): An Advancement in user authentication methods and information security, *In Journal of organizational & End user Computing*, Vol. 16, No. 3, pp 41 – 58.

Wedenbeck, S., Waters, J., Birget, J.C., Brodskiy, A &Memon, N (2005) Passpoints: Design and Longitudinal Evaluation of Graphical password System, *In International Journal of Human-Computer Studies*, Vol. 63, pp 42-49.

Wessels, P.L. &Steenkamp, L.P (2007) Assessment of Current Practices in creating and using passwords as a control mechanism for information Access, *In South African Journal of Information Management*, Vol. 9, No. 2, pp 1-15.

Yan, J., Blackwell, A., Anderson, R & Grant, A (2004) Password Memorability and Security: Some Empirical Results, *In IEEE Security & Privacy* from www.ieeexplore.ieee.org/iel5/8013/29552/0134406.pdf Date visited 20/08/11

Zhang, J., Luo, X., Akkaladevi, S &Ziegelmayer, J (2009) Improving Multiple-Password Recall: An Empirical Study, *In European Journal of Information Systems*, Vol. 8, pp 165 – 176.

# ADDRESSING PRIVACY IN ONLINE BANKING AND TRANSACTIONS IN NIGERIA'S CASHLESS SOCIETY

***B. K. Olorisade**
Mathematics & Computer Sc. Dept.,
Fountain University, Osogbo
gasimbabatunde@yahoo.co.uk

**R. A. Azeez**
Mathematics & Computer Sc. Dept.,
Fountain University, Osogbo
ajeazeez@yahoo.com

***ABSTRACT***

*The Internet is getting increasingly popular as a technological driven channel to retail products and services. Consequently, e-commerce is getting adopted even in developing countries. Nigeria, through its central bank recently announced a new cashless policy for the nation starting with some states. This puts a cap on the daily cash withdrawal or deposit for individual and corporate entities. But the challenge has always been in people's reluctance to adopt e-commerce for security reasons. Security and privacy have always been a challenge to e-commerce or online transactions generally. There is no doubt Nigeria will have its own share of it. The use of static username and password or PIN for ATM cards is not sufficient to protect a customer's privacy or guard against online fraud. Multi-factor authentication techniques have thus been proposed to reinforce static password. In line with this, some Nigerian banks currently give a token device to customers providing two-factor security measure. But this is not the only possible option. In this paper, we review the current state of internet banking in Nigeria vis-à-vis privacy protection issues and bring to fore, use of one time password, card-based authorization codes, transaction password and digital certificate as some other options to addressing customer privacy in online banking and transaction in Nigeria.*

***Keywords***:*E-commerce, identification, security, two-factor authentication*

## 1. INTRODUCTION

As the Internet is getting increasingly popular as a means of technology driven distribution channel for retail products and services and banking services, there is a corresponding noticeable growth and awareness of e-commerce like Internet banking and electronic payment system in developing countries (Susanto and Zo, 2011). Nigeria is not left out of the continuous emergence and wider acceptance of e-commerce. This is apparent in the new cashless policy of the Central Bank of Nigeria (CBN) which among others puts a cap on the individual and corporate daily cash bank transactions in order to encourage wide adoption of e-commerce (CBN, 2011).

In situations like this, potential e-bank customers and online shoppers (referred to as consumers in some cases) have shown reluctance in making decisions to accept and adopt e-commerce. This is largely influenced by how they perceive trust, security and privacy in the electronic system (Susanto and Zo, 2011, Ayo et al., 2010, Adepoju and Alhassan, 2010, Adel, 2001, Pan and Zinkhan, 2006, Miyazaki and Fernandez, 2001, Duh et al., 2002); cultural background may also have a role to play sometimes (Pennanen et al., 2008, Pennanen et al., 2006). Most are usually reluctant to provide online service providers with sensitive personal information which is a prerequisite to transact online not only because of security but also trust (Suh and Han, 2002, Oghenerukevbe, 2008, Susanto and Zo, 2011) and reliability (Miyazaki and Fernandez, 2001).

Due to increasing rate of electronic theft, multi factor access control (authentication) was introduced to complement the inefficiencies of static password and username which are the primary protection means in internet based banking and transaction (Oghenerukevbe , 2010). Generally, before a consumer can engage in online transaction, s/he must first create an account with a username and password as a security and privacy assurance method. However, it implies that if a username and corresponding password is exposed through negligence or more technical means like snooping, phishing, etc. the account is compromised and the level of damage may be unquantifiable unless caught in time. The Antiphishing working group report of first half 2011 shows financial and payment services as the most targeted industry sector for online attacks (Figure 1).

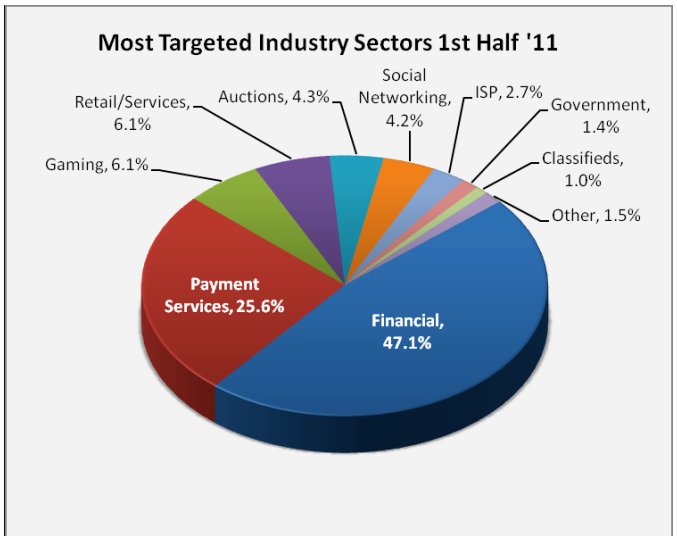



*Figure 1: Most targeted industry sectors according to APWG trends report H1 2011*

The use of this static method has proved useful but is inadequate to protect consumers thus need to be reinforced. Therefore, the suggestion that a multi-factor authentication means is introduced to fortify the static password and username and establishing personality identity (Oghenerukevbe, 2010).However, in Nigeria most efforts at providing a secondary level access control is still focused on Internet banking over other Internet transactions. Even, for the Internet banking, the most popular option is the use of token software. A token is a digital device that is capable of generating instant (random) codes on spot for use in online banking as at when needed. The generated code is required and validated before any transaction requiring authorization is executed in Internet banking. Not all the banks want or have implemented the token technology type as it exist in the industry. So, having options is a good thing for the industry in respect of Nigeria's drive towards a cashless society, same options is good for consumers as well.

This paper brings to fore, four of such techniques that can be utilized as a second level personal security technique useful in both online banking and transactions. Thus, proposing ways that can further assure privacy and confidentiality of information in aspiring cashless society like Nigeria. The methods are: one time pass-code, transaction password, card based pass-code and digital banking certificates.

## 2. LITERATURE REVIEW

World over, security and privacy has been and is still a concern when it comes to online transactions (Ackerman et al., 1999). Nigeria, making the move to join the cashless economies of the world is thus not going to be an exception. In addition, fraud rate in Nigeria or involving Nigerians is currently on the high (FITP, 2010), thus extra security measures might be necessary to ensure a fairly reliable cashless transaction and protect consumers' experience and property. In fact, globally online fraud is a major source of revenue to criminals. Anti-phishing group reported that phishing attacks occur at a constantly increasing rate (Meyer, 2007).

Security can be defined as a consumer's subjective feeling of being secure or safe (Pennanen et al., 2008). Privacy, on the other hand may mean "the claim of individuals, groups or institutions to determine for themselves when, how and to which extent information about them is communicated to others" (Pennanen et al., 2008). Consequently, security can be viewed as a means to accomplish and bolster privacy.

The persistent concern on security and privacy among e-commerce consumers has made it imperative for any meaningful and serious e-commerce based organizations to address these. Several techniques have been implemented on how to address security and privacy issues in e-commerce but no single organization can adopt all. Choice of adoption is usually based on the characteristics, focus or policies of such organization or society.

In any case, it is imperative for organizations to fortify their system security or adjust policies to favor more privacy assurance in order to further gain consumer trust.

Multi-factor authentication adopts a combination of two or more different factors for verifying user's identity. That is, a combination of something you know and something you have or are. This approach has the following potential benefits:

(i) Enhanced security: it is impossible for impostors to steal what you possess (like a card, device etc.) over the Internet.
(ii) Protection for high risk transactions: all high risk Internet transactions are protected by an additional authentication factor that is physically held by the legitimate customer.
(iii) Convenient and easy to use: these options are easy to use and can guarantee more security online.

This approach has been adopted by Nigerian banks but to a limited extent when it comes to online retail of product and services as against online banking. The techniques proposed in this paper can complement the need for multi-factor authentication in online banking and retailing.

### 2.1 E-BANKING IN NIGERIA

Since 2004 when the CBN released the guidelines on e-banking in Nigeria (CBN, 2003), the banks have since begun the drive towards utilizing the IT/ICT to facilitate their operations. The Automated Teller Machine (ATM) is still the most popular and widely accepted or used electronic means of banking and transaction in the country (Adepoju and Alhassan, 2010, Ayo et al., 2010). The ATM card is protected with a 4-digit PIN known only to the card holder. This prevents illegal use of the card. The technique is good but has some noticeable weakness. For example, if an ATM card (or its number) falls into a wrong hand, this card can still be used for online transaction successfully without any recourse to the PIN known only to the user.

Another electronic means of banking or transaction gaining prominence is the Internet or online banking. In Internet banking, the bank customer creates a username and password known only to him/her. In addition to this, he/she is also issued a token (in some banks) for additional security. Tokens can be used to authenticate a user to a secure Web site.

The advent of the Internet revolutionized the way things are done before it, thus, Internet banking is bound to revolutionize the way Nigeria banks function, deliver services and even compete among one another (Oni and Ayo, 2010, Tan and Teo, 2000). Internet banking brings with it a whole lot of new transaction experience like fund transfer, goods and services purchase and payment, even rent or school fees payment, etc. all in the comfort of one's room. It is easy, convenient, relatively cheaper and fast (Agboola, 2006, Oni and Ayo, 2010) and easy to use (Suh and Han, 2002). If anything, it is helping deliver services better and faster and increase the flexibility of their business delivery (Ayo et al., 2010). Thus, it is bound to grow continuously. E-economy has actually been prophesized to be a global, pervasive and encompassing force, that will take over how business is conducted world over (Adekunle and Tella, 2008).

In fact, it will change the scene of the banking industry. Also, it can help banks broaden their customer base and increase their customer retention rate (Ayo et al., 2010) and become a point for competitive edge (Agboola, 2006, Mukherjee and Nath, 2003).

## 2.2 CYBERCRIME IN NIGERIA

Since the introduction of the Internet, electronic financial and economic crime in Nigeria or associated to Nigerians has continue to rise (Gideon, 2002, FITP, 2010). An annual fraud analysis conducted by Cybersources in UK shows that 55% of participants (200 UK companies) indicated they will not ship their goods to Nigeria while 47% of digital-only companies (i.e, those shipping downloadable goods as opposed to physical ones) will not trade with anything originating from the country. Both results put Nigeria ahead of Ghana and the US (Wires, 2011).

Nigeria currently rates high in online crime, thus, privacy assurance mechanisms different from the regular passwords or PIN codes and enhanced up to date technology (Olasanmi, 2010) are well in line to further ensure client's privacy during online transactions. The methods proposed in this paper can be used by banks or card issuing organizations to guard against unauthorized use of client's cards for online purchases or access to bank accounts of clients online.

## 3.0 REINFORCEMENT OPTIONS FOR STATIC PASSWORD

As stated earlier, the primary means of authentication in online banking and transaction is the use of personal username and password. This method requires some reinforcement as research have shown people to stick to a routine in username and password choice. Also, the password and username can be stolen through different online fraud method like snooping, spoofing, phishing etc. which is now more paramount. Thus, the option of dynamic passwords or second level security password becomes inevitable.

One of the options to strengthen online transaction security that currently operate in Nigeria is the use of token as mentioned earlier. Some other possible options usable as secondary level security are highlighted in the following sections 4.1 – 4.4.

### 3.1 ONE-TIME PASSWORD

This is a series of randomly generated concealed 4-digit tokens issued by the bank to account holders for the purpose of online banking or transactions related to their ATM card. The numbers are pre-generated and concealed, thus, each will be scratched to reveal it only when it is required for use. The use of the codes must be strictly sequential. The codes are usually required as a secondary identity validation step to authorize customer online transaction requests. Usually, this is very useful for account holders who wish to access their accounts online on public computers. This technique is an alternative technique to the token currently issued by some banks in Nigeria. The one time password card may appear as shown in figure 1.

| Card no. y | | | | | | | some control information |
|---|---|---|---|---|---|---|---|
| 1 | xxxx | 11 | | 21 | | 31 | |
| 2 | xxxx | 12 | | 22 | | 32 | |
| 3 | xxxx | 13 | | 23 | | 33 | |
| 4 | xxxx | 14 | | 24 | | 34 | |
| 5 | | 15 | | 25 | | 35 | |
| 6 | | 16 | | 26 | | 36 | |
| 7 | | 17 | | 27 | | 37 | |
| 8 | | 18 | | 28 | | 38 | |
| 9 | | 19 | | 29 | | 39 | |
| 10 | | 20 | | 30 | | 40 | |

*Figure 1: Sample appearance of the pass code card*

The order of usage is strictly sequential from 1 through 40. A new card will be issued against the account as soon as the current one finishes. The cards are numbered and tracked accordingly. For each transaction request, a new code will be requested in the format:

*Enter the xth code of card 1.*

If the account holder's sign-on information is compromised, no transaction can take place on the account without knowing the next code in the sequence; that is, being in possession of the card. However, the lost of the card ordinarily pose no threat to the owner; if the account's personal information is not compromised, the consumer only need to report and order for a new card. If the card is not compromised, it is actually a useful protective means as statistically, a guess work of the next number has a probability of 1/10,000 chance of guessing the four numbers in a sequence correctly.

### 3.2 CARD-BASED AUTHORIZATION CODES

This is a set of codes organized in a matrix form used like the one-time password but in this case, the set of codes (2-digits) are printed on the backside of the debit or credit card (separate card but not concealed) configured against individual's account. This takes care of the need to renew exhausted cards or buy token software. The codes are a set of randomly generated numbers. It is requested occasionally when the customer is conducting any transaction on the Internet with his account or ATM card. The request serves as an additional authorization step for the transaction. The code is organized in matrix format (Figure 2).

Except if this card is lost or stolen, which the holder is expected to report immediately. The codes are a very powerful secondary security feature to supplement password and username in online banking since the possibility of a correct guess without holding the card is 1/100. The code request is of the form (row, column) e.g. (6,i)th code.

| | a | b | c | d | e | f | g | h | i | j |
|---|---|---|---|---|---|---|---|---|---|---|
| 0 | XX | XX | XX | XX | XX | XX | XX | XX | XX | XX |
| 1 | XX | XX | XX | XX | XX | XX | XX | XX | XX | XX |
| 2 | XX | XX | XX | XX | XX | XX | XX | XX | XX | XX |
| 3 | XX | XX | XX | XX | XX | XX | XX | XX | XX | XX |
| 4 | XX | XX | XX | XX | XX | XX | XX | XX | XX | XX |
| 5 | XX | XX | XX | XX | XX | XX | XX | XX | XX | XX |
| 6 | XX | XX | XX | XX | XX | XX | XX | XX | XX | XX |
| 7 | XX | XX | XX | XX | XX | XX | XX | XX | XX | XX |
| 8 | XX | XX | XX | XX | XX | XX | XX | XX | XX | XX |
| 9 | XX | XX | XX | XX | XX | XX | XX | XX | XX | XX |

*Figure 2: Set of matrix codes behind bank cards*

If the card is lost, the card owner is still protected if the account's personal information or card's security (like username, password, PIN) is not compromised. The use of this method may require some level of literacy and education but this is not a want for anybody that can engage in online banking or transaction.

### 3.3 TRANSACTION PASSWORD

A transaction password is an extra password created for the purpose of online transactions with the card issuing bank apart from the username and password for Internet banking or the account username and password with the online trader. At the final stage of transaction, the banks website is invoked just before the online payment for the bank's client identification and approval. On the bank's website, the customer will need to identify himself/ herself by supplying his/her transaction password registered for the card in use for final authentication. Failure to do so will terminate the payment process.

This is a very good way to protect and ensure the identity of online shoppers by their banks. This method can be employed alongside other techniques described in this paper. Though, this idea can be extended and employed in other techniques as well, as long as the payment card issuing company's website can be invoked at the payment confirmation point. However, this method is more appropriate for privacy protection in ecommerce since it is not inscribed on any physical document. So if someone's card falls into wrong hands, it can still not be used successfully to shop online without the transaction password. More importantly, verification of the transaction password is done on the secure website of the bank or organization that issued the card to be used. This technique has the advantage of identifying the consumer; it also provides the opportunity to analyze the transaction website against phishing.

### 3.4 DIGITAL CERTIFICATE

Digital certificate is electronic security software downloaded, installed and configured for bank customers who own personal systems by their banks. It is a token software unlike the digital token device currently in use by some banks in Nigeria.

On installation, the user will have to create an identity with a name and Personal Identification Number (PIN). This certificate will always be invoked to sign the user in to the banks secure website at log in. Also, the user will have to select an account (in case of multiple accounts or identity) and sign for the account every time a transaction requires authentication.

Once created, the certificate will be configured not only with the user's identity but also the system identity. The identity can then be exported into a USB drive for external storage. In case of system crash or format, the certificate will just need to be imported back into the system. This is an alternative to one time pass codes for customers accessing their account on public systems.

## 4.0 DISCUSSION

These techniques are actually relevant, needed and can work in Nigeria given the fact that some of the banks are already adopting similar methods of two factor authentication. Moreover, this is now the global standard because of increasing rate and sophistication of online fraud (Meyer, 2007). In 2005, US enacted a law mandating all financial institution to provide consumers dealing in any form of online financial services with at least two-factor authentication (Meyer, 2007). In South Korea, users are obliged to install proprietary security software for protection (Huh, 2010), in Hong Kong all financial institutions were also advised on measures to combat or reduce online fraud and further protect consumers (Lau et al., 2004). Similar practices abound all over the developed nations of the world.

Though, it will be interesting if a form of handshaking exists between the e-commerce providers and the card issuing banks in user identification like is done while using the transaction password. This will make all the techniques adaptable as online transaction user identification means as against being used only for Internet banking.

## 5.0 CONCLUSION

Nigeria is currently aggressive in its drive towards cashless society. The implementation of this starts way back 2004 when Nigerian banks started electronic banking after the CBN released electronic banking guidelines in 2003. The step is now more apparent with the new CBN directive placing a cap on the cash transactions allowed in the country beginning 2012. Consequently, the issue of ecommerce security and privacy become all more important. This has surfaced since the advent of Internet and is more pertinent in e-commerce because of the sensitivity of data involved and loss associated with its risk. Multi factor authentication means have thus been proposed to complement static username and password to protect e-commerce patrons.

In Nigeria, only the token software is popular yet, as a two-factor authentication technique. In this paper, we presented four possible other options that can be adopted by Nigerian banks as user identification measure to further secure the privacy of the intending adopters of e-commerce - internet banking and online shopping. The methods are: one time password, card based codes, digital certificate, which are tailored more towards internet banking and transaction password which is meant for second level protection in online shopping.



**REFERENCES**

FITP, 2010. Security and Risk Landscape of Internet Banking in Nigeria. Available: www.financeinfotech.com/security-and-risk-landscape-of-internet-banking-nigeria/.

Ackerman, M. S., Cranor, L. F. & Reagle, J. 1999. Privacy in e-commerce: examining user scenarios and privacy preferences. *Proceedings of the 1st ACM conference on Electronic commerce.* Denver, Colorado, United States: ACM.

Adekunle, P. A. & Tella, A. 2008. Nigeria SMEs Participation in Electronic Economy: Problems and the Way Forward. *Journal of Internet Banking and Commerce,* 12**,** 1-13.

Adel, A. M. 2001. Online banking: a field study of drivers, development challenges, and expectations. *International Journal of Information Management,* 21**,** 213-225.

Adepoju, A. S. & Alhassan, M. E. 2010. Challenges of Automated Teller Machine (ATM) Usage and Fraud Occurrences in Nigeria – A Case Study of Selected Banks in Minna Metropolis. *Journal of Internet Banking and Commerce,* 15**,** 10.

Agboola, A. A. 2006. Electronic Payment Systems and Tele-banking Services in Nigeria. *Journal of Internet Banking and Commerce,* 11, 1-10.

Ayo, C. K., Adewoye, J. O. & Oni, A. A. 2010. The State of e-Banking Implementation in Nigeria: A Post-Consolidation Review. *Journal of Emerging Trends in Economics and Management Sciences (JETEMS),* 1**,** 37-45.

CBN 2003. Guidelines on Electronic Banking in Nigeria. *In:* NIGERIA, C. B. O. (ed.). Central Bank of Nigeria.

CBN 2011. Questions and Answers on the CBN Policy on Cash Withdrawal/Lodgement Limit. *In:* NIGERIA, C. B. O. (ed.). Abuja: CBN.

Duh, R.R., Jamal, K. & Sunder, S. 2002. Control and Assurance in E-Commerce: Privacy, Integrity, and Security at e-BAY. *Taiwan Accounting Review,* 3, 1-27.

Gideon, F. 2002. U.S. warns Nigeria over online fraud schemes. Available: www.crime-research.org/news/2002/09/Mess2801.htm [Accessed 1/15/2012].

Huh, J. H. 2010. On the Security of Internet Banking in South Korea.

Lau, K. C., Tam, C., Ho, J. & Fung, W. W. 2004. Identity Theft: Phishing, Email Scams Fake Websites. *In:* ISACA (ed.). Hong Kong: EMA Project Team.

Meyer, R. 2007. Secure Authentication on the Internet. *SANS Institute InfoSec Reading Room* [Online].

Miyazaki, A. D. & Fernandez, A. 2001. Consumer Perceptions of Privacy and Security Risks for Online Shopping. *The Journal of Consumer Affairs,* 35**,** 27-44.

Mukherjee, A. & Nath, P. 2003. A model of trust in online relationship banking. *International Journal of Bank Marketing,* 21**,** 5-15.

Oghenerukevbe, E. A. 2008. Customers Perception of Security Indicators in Online Banking Sites in Nigeria. *Journal of Internet Banking and Commerce,* 13**,** 14.

Oghenerukevbe, E. A. 2010. Mnemonic Passwords Practices in Corporate Sites in Nigerian. *Journal of Internet Banking and Commerce,* 15**,** 11.

Olasanmi, O. O. 2010. Computer Crimes and Counter Measures in the Nigerian Banking Sector. *Journal of Internet Banking and Commerce,* 15**,**1-10.

Oni A. & Ayo, C. 2010. An Empirical Investigation of the Level of Users' Acceptance of E-Banking in Nigeria. *Journal of Internet Banking and Commerce,* 15**,**1-13.

Pan, Y. & Zinkhan, G. M. 2006. Exploring the impact of online privacy disclosures on consumer trust. *Journal of Retailing,* 82**,** 331-338.

Pennanen, K., Kaapu, T. & Paakki, M. K. Trust, risk, privacy, and security in ecommerce. 2006.

Pennanen, K., Paakki, M. K. & Kaapu, T. 2008. Consumers' views on trust, risk, privacy and security in e-commerce: a qualitative analysis. *Trust and New Technologies: Marketing and Management on the Internet and Mobile Media. Cheltenham: Edward Elgar***,** 108-126.

Suh, B. & Han, I. 2002. Effect of trust on customer acceptance of Internet banking. *Journal of the Association for Information Systems,* 1**,** 247-263.

Susanto, A. & Zo, H. 2011. Factors Influencing Users' Acceptance in Internet Banking Success: Proposing a Unified Model. *2nd International Conference on Networking and Information Technology IPCSIT* Singapore: IACSIT Press

Tan, M. & Teo, T. S. H. 2000. Factors influencing the adoption of Internet banking. *J. AIS,* 1**,** 5.

Wires, T. 2011. Nigeria, Ghana and US lead in onlinefraud - Report. *Daily Times NG.* Lagos: TheDaily Times of Nigeria PLC.

# A PRIVACY CONTROL OPTION FOR CALL CENTERS IN NIGERIA'S CASHLESS ECONOMY

***B. K. Olorisade**
Mathematics & Computer Sc. Dept.,
Fountain University, Osogbo
qasimbabatunde@yahoo.co.uk

**M. A. Ogunrinde**
Mathematics & Computer Sc. Dept.,
Fountain University, Osogbo
bukky2004_ui@yahoo.com

***ABSTRACT***

*Customers' trust has been identified as a factor that must exist for customers to embrace e-commerce. An effective, reachable and responsive call center is one key to gaining this trust for organizations or banks that rely on e-commerce. However, an issue with call centers is the proper identification of the caller so that sensitive information is not divulged to wrong persons. Thus, a second level security check is needed before resolving any issue or divulging any account or transaction related information to the caller. This is seen as a necessary step to guard against privacy intrusion, scam or identity theft. Therefore, this paper proposes the use of a 7-digit identification code issued to customers solely for the purpose of remote communication with the bank. At the point of service rendering, the customer will only need to supply the digits occupying two or three randomly selected positions out of the seven. We believe this will further strengthen the privacy of customers in the banks through the call centers.*

***Keywords****: Call Center, e-Commerce, customer privacy, identification code*

## 1. INTRODUCTION

An effective, reachable and responsive call center cannot be ruled out in any bank or organization that relies on e-commerce – internet banking, online shopping, phone banking etc. Therefore, as Nigeria moves towards becoming a cashless economy based on the pronouncement of the Central Bank of Nigeria (CBN), starting January 2012 (CBN, 2011), an effective call center for each of the banks and other business organizations is inevitable to instantly resolve any issues experienced by customers as at when required. An outstanding call center must be one of the hallmarks of any organization that will succeed in a cashless economy that Nigeria is currently evolving to because clients will need means of instantly reporting any suspicious and authorized transactions or even encountered problem(s) anytime of the day (FITP, 2010).

Consumer trust has been identified as a factor that must exist for consumers to embrace e-commerce (Adel , 2001, Adepoju and Alhassan, 2010, Ayo et al., 2010, Oghenerukevbe, 2008). This is evident from the fact that there are many with internet access, yet, they did not agree to sign up for e-banking talk less of online shopping. Statistically, Shao (Shao, 2007)reported that only 44% of internet users in the United States adopt online banking while in China it was reported to be only 14% . This may be adduced to the fact that these people did not trust the system's security (Dauda et al., 2007, Susanto and Zo, 2011) and reliability enough to embrace e-commerce. Customers are afraid of identity theft through various means (Oghenerukevbe, 2010, Longe and Chiemeke, 2008), hacking, phishing (Adepoju and Alhassan, 2010) and other internet abuse techniques (Oghenerukevbe, 2008), all means of infiltrating systems and stealing sensitive information.

Thus, banks need to further protect their customer's privacy and gain their trust. Trust is a critical factor in an online environment. In order to gain customer trust, banks must build an economic relationship with them (Nor and Pearson, 2007) even in a cashless society. The primary source of such relationship building is a reliable customer care center. An enhanced customer care center will give any bank an edge over others and the power to face the pressure of expansion and growth with limited liability (Genesys, 2008, Adesina and Ayo, 2010). A good call center is important because customer satisfaction is proportional to a bank's growth and cost reduction (Dauda et al., 2007, Adesina and Ayo, 2010). In fact, organizations engaging in e-commerce must be customer-centric to endure and develop (Microsoft, 2003).

A scenario of the call center operation in some countries: the call center agent only requests for the caller's National Identification Number (for citizens) or International Passport Number (for foreigners) to establish identity and access his/her record with the bank. But the use of these may be currently impracticable in Nigeria because not all citizens have either Passport or National Identification Number instead the caller's account number is used.

This information may not actually be enough to establish the true identity of the call. Therefore, there is a need for a secret personal second level identification means before private information or any needed assistance is offered over the phone. Thus, in this paper we propose the use of an assigned identification number as a second level confirmation of identity before rendering any service over the phone. This step we believe will increase the customer confidence in their adoption of e-commerce.

The paper is organized as follows: section 2 of this paper stresses the importance of call centers, section 3 discussed a scenario of call center operation. In section 4 we presents the private identification code as a means of strengthening customer privacy at call centers, while section 5 provides the concluding remarks.

## 2. CALL CENTER AND BANK OPERATIONS

Use of Information and Communication Technology (ICT) can improve banking efficiency and effectiveness (Adesina and Ayo, 2010). Thus, in 2004, the Central Bank of Nigeria (CBN) released guidelines for e-banking in Nigeria (CBN, 2003). Since then, Nigerian banks have embarked on vigorous moves to upgrade their facilities and systems taking advantage of the ICT and its available infrastructures to enhance and automate their operations. This move thus necessitated the introduction of central call centers as against the conventional customer care desk officers in each of their branches.

The call centers are essential to resolve as quickly as possible any possible issues that might arise in several areas of bank operations such as online banking and internet transactions. A more sophisticated and responsive call center is even now compulsory with the new CBN directive on the cashless economy. Bank customers engaging in online transactions because of their inability to move cash around due to the new policy must be able to get any arising issue or enquiry resolved on the spot as at when required without necessarily visiting any bank's branch.

The effectiveness of call centers in a cashless economy will go a long way to determine the success of the system and growth of individual organizations. These call centers are important because they provide a bridge between the tri-party of online transactions – the customer, environment and the internal operations of the organization (Mukherjee and Nath, 2003). They actually influence the service quality perception of the customer (Mukherjee and Nath, 2003).

The watchword for service quality should be: reliability, responsiveness, assurance, empathy (Broderick and Vachirapornpuk, 2002) and reachability. Call centers offer comfort and ease of use to customers thereby improving customer experience. They have the potential to replace customer care desks currently found in most banks as more people will prefer to resolve their issues remotely and instantly instead of visiting any branch, thereby, saving cost and time. For example, a report shows that two-third of customer interaction in the United Kingdom occurs through the call center (Mukherjee and Nath, 2003).

## 3. CALL CENTER SCENARIO

When contacting a call center, the first task is for the agent to identify the caller with as minimum information as possible. As said earlier, in Nigeria the agent will request for the caller's account number to establish his identity and access his/her record. This step needs to be strengthened because unauthorized persons with the knowledge of the account number can simply extract some information on the account through the call center.

Thus, we believe there is a need for a second level security check before resolving any issue or divulging any account related information to the caller. This is seen as a necessary step to guard against privacy intrusion, scam or identity theft.

Currently in Nigeria, some banks have adopted the second level privacy assurance concept but they request for information like home address or phone number which can still be known to anybody, other than the owner of the account. So, in our opinion, this is not a very strong security check for the purpose though it is a step in the right direction.

## 4. PRIVATE IDENTIFICATION CODE

The importance of an effective and efficient call center cannot be over emphasized in a cashless economy. It will help build customer trust; an aspect of the trust is privacy assurance i.e. only necessary account and personal information is exposed even to call center agents. Trust by customers can only be built or determined as seen exhibited in the bank's attitude and policies that guide their operation. For example, customers need assurance that the bank will thoroughly resolve the true identity of the person at the caller end before vital information about personal bank statements or financial issues are divulged. Trust is something that develop with time, therefore, banks should adopt practices that can further strengthen the trust level against risk threshold of customers (Ayo et al., 2010). A research has speculated that billions can be lost in sales in internet related business due to privacy concerns (Moores, 2005). Therefore, e-commerce organizations should show that they take customer privacy seriously (Pan and Zinkhan, 2006) for improved sales and performance.

So, we propose in this paper, the use of a private identification codes as against the request of general information like the phone number or home address as a second level privacy assurance step at call centers.

Apart from username and password used for internet banking or online transaction and ATM card PIN that should not be revealed to anybody by the owner irrespective of their position, banks managing a customer's account and card should issue a randomly generated 7-digit Private Identification Code (PIC) to customers. The customer is expected to keep this number save. It will come handy whenever the customer needs to resolve any sensitive issue through the call center.

The idea here is not for the customer to always repeat all the digits to the agent as a form of identification. When required, the system will automatically generate a prompt for at least two random digits of the seven digits (based on their position) from the PIC. These two digits must be correctly provided at once before any sensitive transaction or financial detail discussion is held with the caller.

We believe this step will add strength to the security trust level of bank customers as they will not only be seen as taking their privacy serious but actually doing it.

## 5. CONCLUSION

Call centers are an essential part of a cashless society. Usually, customers will want their issues resolved without leaving the point of incident. So, any bank determined to grow in a cashless environment must increase its customers' confidence by taking proper care of its call centers to make them reachable, responsive, and reliable with empathy for customers.

Customer trust is a key issue in online environment and this can be built through displayed customer-centric practices by the bank. Call centers have been identified as one of such

factors a bank can use to increase its relationship with customers. But releasing sensitive information to unidentified callers of the call centers can rub off on the relationship it is attempting to build.

Call centers need a second level personality identification means to guard against impostors. Currently, some banks' call centers request for information like phone number or home address as a second level security check. We believe these are still general, so this paper proposed the issuance of a 7-digit personal identification code mainly for remote identification with the bank. Whenever required, the bank's system through its agent will only prompt for the digits occupying two or three positions out of the seven. We believe this will further strengthen the privacy of customers in banks through the call centers.

## REFERENCES

FITP, 2010. Security and Risk Landscape of Internet Banking in Nigeria. Available: www.financeinfotech.com/security-and-risk-landscape-of-internet-banking-nigeria/.

Adel M. A. 2001. Online banking: a field study of drivers, development challenges, and expectations. International Journal of Information Management, 21, 213-225.

Adepoju, A. S. & Alhassan, M. E. 2010. Challenges of Automated Teller Machine (ATM) Usage and Fraud Occurrences in Nigeria – A Case Study of Selected Banks in Minna Metropolis. Journal of Internet Banking and Commerce, 15, 10.

Adesina, A. A. & Ayo, C. K. 2010. An Empirical Investigation of the Level of Users' Acceptance of E-Banking in Nigeria. Journal of Internet Banking and Commerce, 15, 13.

Ayo, C. K., Adewoye, J. O. & Oni, A. A. 2010. The State of e-Banking Implementation in Nigeria: A Post-Consolidation Review. Journal of Emerging Trends in Economics and Management Sciences (JETEMS), 1, 37-45.

Broderick, A. J. & Vachirapornpuk, S. 2002. Service Quality in Internet Banking: The Importance of Customer Role. Marketing Intelligence and Planning, 20, 327-335.

CBN 2003. Guidelines on Electronic Banking in Nigeria. In: NIGERIA, C. B. O. (ed.). Central Bank of Nigeria.

CBN 2011. Questions and Answers on the CBN Policy on Cash Withdrawal/Lodgement Limit. In: NIGERIA, C. B. O. (ed.). Abuja: CBN.

Dauda, Y., Santhapparaj, A. S., Asirvatham, D. & Raman, M. 2007. The Impact of E-Commerce Security, and National Environment on Consumer adoption of Internet Banking in Malaysia and Singapore. Journal of Internet Banking and Commerce, 12, 20.

Genesys. 2008. Customer Service Strategies for the Retail Banking Industry. Industry Strategy Guide [Online].

Longe, O. B. & Chiemeke, S. C. 2008. Cyber Crime and Criminality in Nigeria – What Roles are Internet Access Points in Playing? European Journal of Social Sciences, 6, 8.

Microsoft. 2003. Improving Customer Service in the Banking Industry: Implementing Automation Around an Integrated Customer Information System. Microsoft in Financial Services [Online].

Moores, T. 2005. Do consumers understand the role of privacy seals in e-commerce? Commun. ACM, 48, 86-91.

Mukherjee, A. & Nath, P. 2003. A model of trust in online relationship banking. International Journal of Bank Marketing, 21, 5-15.

Nor, K. M. & Pearson, J. M. 2007. The Influence of Trust on Internet Banking Acceptance. Journal of Internet Banking and Commerce, 12, 10.

Oghenerukevbe, E. A. 2008. Customers Perception of Security Indicators in Online Banking Sites in Nigeria. Journal of Internet Banking and Commerce, 13, 14.

Oghenerukevbe, E. A. 2010. Mnemonic Passwords Practices in Corporate Sites in Nigerian. Journal of Internet Banking and Commerce, 15, 11.

Pan, Y. & Zinkhan, G. M. 2006. Exploring the impact of online privacy disclosures on consumer trust. Journal of Retailing, 82, 331-338.

Shao, G. 2007. The Diffusion of Online Banking: Research Trends from 1998 to 2006. Journal of Internet Banking and Commerce, 12, 13.

Susanto, A. & Zo, H. 2011. Factors Influencing Users' Acceptance in Internet Banking Success: Proposing a Unified Model. 2nd International Conference on Networking and Information Technology IPCSIT Singapore: IACSIT Press

# ENHANCED PLAYFAIR CRYPTOGRAPHIC SYSTEM FOR DATA SECURITY AND INTEGRITY IN A CASHLESS SOCIETY

**Okure U. Obot,**
Department of Computer Science
University of Uyo, Uyo.
1abatakure@yahoo.com

**Victor E. Ekong**
Department of Computer Science
University of Uyo, Uyo.
victorekong@ieee.org

**MfonObong I. Okon**
Department of Computer Science
University of Uyo, Uyo.
okonmfonobong@yahoo.com

***ABSTRACT***

*Data security and integrity is an essential measure for the drive toward a cashless society. There are different cryptographic ciphers lending themselves to ensure that only authorized persons have access to data. One of the earliest of such ciphers is the Playfair cipher. The Playfair cipher has been found to be limited to very short messages and so was discarded for better ciphers long ago. In this study, the Playfair cipher is modified to enhance a better security of data. The enhanced Playfair cipher can accept more datasets than its earliest version and is also made more difficult to crack. Despite these innovations, the enhanced Playfair with all its simplicity and friendliness is not very strong like the popular RSA cipher in decrypting data. To this end, we propose the generation of decryption key using RSA algorithms to give it stronger, more robust and better immunity against hacking.*

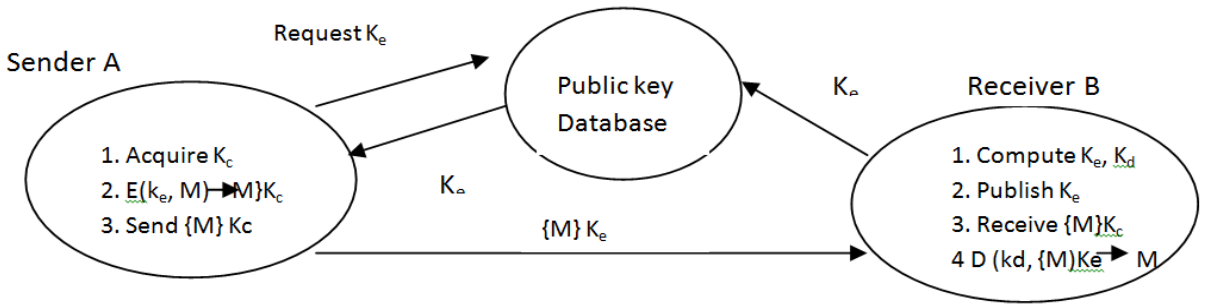
***Keywords****: Cipher, Playfair, encryption, decryption, RSA, digraphs*

## 1. INTRODUCTION

Cryptography is the practice and study of hiding information as it applies to confidentiality, data integrity, entity authentication and data origin authentication (Stallings, 2001). It has found applications in the areas of electronic commerce, bank payment systems such as Automated Teller Machine (ATM), information storage and retrieval systems and establishing the authenticity of users or an entity in a distributed system. A message sent is converted (encrypted) into a form that only persons authorized to access such message can understand the message after it has been reconverted (decrypted) into its original form using a key agreed on by both the sender and the receiver. Measures are needed to ensure that if an intruder gains access to such confidential information it is meaningless and useless to him. Modern cryptography follows a strongly scientific approach and designs cryptographic algorithms around computational hardness assumptions making such algorithms hard to break or compromise by hackers. Conventional encryption systems consist of plaintext, encryption algorithm, secret key, ciphertext, and decryption algorithm (Menezes, et al., 1997).

While the symmetry ciphers employ a single key for both encryption and decryption the asymmetry ciphers offer separate keys for encryption and decryption. The public key is used for encryption while decryption is done using the private key which must be kept secret. In asymmetric cipher, each potential recipient of a message makes a pair of keys, $K_e$ and $K_d$ and keeps the decryption key $K_d$ a secret. The encryption key $K_e$ can be made known publicly for use to anyone who wants to communicate. It is based on two separate well-known functions E and D and two separate keys $K_e$ and $K_d$ for encryption and decryption respectively. For example, if B expects to receive secret information from other agents, B generates a pair of keys $K_e$ and $K_d$. and publish $K_e$ and keeps $K_d$ secret. It may do this either by sending $K_e$ to a public key distribution service that maintains a database of public keys. Any agent wishing to send secret information to B acquires B's public key $K_e$ and uses $E(K_e, M)$ to produce $(M)K_e$ before sending it to B. Only B knows $K_d$ and can apply $D(K_d,\{M\})K_e)$ to decrypt the message (Coulouris, et al, 1994). This is depicted in Figure 1.

Playfair cipher is a multiple substitution symmetric encryption technique invented by Charles Wheatstone fortelegraph secrecy. But it is named after his friend Lord



Playfair. The Playfair is significantly harder to break since the frequency analysis used for simple substitution ciphers does not work with it because of its ability to encrypt pairs of letters

constructed using a keyword. Calculating the key stream can be very easy if plaintext and ciphertext are known. The problem with Playfair cipher is that it can only allow the plaintext containing alphabets but fails for the plaintext containing alphanumeric values and special characters. It is also case sensitive. For current computing systems, this method can be easily hacked in few seconds (Murali and Senthilkumar, 2009).

Several researchers have modified the Playfair algorithm to meet prevailing data security challenges (Murali and Senthilkumar, 2009; Srivastava and Gupta, 2011; Ravinda, et al., 2011). This study seeks to enhance the existing Playfair cipher using a 9x10 matrix that processes a plaintext containing alphanumeric values, space and some basic special characters. This method will rapidly increase the security of transmissions over unsecured channels thereby building a more secured information system that will achieve a secured cashless transaction. The enhanced Playfair can also process a large datasets unlike the classical Playfair.

## 2. EXISTING PLAYFAIR ALGORITHM

The best-known multiple-letter encryption cipher is the Playfair cipher (Ravinda, et al., 2011). The cipher is based on the use of a 5x5 matrix of letters constructed using a keyword. Considering the keyword 'MONETARY', the 5x5 matrix constructed is as shown in Table 1.

*Table 1: Existing Playfair 5x5 matrix*

| | | | | |
|---|---|---|---|---|
| M | O | N | E | T |
| A | R | Y | B | C |
| D | F | G | H | I/J |
| K | L | P | Q | S |
| U | V | W | X | Z |

The matrix is constructed by filling in the letters of the keyword (minus duplicates) from left to right and from top to bottom, and then filling in the remainder of the matrix with the remaining letters in alphabetic order. The letters I and J are considered as one letter so as to have a square matrix (a 5x5 matrix). The process of the algorithm is summarized in Figure 2.

(digraphs), instead of single letters. The algorithm is based on the use of a 5x5 matrix of letters

*Figure 1: The process of encryption and decryption with a key*

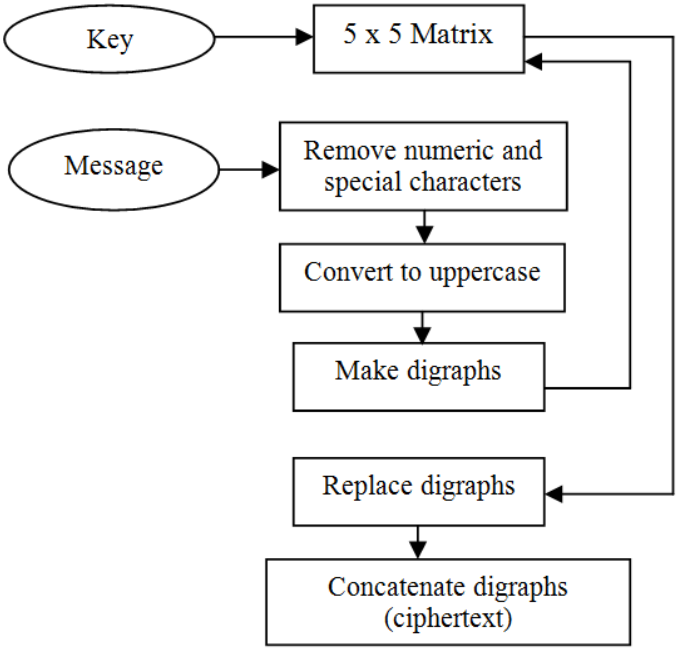



*Figure 2: Block diagram of the existing Playfair algorithm*

Plaintext is encrypted in two letters at a time according to the rules. Repeating plaintext letters that would be in the same pair are separated with a filler letter, such as x or _, so that victory would be enciphered as vi ct or yx. Plaintext letters that fall in the same row of the matrix are each replaced by the letter to the right, with the first element of the row circularly following the last. For instance ET is encrypted as TM. Plaintext letters that fall in the same column are each replaced by the letter beneath with the top element of the row circularly following in the last. For instance, MU is encrypted as AM. Otherwise; each plaintext letter is replaced by the letter that lies in its own row and the column occupied by the other plaintext letter. Thus, RQ becomes BL, and DT becomes IM or JM (Sastry, et al., 2009).

### a. Strengths

The strengths of using the existing algorithms are:

(i) It is simple to operate

(ii) Only 1 key is required for both encryption and decryption.

(iii) It creates a 26x26 = 676 digraph, which requires a frequency table of size 676 to analyze encrypted messages.

(iv) Substitutions of letters depend on the key selection. As the 5x5 matrix is generated according to the key, the plaintext digraphs are replaced with the corresponding ciphertext digraph depending on the inputted key. This results in an improved security of the algorithm.

(v) Simple cryptanalysis techniques like frequency analysis may not work easily to break it.

**b. Limitations**

Some of the observed limitations of the existing algorithm are:

(i) No encryption of the numeric data or punctuation symbols.
(ii) All characters in the encrypted message are either uppercase or lowercase.
(iii) It does not maintain the plaintext format after encryption and decryption process.
(iv) The original Playfair cipher does not encrypt message that exceeds one line.

## 3. DESIGN OF THE ENHANCED PLAYFAIR CIPHER

In trying to overcome the limitations of the Playfair cipher, we enhance and modify the way the Playfair algorithm works. Our proposed algorithm incorporates the following:

(i) Increase the size of the matrix from 5x5 = 25 to 9x10 = 90
(ii) Inclusion of the digits 0-9 and commonly used punctuation symbols like (, &@ : ; " ' ?) and the white space character.
(iii) Separate use of alphabets I and J.
(iv) Try to maintain the text font format after encryption and decryption. That is, differentiate between uppercase and lowercase characters.
(v) No repetition of the characters within a key.
(vi) Maintain the plaintext format after encryption and decryption process.
(vii) The algorithm can encrypt any length of message.

**a. How it Works**

It works the same way as the Playfair cipher, but with some enhancements. The following steps are applied:

When encrypting a message

(i) Create a 9x10 matrix using the key. The characters in the key will be placed first before other characters or punctuation symbols.
(ii) If the plaintext has an odd number of characters, append a white space at the end to make it an even number.
(iii) Break the plaintext into pairs of letters (digraphs).
(iv) The algorithm works on each of the letter pairs. Locate the letters of each digraph in the 9x10 matrix and apply the following conditions:

**Condition 1:** If the characters in the digraph are in different rows and columns, apply case 1:

**Case 1:** Replace the pair with the letters on the same row respectively but at the other pair of corners of the rectangle defined by the original pair. The order is important; the first encrypted letter of the pair is the one that lies on the same row as the first plaintext letter.

**Condition 2:** If the characters in the digraph appear on the same row of the matrix but different columns apply case 2:

**Case 2:**Replace characters with the character to their immediate right respectively (wrapping around to the left side of the row if a letter in the original pair was on the rightmost side of the row).

**Condition 3:** If the characters in the digraph appear on the same column of the matrix but different rows apply case 3:

**Case 3:** Replace characters with the character immediately below respectively (wrapping around to the top side of the column if a letter in the original pair was on the bottom side of the column).

**Condition 4:** If the characters in the digraph appear on the same row and column of the matrix apply case 4:

**Case 4:** leave the character unchanged.

(v) Concatenate all the digraphs to give the cipher text.

When decrypting the message

(vi) To decrypt the ciphertext, follow steps i to v in the encryption process.
(vii) Perform the following conditions and their respective cases.

**Condition I:** If the characters in the digraph are in different rows and columns, apply case I:

**Case 1:** Replace the pair with the letters on the same row respectively but at the other pair of corners of the rectangle defined by the original pair. The order is important; the first encrypted letter of the pair is the one that lies on the same row as the first plaintext letter.

**Condition II:**If the characters in the digraph appear on the same row of the matrix but different columns apply case II:

Case II:Replace characters with the character to their immediate left respectively (wrapping around to the right side of the row if a letter in the original pair was on the leftmost side of the row).

**Condition III:** If the characters in the digraph appear on the same column of the matrix but different rows apply case III:

**Case III:** Replace characters with the character immediately above it respectively (wrapping around to the bottom side of the column if a letter in the original pair was on the uppermost side of the column).

**Condition IV:** If the characters in the digraph appear on the same row and column of the matrix apply case IV:

**Case IV:**Leave the character unchanged.

For a better security of the keys, the Rivest, Shamir, Adleman (RSA) cipher is used to generate the decryption key. The key is then sent to the authorized user who can decrypt it and use it to decrypt a message (plaintext) received from the sender using the Enhanced Playfair cipher. This approach is followed because RSA though more invulnerable to attack than the enhanced Playfair, it is found to process slower than the Enhanced Playfair more so when a large datasets is processed.

**b. An Example**

Considering a plaintext "Our Algorithm is too much" with the secret cipher key "Mfon503". (Note there should be no repetition of character in the cipher key)

**Solution**

**Step 1:** We create a 9x10 matrix with the key characters appearing first before other characters:

MAT (i, j) =

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| M | f | o | n | 5 | 0 | 3 | A | B | { |
| C | D | E | F | G | H | I | J | K | } |
| L | @ | N | O | P | Q | R | S | T | ] |
| U | V | W | X | Y | Z | a | b | c | [ |
| d | e | g | h | i | j | k | l | m | \n |
| p | q | r | s | t | u | v | w | x | % |
| y | z | 1 | 2 | 4 | 6 | 7 | 8 | 9 | $ |
| ? | ( | ) | # | = | < | > | ; | : | ! |
| / | * | + | - | space | & | " | ' | . | |

where i = 1, 2, ..., 9 and j = 1, 2, ..., 10.

**Step 2:** Since there are 21 (odd number) characters in the plaintext, we append a white space character to the plaintext to make it 22 (even number).

**Step 3:** Creating digraphs of the plaintext (message) we have: [Note that the white space character is represented by (_)].

**Step 4:** Picking each digraph, test and apply the conditions and its respective cases as described in the rules above. We have:

| | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Plaintext:** | Ou | r_ | Al | Go | ri | Th | m_ | Is | _t | oo | _m | uc | h_ |
| **Ciphertext:** | Qs | T+ | Jw | rE | tg | Si | i. | Ht | 54 | oo | .i | xZ | i- |

**Step 5:** Concatenating all the digraphs of the ciphertext we have our ciphertext for the message "Our Algorithm is too much" as "QsT+JwrEtgsii.ht54oo.ixZi-".

**Step 6:** Decrypt the decryption key using the RSA algorithm and use the plaintext obtained to decrypt the message (plaintext) using the enhanced Playfair algorithm.

## 4. SOFTWARE DESIGN AND CODING

The software design and coding was done using Java. We develop the enhanced Playfair cipher based on the following algorithm:

(i) count = 0
(ii) Input message to be encrypted or decrypted
(iii) Request for the secret key (key length should not be less than 6 and no character should be repeated in the key).
(iv) If secret key is valid then Encrypt
(v) Display the ciphertext on the screen
(vi) Save, print or send to another node by clicking the send button
(vii) Decipher? (Yes or No) if yes then Input message to be decrypted
(viii) Request for the secret key (key length should not be less than 6 and no character should be repeated in the key).
(ix) If secret key is valid then
(x) Decrypt (using RSA) and do step 15
(xi) Else If secret key is not valid then
(xii) Increment count (count = count + 1)
(xiii) If count > 3 then exit the system
(xiv) Else, do step 12
(xv) Display the plain text on the screen
(xvi) Save, print or send to another node by clicking the send button
(xvii) End

We test the system with a plaintext '*Transfer N40,000.68 to account 0910000246 of UBA*', encrypted using the public key '*project*'.The program produces the following encrypted message:

**JudkGnho"L51y811(25'up-Zddpvjx;5021111355-pe;ZDB/#**

The results of the encryption and decryption processes are presented in Figure 3. Coding of the program that produces these results was done in java application programming environment using the javac compiler.

| Digraphs: | O | R_ | Al | Go | Ri | t | m | Is | _t | oo | _m | u | h |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|

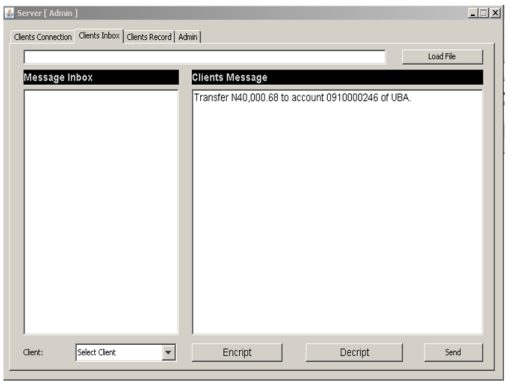
## 5. DISCUSSION AND CONCLUSION

One of the major concerns for an effective cashless operation has been security of transactions between different entities in an electronic payment system. Amongst the security features established to strengthen integrity and trust in electronic transactions is cryptography. Understanding cryptographic attacks and improving cryptographic algorithms is important in information security. While strong cryptography may not guarantee strong security, weak cryptography as well guarantees weak security. In this paper, we have presented an

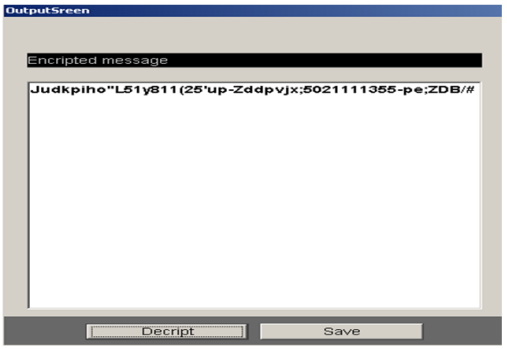
enhanced Playfair cryptographic algorithm as an improvement on the classical Playfair cipher for data security and integrity.

We pointed out the strengths and weaknesses of the original algorithm and proposed an enhanced version that is potentially stronger. Through our proposed Playfair we can encrypt any length of plaintext containing any alphanumeric and special characters by

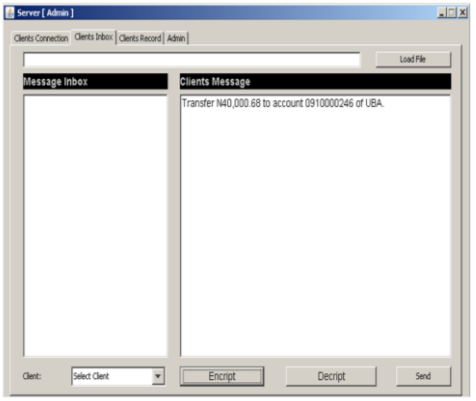

*(a)*




*(b)*




*(c)*




*(d)*

*Figure 3a,b,c,d: Java program screenshots of data transfer using the Enhanced Playfair cipher.*

utilizing a 9 x 10 grid table. A user does not face any ambiguity at deciphering an encrypted plaintext because the characters I and J are placed in separate cells of the matrix. The RSA cipher is proposed to generate the decryption key which could then be used to decrypt a message using the Enhanced Playfair cipher. The choice of RSA algorithm is based on its established attribute of high invulnerability to attacks. However decrypting a large set of data with the RSA cipher takes a pretty long time, a weakness that the Enhanced Playfair has been able to solve. The implementation in hardware and software is also easy as we have demonstrated using Java programming.

## REFERENCES

Coulouris G , Dollimore J and Kindberg T (1994) *Distributed Systems, Concepts and Design, 2nd Edition,* Addison Wesley, London.

Menezes, A.J, Ooschot, PCV, Vanstone, S.A (1997) *Handbook of applied cryptography*, CRC press, Boca Raton, Florida, USA.

Murali, P and Senthikumar, G. (2009) Modified version of Playfair cipher using Linear Feedback Shift Register, *In Proc. of IEEE Conf. on Information Management and Engineering*, p.3, DOI: 10.1109/ICIME 2009.

Ravinda, B. K., S. U. Kumar, A. V. Babu, I. V. Aditya, and P. Komuraiah (2011) An extension to traditional Playfair Cryptographic method, *Int'l, Journal of Computer Applications*, Vol. 17, No. 5, pp.1.

Sastry, V. U, Shankar, N. R., and Bhavani, S.D (2009) Modified Playfair cipher involving interweaving and iteration, *International Journal of Computer Theory and Engineering*, Vol. 1, No. 5, pp. 1793-1801.

Srivastava, S.S and Gupta, N (2011) Security aspects of the extended Playfair cipher, *In Proceedings of International Conf. on Comm. Sys. and Networks Technologies*, p. 144. DOI: 10.1109/CSNT.2011.37.

Stallings, W (2001) *Cryptography and network security: principles and practice*, 2nd ed., Pearson education, USA.

# CASHLESS ECONOMY AND ONLINE TRANSACTION SYSTEM IN NIGERIA

**A. A. Obiniyi**
Department of Mathematics,
Ahmadu Bello University, Zaria
aaobiniyi@gmail.com

***H. A. Sulaimon**
Department of Computer Science,
Federal College of Education, Zaria
sulaimha@yahoo.com

**I. Abdullahi**
Department of Mathematics/Computer Science,
Ibrahim Badamasi Babangida University, Lapai
Ibrojay01@yahoo.co.uk

***ABSTRACT***

*Online transaction systems have increasingly become a necessary component of business strategy and a strong catalyst for achieving cashless economy and economic development. Nigeria, as one of the developing countries, is lacking behind in reaching the expected level in global economy and banking system, so there is a need to improve on the banking system and any other financial industries. This study was carried out mainly on primary and secondary sources of data or information, which included different publications. This paper is aimed at determining the present scenario of online transaction system and banking sectors in Nigeria, demonstrates the scope and benefits of cashless means of business transaction compared with the existing system. This paper addressed significant gaps in existing knowledge about the Internet banking and landscape. The actual situation of online transaction system in the marketing point of view in Nigeria is presented. The results showed that online transaction system has various benefits to lead Nigerian into a cashless society; however, this study also observed that the Nigerian customers do not have enough knowledge regarding online transaction system which is rendered by banking sector. A discussion of the implications of these results and limitations were provided at the end.*

***Keywords**: Banking, Sector, Cashless, Economy, Online, Transaction, System, Nigeria*

## 1. INTRODUCTION

Online transaction system is now a global phenomenon. It is an invaluable and powerful tool driving development, supporting growth, promoting innovation and enhancing competitiveness. Technological innovations have been identified to contribute to the distribution channels of banks and these electronic delivery channels are collectively referred to as electronic banking (Goi, 2005). The evolution of banking technology has been driven by changes in distribution channels as evidenced by automated teller machine (ATM), Phone-banking, Tele-banking, PC-banking and most recently Internet banking (Chang, 2003; Consulting, 2008). The use of automated teller machine (ATM), Phone-banking, Tele-banking, PC-banking and most recently Internet banking are the technology depended on to achieve cashless society. The developed country as a part and parcel of their economy is now using online banking. Apart from the developed countries, the developing countries, such as India and the Republic of Korea are experiencing strong growth in e-banking. In Southeast Asia, Thailand, Malaysia, Singapore and Philippines, Internet banking is also developing rapidly (Mia *et al*., 2007). In Nigeria, ATMs are the most popular electronic delivery channel for banking services but only a few customers are using Internet banking facilities.

A strong banking industry is important in every country and can have a significant effect in supporting economic development through efficient financial services (Salehi and Zhila, 2008). However, there have been several major challenges and issues such as security and payment options faced by the online transaction system growth and the e-business in general. Limited payment options and outlets available to online customers are being complained (Furash, 1994). As an Internet based technology, online transaction system is new and quite unfamiliar for some people in Nigeria due to the digital divide and the different level of Internet experience and environments. Online transaction system services have been available in Nigeria since 2000. As of today, all the banks offered online financial services. The reason for the lack of complete adoption of online transaction system in developing countries like Nigeria is an important research that will be addressed by this paper. In other words, despite this growth of IT Worldwide, Nigeria banks continue to use blended online banking transactions. Electronic banking refers to several types of services through which bank customers can request information and carry out most retail banking services via computer, television or mobile phone (Daniel, 1999). Burr (1996) describes it as an electronic connection between bank and customer in order to prepare, manage and control financial transactions.

Cashless society is a form of a society, where funds are transferred through an exchange of electronic signals between financial institutions, rather than the exchange of cash, checks, or other negotiable instruments. The ownership of funds and transfers of funds between financial institutions are recorded on computer systems networked together. Customers' identification is by access code, such as a password or Personal Identification Number (PIN), instead of a signature on a check or other physical document. Online transaction system involves individual and corporate clients, and includes bank transfers, payments and settlements, documentary collections

and credits, corporate and household lending, card business and some others (UNCTAD, 2002). Banking has never been more important to our society than it is today. The advance of communication and computer technology and the availability of the Internet have made it possible that one can do most banking transactions from a remote location even without stepping into a physical financial structure that is, the emerging of electronic banking (Bruene, 2002). The way Bill Gates (2008) announced that "banking is essential, banks are not". This quotation means that the traditional bank branch is going to vanish in order to be surrogated by electronic banking which continues to attract new users.

The banking industry believes that by adopting new technology, the banks will be able to improve customer service level and tie their customers closer to the bank. Meanwhile, the banking industry has been also looking for new methods to expand its customer base and to counteract the aggressive marketing effort of those non-traditional banking entities. Many banks quickly realized that there are a momentous number of customers like to do banking electronically. The application of online transaction system will reduce the costs of operation for the financial institutions and give security to the banks. For instance, the services will allow banks to reduce expenditures on physical structures. On another hand, online transaction system services could be highly demanding and desirable to accommodate the sudden, rapid growth that has occurred in other information-intensive industries such as travel and securities brokerage. Finally, the development of online transaction system service has encouraged the adoption of a decentralized approach to give banks more needed flexibility to distribute Internet access to a much larger number of employees and potential customers. The aim of this paper is to look at the emergence, advantages and acceptance of online transaction system in Nigeria. The paper is also aimed at determining economical prospects of online transaction system and to explain the present scenario of banking sectors in Nigeria and at the same time it demonstrates the scope and benefits of online transaction system compared with the existing systems. It also tries to present the actual situation of online transaction system in the marketing point of view. This study will also examine the present status of existing online transaction system in Nigeria.

## 2. METHODOLOGY

The study has been done mainly on primary and secondary sources of data or information. The first is an exploratory research based on secondary data obtained through the Internet, books and related journals. Secondly, survey questionnaire was administered to empirically assess the level of acceptability of online transaction system in Nigeria.

### a. Data Collection Procedure

*i. Primary data sources*

Primary data has been collected from Zaria Metropolis based on some selected banks e.g. First Bank Ltd, Oceanic Bank, United Bank for Africa (UBA), and Union Bank Nigeria Ltd. in the year of 2010. These banks are considered as the private commercial banks. Primary data collections are done by the interviewing method with questionnaire.

*ii. Secondary data sources*

Secondary data has been collected from different publication material and web site as well as the books and the material from different libraries and research related to the issue are taken into account. The sample size determinations on online transaction system were interviewed. The sample size determination ensures the minimum number of respondents on online transaction and cashless society. Since there are many indicators the sample size is calculated using 50% as indicator percentage for survey that gives maximum sample size.

According to Godden (2004) the sample size formula for an infinite population (where the population is greater than 50,000) is;

$$SS = \frac{Z^2 x(p) x (1-p)}{C^2}$$

SS = Sample Size
Z = two-sided normal variant at 95% confidence level (1.96)
P = Percentage of population picking a choice, expressed as decimal
C = Confidence interval, expressed as decimal (e.g., .04 = +/- 4 percentage points)
Z-values (Cumulative Normal Probability Table) represent the probability that a sample will fall within a certain distribution.
The Z-values for confidence levels are:
1.645 = 90 percent confidence level
1.96 = 95 percent confidence level
2.576 = 99 percent confidence level
Example:
SS =( 3.8416 x 0.5 x 0.5)/0.0016
SS = 600
Hence, the minimum sample size required is 600.

### b. Survey Design

The present study used a survey that was designed and conducted to find out the feasibility of the online transaction system in Zaria private commercial banks. A specifically designed questionnaire was used as a tool and the survey covered a sample of 600 respondents for the purpose of the analysis. These respondents were the customers of various banks:
the age groups were 18 to 25, 26 to 35, 36 to 45 and 46 to 55 and above 56 years.
The survey included queries on the following topics:

(i) Income ranges for the customers (per month)
(ii) Problem faced regarding service in the bank
(iii) Willingness to visit a web site for the relevant information
(iv) Willingness to pay fee (Monthly)
(v) Opinion about online banking
(vi) Additional services they would like to have.

Microsoft office Excel 2007application software was used for the statistical analysis while descriptive statistics were computed and used in the interpretation of findings. The data was presented in the form of tables and graphs in section 3.1.

## 3. RESULTS AND DISCUSSION

This section dealt with the results and discussion on both the quantitative and qualitative research based on the primary and secondary data sources.

### a. Acceptance of Online Transaction System by Respondents

Male respondents were more interested in online banking than female respondents; hence, most of our respondents are males as displayed in table 1 and figure 1. However, the number of females was increasing which was a good sign. At the same time, it was observed that young people adopt the use of Internet more rapidly. Regarding monthly income, table 2 and figure 2 showed the percentages of respondents whose monthly incomes were found to be higher than the others.

Regarding service in the Bank, table 3 and figure 3 revealed that 44% respondents of the total sample size were faced with the problem of queuing and 32% respondents faced hassle to get the ATM card in the Bank. It was observed that most of the respondents of the total sample size were not willing to pay monthly fees for their service as revealed in both table 4 and figure 4.

*Table 1: Number and Percentage of Respondents by Gender*

| Gender | Number | Percentage (%) |
|---|---|---|
| Male | 348 | 58 |
| Female | 252 | 42 |
| Total | 600 | 100 |

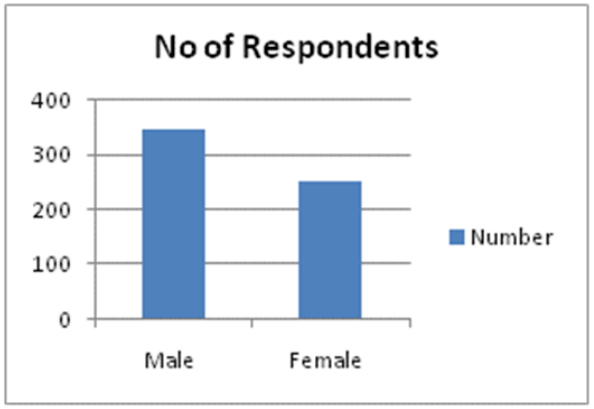



*Figure 1: Number and Percentage of Respondents*

*Table 2: Number and percentages' income range per month*

| Income/Month | No of respondents | Percentage (%) |
|---|---|---|
| Below N 10T | 80 | 13 |
| N10T – N20T | 188 | 31 |
| N20T – N30T | 116 | 19 |
| Above N30T | 216 | 37 |
| Total | 600 | 100 |

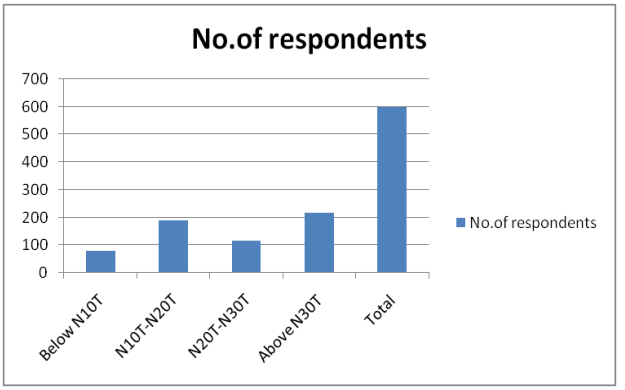



*Figure 2: Number and Percentage of Respondents' income range per month*

*Key: T = 1000.00*

*Table 3: Number and percentage of respondent's Problem faced in the banks*

| Problem faced | No of respondents | Percentage (%) |
|---|---|---|
| Queue problem | 268 | 44.66 |
| Hassle to get the telephone lines free | 192 | 32 |
| Information is not readily available | 80 | 13.34 |
| Lack of Confident | 60 | 10 |
| Total | 600 | 100 |

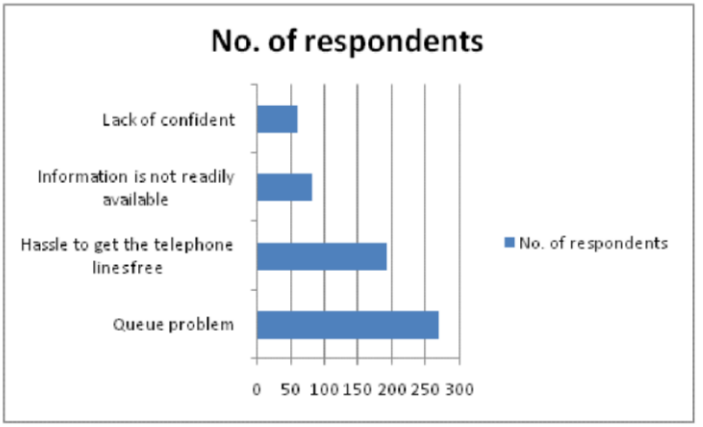



*Figure 3: Number and percentage of respondent's Problem faced in the banks*

*Table 4: Number and percentage of respondents by monthly fees*

| Monthly fee | No of Respondents | Percentage (%) |
|---|---|---|
| Disagreed | 176 | 46 |
| Not Decided | 160 | 26.67 |
| Agreed | 144 | 24 |
| Strongly Agreed | 20 | 3.33 |
| Total | 600 | 100 |

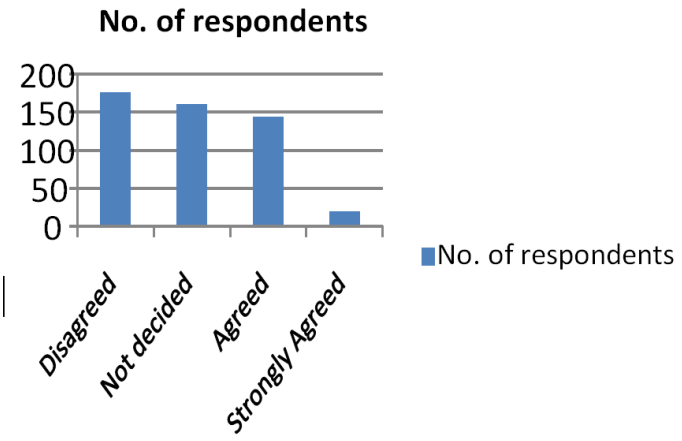



*Figure 4: Number and percentage of respondents by monthly fees*

In addition, 476 customers interviewed which of about 79% of the total sample size responded that they needed more knowledge in operation of the computer. 448 of the interviewee who is 74.66% of the total sample size responded that they have little knowledge about browsing Internet. Literacy results showed that online transaction system would not be a tough operation to the people because of their computer knowledge. 89% responded that they used to call the bank frequently for their balance. 95% of the customers assert that they were willing to pay the utility bill payment through Internet, which would be very convenient for them. The above finding showed that people's perception about Internet and online transaction system are satisfactory and they are ready to accept cashless economy if Nigeria should fully implement it.

*3.1.1. Present status of online transaction system in Nigeria*

Online transaction system satisfied customer demand in banking activities electronically throughout the world. At present, several banks in Nigeria offered limited services of telebanking and online banking facilities working within the branches of individual bank in a closed network environment. The Banks played the pioneering role with adoption of modern technology in retail banking during the early 1990s. Below are some of the modern day's online banking systems;

*a. Mobile banking:* Mobile banking was a term used for performing banking functions such as checking of balance, account transactions and payments. via a mobile device such as a mobile phone. The standard package of activating that mobile banking covers are: mini-statements and checking of account history; alerts on account activity or passing of set thresholds; monitoring of term deposits; access to loan statements; access to card statements; mutual funds/equity statements; insurance policy management; pension plan management; status on cheque, stop payment on cheque; ordering check books; balance checking in the account; recent transactions; due date of payment; PIN provision, change of PIN and reminder over the internet; blocking of (lost/stolen) cards; domestic and international fund transfers; micro-payment handling; mobile recharging: commercial payment processing; bill payment processing; peer to peer payments; withdrawal at banking agent; and deposit at banking agent. Despite huge prospects, Nigeria is yet to adopt mobile banking which is what Central Bank of Nigerian (CBN) is introducing to enhance cashless economy.

*b. Tele banking:* Tele banking service was provided by phone. To access an account it was required to dial a particular telephone number and there were several options of services. Most banks have so far provided a few options of tele banking services such as detail account information, balance inquiry, information about products or services, ATM card activation, cheque book related service, bills payment and credit card service. Funds transfer between current, savings and credit card account and stock exchange transactions were still online transaction system services.

*c. CitiDirect:* The facilities of CitiDirect were online direct debit transaction process; information reporting; real-time information reporting for more effective cash management; delivered with the highest level of security; easy-to-use application; world link through CitiDirect; comprehensive payment transaction solution; flexible, streamlined functionality; reliability, speed and information; payments through CitiDirect; a comprehensive payments solution globally and locally; simplified, secure transaction management; timely, accurate information: email and wireless banking alerts by CitiDirect.

*3.1.2. Benefits of online transaction system in Nigeria*

*a. Short term benefits.* Reduce extra time; Increase productivity and efficiency; Eliminate duplication and wastage; Cut down maintenance, and shortage cost; Curtail security cost.

*b. Long-term benefits.* Create new opportunities of jobs for jobless; participate in the country's economic health; proper planning and monitoring; Proper use resources.

*c. Job creation.* The issue of computers eliminating jobs of people was quite emotional and painfully real. But it has two sides that automation will eliminate certain types of job like record keeper and also created jobs such as system administrator, system analyst, system programmer and operator. It also helped to reduce unemployment problem.

d. *Contribution to General Development Programmes.* Banks with a national economy, work towards building national capital, increasing national savings and mobilizing investments in trade and industry.

*3.1.3. Benefits from the banks' point of view*

From the banks view point, the first benefits for the banks offering online transaction system services was better branding and better responsiveness to the market. The other benefits were possible to measure in monetary terms. The main goal of every company was to maximize profits for its owners and banks were not any exception. Automated online transaction system services offered a perfect opportunity for maximizing profits.

*3.1.4. Benefits from the customers' point of view*

The main benefits of online transaction system from the bank customers point of view was significant saving of time by the automation of banking services processing and introduction of an easy maintenance tools for managing customer's money. The other benefits of online transaction system from the customers' point of view are as follows:

(vii) One can Cash his money without requiring the physical interaction of the customers in the bank.
(viii) Quick and continuous access to information.
(ix) Corporations had easier access to information as, they checked on multiple accounts at the click of a button.
(x) Better cash management.
(xi) Online transaction system facilities speed up cash cycle and increases efficiency of business processes as large variety of cash management instruments is available on Internet sites of banks.
(xii) Private customers looked for slightly different kind of benefits such as from online transaction.
(xiii) Reduced costs: This was in terms of the cost of availing and using the various banking products and services.
(xiv) Convenience: All the banking transactions performed from the comfort of the home or office or from the place a customer wants to.
(xv) Speed: The response of the medium was very fast; therefore customers actually waited till the last minute before concluding a fund transfer.
(xvi) Fund's management: Customers downloaded their history of different accounts and do a "what-if" analysis on their own PC before affecting any transaction on the web.

*3.1.5. Economic benefits*

Online transaction system served so many benefits not only to the bank itself, but also to the society as a whole. Online transaction system made finance economically possible by:

a. Lower operational costs of banks
    i. Automated process
    ii. Accelerated credit decisions
    iii. Lowered minimum loan size to be profitable.
b. Potentially lower margins:
    i. Lower cost of entry
    ii. Expanded financing reach
    iii. Increased transparency.
c. Expand reached through self-service:
    i. Lower transaction cost
    ii. Make some corporate services economically feasible for society

Make anytime access to accounts and loan information possible.

*3.1.6. Policy Implications*

The comprehensive set of online transaction system products can help us run our business more effectively by automating many of our critical banking activities and interacting electronically with our bank. Initial cost of online transaction system may be high, but it can be recovered within few years. Electronic banking may play a vital role in order to promote an automated service to the potential customers. Ministry of finance can also play some role for conveyance. Arrange monthly seminar in the banks or in the training academy of the banks to make awareness about the new technology available in banks. Electronic security and viability may require taking faith from the potential clients. Communication should be liberalized for technological advancement.

*3.1.7. Limitations and Constraints*

The focus of the study is mainly on some selected banks in Nigeria. Online transaction system is the important issue in the world of banking but Nigeria is a developing country with the limited infrastructure facility and limited skill manpower in e-banking. Computer literacy was found very few and information technology was in the growing position. This study was based on limited variable. Difficulties faced to collect the desire information. Disclosing the information was very restricted. IT division was not cooperative all the time. In addition, interviewing targeted respondents adopted convenience sampling as alternative to random sampling, at some phases where respondents were inaccessible or not available. Bank officials were found too busy and also reluctant to talk without a proper written permission from the competent authority. Although online transaction system has bright prospects, it involved some financial risks as well. The major risk of online transaction system included operational risks (e.g. security risks, system design, implementation and maintenance risks); customer misuse of products and services risks; legal risks (e.g. without proper legal support, money laundering may be influenced); strategic risks; reputation risks (e.g. in case the bank fails to provide secure and trouble free online transaction system services, this will cause reputation risk); credit risks; market risks; hackers' risk and liquidity risks.

## 4. CONCLUSION

Online or mobile transaction as one of the practices that lead to cashless economy or society, opened up new window of opportunity to the existing banks and financial institutions. Most of the banks have their own websites but not all of them offered Internet facilities. The main reason of this was that the banks did not have the IT infrastructure and proper security features. In Nigeria most of the people were illiterate and obviously they were technologically ignorant. More so, among the literate portion many of them had computer phobia and for adequate usage of Internet banking, the overall population of computer literacy must be developed. Nevertheless, with cashless economy and equity network, every citizen can grow comfortably with the digital lifestyle. Most Nigerian has not fully understood the power of technology and seek to leverage

it to enjoy better control over their banking operations. In conclusion, online transaction system also provides other benefits. For instance, creating new markets, and reducing operational costs, administrative costs and workforce are increasingly important aspects for the banks' competitiveness, and online transaction system improved these aspects as well. So, Nigerian should take these advantages of cashless economy as being introduced by the central bank of Nigerian (CBN) as early as possible.

**REFERENCES**


Bruene ,J. (2002). Online banking by the numbers.Http://www.onlinebankingreport.com Retrieved on August 25, 2003.

Burr, W. (1996). Wieinformationstechnik die bank organization,*Verandernkonnte*,Bank und Markt 11: 28–31.

Chang ,Y.T. (2003). Dynamics of banking technology adoption: an application to Internet banking, Department of Economics, *Workshop Presentation*, University of Warwick, Coventry, UK.

Consulting, G. (2008). Using technology to engage retail banking customers. Why banks must carefully manage their digital touch points to create a seamless customer experience.http://www.adobe.com/engagement/pdfs/gallup_retail_banking_white _paper.pdf.Retrieved on 27th December, 2011

Daniel, E. (1999). Provision of electronic banking in the UK and the Republic of Ireland.Int. J. Bank Mark. 17(2): 72–82.

Furash, E.E. (1994). Payments system under siege: customers want information along with monetary transfers, Non-banks are providing it. ABA Bank. J. 86(6): 55.

Gates, B. (2008). Banking is essential, banks are not.http://www.slideshare.net/Carolederks/banking-is-essential-banksare-notpresentation. Retrieved on December 12, 2008.

Godden, B. (2004). Sample Size Formulae. January, Pp 1.http://williamgodden.com/samplesizeformula.pdf Retrieved on 27th December, 2011

Goi, C.L. (2005). Online transaction system in Malaysia: Opportunities and Challenges, J. Internet Bank. Comm., 10(3).

Mia, M.A.H., Rahman, M.A. and Uddin, M.M. (2007). E-banking: evolution, status and prospects. Cost Manage. 35(1): 36-48.

Salehi M and Zhila A (2008). Fraud detection and audit expectation gap: empirical evidence from Iranian bankers. Int. J. Bus. Manage., 3(10): 65-77.

United Nations Conference on Trade and Development (UNCTAD) (2002). E-commerce and development report. New York and Geneva: United Nations.

# TRUSTED CASHLESS CLOUD: A FLEXIBLE APPROACH FOR THE NEW CASHLESS SOCIETY

**M. C. Ndinechi**
Electronics Development Institute, Awka,
National Agency for Science and Engineering Infrastructure,
Federal Ministry of Science and Technology.
*mikez4god@yahoo.com*

**K. C. Okafor**
Electronics Development Institute, Awka,
National Agency for Science and Engineering Infrastructure,
Federal Ministry of Science and Technology.
*arissyncline@yahoo.com*

**C. C. Udeze**
Electronics Development Institute, Awka,
National Agency for Science and Engineering Infrastructure,
Federal Ministry of Science and Technology.
*udezechidi@yahoo.com*

***ABSTRACT***

*Contemporarily, the paradigm shift created by cloud computing will facilitate the usage of cashless solutions in the Nigerian educational sector, enabling reliable funds transaction from cash-based instruments to cashless-based platforms. This work presents an ongoing research and proposes a secured cashless cloud solution using high speed Google App Engine Platform as a Service (GAEPaaS) for the proposed cashless strategy in Nigeria while focusing on the Nigerian educational sector. The contribution of this paper will leverage on Trusted Cloud Computing (TCC) for e-Payment Solutions, its security and economic implications in the Nigerian Educational sector. The proposed technique seeks to improve speed and provide a reliable trust in the electronic system before a switching wired transfer is made on the platform.*

***Keywords****: Cashless-based platform, e-payment, Google App Engine, PAAS, Trusted cloud computing.*

## 1. INTRODUCTION

For many years, the idea of a cashless society has continued to draw attention to various governments, institutions with mixed understanding on the implementation strategy. Around the world, coins and banknotes, cheques, cash are used as payment in increasingly few transactions as more and more systems present themselves not only as viable, but as potentially better alternatives: e-systems.

The use of electronic communication channels to conduct businesses without the need for physical conduct or presence has already been established and accepted warmly, but the issue of paying electronically still remains risky and muddy (Theodosios and Sthephanides, 2005). Basically, strong and long-lasting business relationships have always been depended on trust. The transition to digital cashless economy now compels enterprises not only to develop client based intimacy but also to ensure that security requirements are part of the client relationship strategy.Transactions in cashless strategy can occur without any prior human contact or established interpersonal relationships. This lack of interpersonal trust creates a circumstance for a security threat. The authors in (Theodosios, &Sthephanides,2005) defines security as a set of procedures, mechanisms and computer programs to authenticate the source of information and guarantee the integrity and privacy of the information (data) to abstain this circumstance to lead to a hardship (economic) of data or network resources. Their work outlines three basic building blocks of security mechanisms in any cashless solution viz:

(i) Encryption: provides confidentiality, authentication and integrity.
(ii) Digital signatures: provide authentication, integrity protection and non-repudiation.
(iii) Checksums/hash algorithms: provide integrity and authentication.

In our cashless context, the focus of every transaction is to minimize the transaction risk. In parallel, a trust framework must address scalability and cost. Consequently, a flexible cashless solution that addresses speed, security and trust issues are essential for every electronic payment mechanism. Such a solution will be widely accepted and established as a common medium of financial transactions. The growth of the Internet as a medium of transaction has made possible an economic transformation in which payment options in Nigerian Educational sector is majorly electronic. The critical factor of success of cashless acceptability in this context is money flow, comprehensive data and information flow. The policy by CBN for cashless society creates a new thinking for developing trusted payment solutions that will completely eradicate cash based instruments, but supports highly efficient, secured, and trusted solution that will benefit our educational sector.

This paper seeks to analyze the implications of an increased usage of our proposed payment systems in bringing about the future of a cashless society while presenting TCC model. This will be achieved through analyzing the payment options which are enabling a decline in cash payments, both in terms of the reasons for wanting such systems, and the technology required for them to work. With this in mind, an emphasis has been placed on trusted computing framework derived from cloud computing using Google App Engine Platform as a Service (GAEPaaS).

## 2. LITERATURE REVIEW

### 2.1 CASHLESS FORMS

Card-based alternatives (Credit cards, Debit cards and ATM cards)Credit cards are typically a plastic card (figure 1) with data stored on a magnetic stripe and, increasingly, a microchip (section 2.2). The majority of cards are the same size of 85.60 × 53.98 mm, as set forth by the ISO 7810 international standard (Paul, 2006). The debit cards are a further popular alternative to the use of cash when making purchases and bank withdrawals. The major difference, as the name suggests, is that in this case funds are withdrawn directly from the purchaser's bank account, rather than accumulating credit which then has to be paid off at a later date, potentially with an interest. Debit cards are popular than credit cards but are particularly favoured by the banks over alternative more traditional payment methods, such as cheques, which are more costly for them to process with little profit.


*Figure 1: Credit cards issued by VISA and MasterCard (sourced from online stock image library stock.xchng) (Paul, 2006)*

Online electronic payments are not tantamount to electronic payments (Yang,2009). With the emergence of e-commerce, credit cards have long been represented as electronic means of payments. Many utility bills are now addressed with online electronic payments, (electronic currency). Figure 2 showing interswitch quick teller portal in (www.quickteller.com). Online electronic payment refers to a transaction in the online exchange of funds; it is a network-based electronic business card transaction for all types of electronic tools and media (Yang,2009). Electronic Payment System is the basis for online payments. The use of electronic cash such as visa cards, master cards, gift cards plays a significant role in the cashless strategy. Switching vendors facilitates the wire transfers with mobile phones or World Wide Web (www) in all electronic solutions. In our cashless solution, in order to prevent mismatched data leading to inconvenience for the user as well as falsification of user details, it is imperative for such a system to address trust before authorizing payments in real-time (wired transfer). The fact that such a solution is technically possible makes the future of a cashless society increasingly feasible in our Educational sector. Figure 3 shows a PoS deployment terminal that manages the selling process by a salesperson accessible interface in a supermarket. The same system allows the creation and printing of the receipt. This is a cashless instrument as well. With this, transactions can be tracked in real time.

Basically, an Eduportal is a complete suite of computed web based Educational management solution developed for Educational Institution to enhance the effective running of the school administration.This system is bureacratic as it allows intial cash based transaction with the bank before using the portal. Figure 4 and 5 shows an exsiting model which are cash based in its functionality.

The bank operator is the debit card provider. Visa/Master is credit card providers while switching operators synchronizes the transactions (Interswich). However, from figure 5, there is no cashless strategy in the model, as such presents non compliance to the CBN policy of cashless legislation. The authors in (Ahmed,&Al-Mukaddim,(unpubilished)) outline considerations in designing an on-line electronic payment system which is taken into consideration in this work viz:

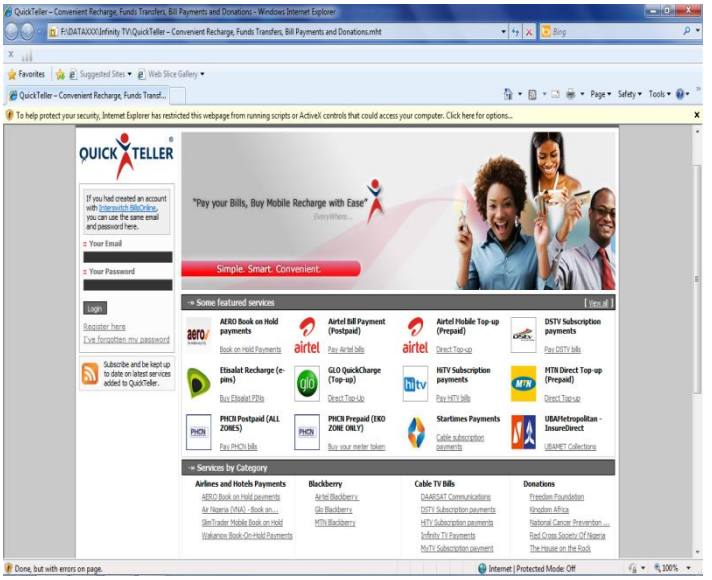



*Figure 2: A cashless utility electronic platform by interswitch Nigeria(www.quickteller.com)*

*Figure3: A Point of Sale Deployment (www.wikipedia.org/wiki/HEBcashRegister)*

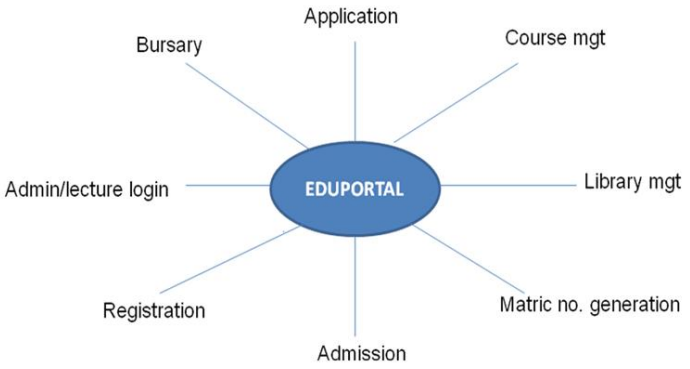



*Figure 4: A generic web portal*

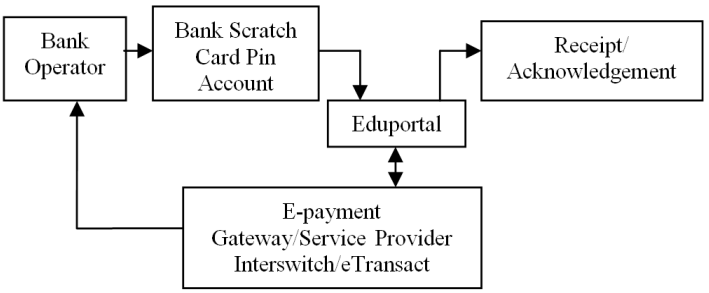



*Figure 5: Traditional Payment Model (Cash-based)*

(i) Privacy should be assured as the users expect to trust a secure system. Electronic communication through the use of electronic payment system should be as safe as a private medium like a telephone free of wiretaps and hackers.

(ii) Although no systems are yet fool-proof, electronic payment systems designers should concentrate closely on security.

(iii) As the users value convenience more than anything, the payment interface should be user friendly having intuitive outlook and must be as easy to use as a telephone.

(iv) Designing an EPS should handle the challenge to integrate the databases used by each of the users, while keeping the data up-to-date and error free.

(v) A "network broker"- someone to broker goods and services, settle conflicts and facilitate financial transactions electronically- must be in place (Kalakota & Whinston, 2000).

(vi) An EPS should resolve the issue of how to price payment system services. The necessity of using subsidies to price all service affordably should be recognized and the potential waste of resources for using subsidies to encourage users to shift from one form of payment to another should be considered.

vi. A common standard should be imposed and followed; since without standards the wielding of different payment users into different networks and different systems is impossible (Kalakota, R. And Whinston, 2000).

## 3. CLOUD COMPUTING (PAAS): A PARADIGM SHIFT

With the rapid growth of Information and Communication Technology, Electronic payment solutions is now acting as a new means of carrying out business transactions through electronic means such as Internet environment. Cloud computing has received a lot of attention in the enterprise market segments. It utilizes the internet backbone to deliver services, platforms and infrastructures with high cost optimization. According to (Leena, 2010),(Srinivasa, et al, 2009), (Daniel, et al, 2009),(Rajkumar.et al, 2009), various definitions has been given to this new technology, however following the definition in (www.en.wikipedia.org/wiki/file:cloudcomputing.svg), this work defines cloud computing as the delivery of computing as a service whereby shared resources, software, and information are provided to computers and other devices as a utility over a network (Internet). Figure 6 shows a typical cloud transaction in (Rajkumar.B et al, 2009) while figure 7 shows a literal diagram as presented in (www.en.wikipedia.org/wiki/file:cloud computing.svg.). Enterprise cloud computing is a controlled, internal place that offers the rapid and flexible provisioning of compute power, storage, software, and security services. Cloud enables enterprises to unleash their potential for innovation through greater intelligence, creativity, flexibility and efficiency, all at reduced cost. Today, cloud computing gives businesses more control and flexibility over the technology they deploy and the way they deploy it. It helps companies reduce costs and focus resources on gaining strategic advantage. While deployment strategies differ, it is critical that an organization's infrastructure is managed as a utility made up of secure, scalable and standards-based building blocks of integrated IT resources from storage to servers and network management (Leena,2010). A cashless solution for the educational sector in Nigeria can leverage on the benefits of cloud to create a trusted framework for a more innovative cashless environment. In this context, this work adopts Google App Engine Platform as a service to create a cashless Trust model while outlining its implementation methodology using software life cycle development.

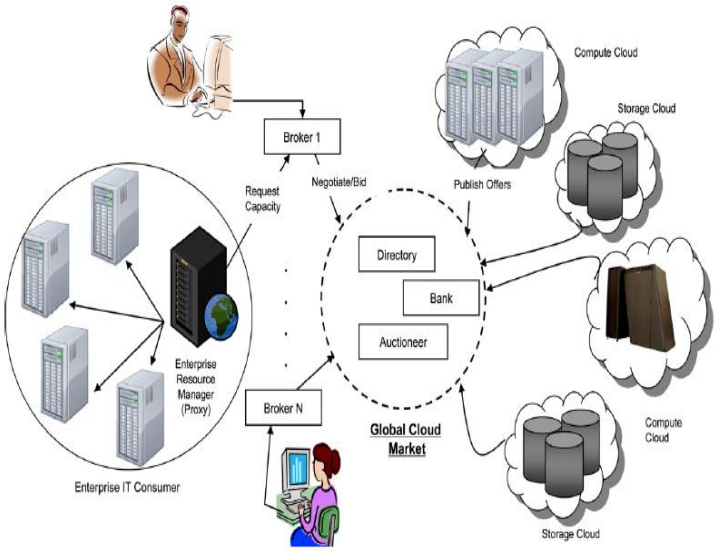



*Figure 6: Global Cloud exchange (Rajkumar. B et al, 2009)*

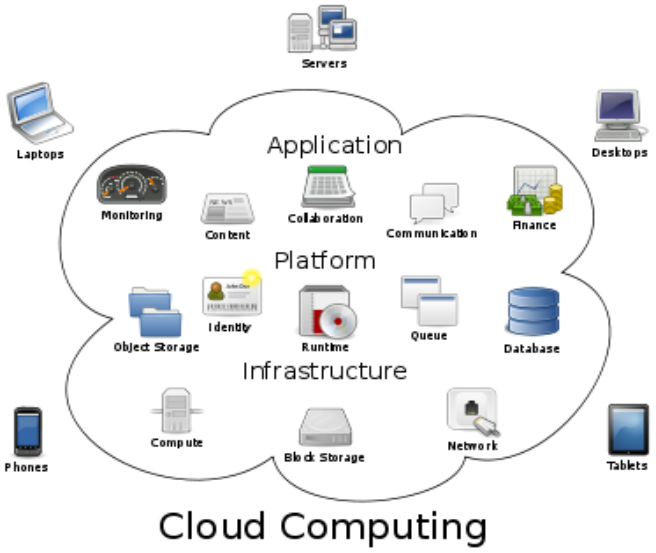



*Figure 7: Cloud computing logical diagram (Http://www.en.wikipedia.org/wiki/cloud computing.svg.)*

### 3.1 A MODEL OF TRUSTED CASHLESS CLOUD (TCC)

This work proposes a cashless solution that will address the issues of speed, trust, risk, and payment flexibility, avoidance of forgery and repeatability before allowing for wire transfer via the payment gateway. In this paper, we proposed architecture for secured data and arbitrary computations to Trusted Commodity Cloud (TCC). In our approach, the user communicates with a trusted cloud (a private cloud) via the portal which encrypts and verifies the data stored and operations performed in the portal. We split the computations such that the trusted cloud is mostly used for security-critical operations in the less time-critical setup phase, whereas queries to the payment gateway are processed in parallel by encrypted data and switching wire transfers to the selected banks. Figure 8 shows a simple architecture of the proposed model. Figure 9 shows a conceptual framework for cloud technologies.

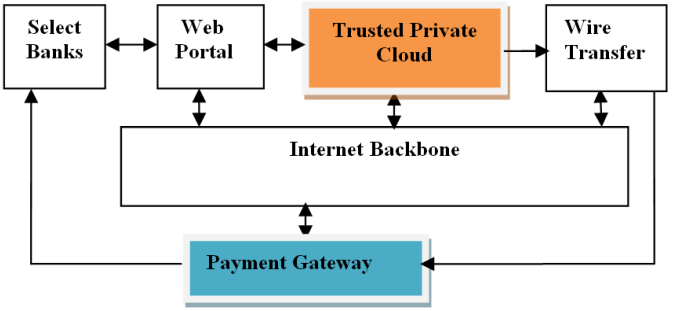



*Figure 8: A Trusted Cashless Cloud Model*

A payment gateway shown in figure 8 is an e-commerce application service provider that authorizes wired transfers after the verification and certification in the trusted cloud payments. Payment gateways protect user credit card details by encrypting sensitive information, such as credit card numbers, to ensure that information is passed securely between the client and the institution's portal and also between portal and the payment processor. The trusted private cloud is an electronic verification solution running on Google App engine with the web portal. This takes care of the Integrity of the Information, the Validity of client Information, the Non-repudiation of Information, the Authenticity of the Transaction Status and The transfer control to payment gateway

#### a. Our Approach

The architecture we proposed consists of the blocks in figure 8. Our approach allows separating the underlying computations into their security verification and performance aspects: the security-critical operations are performed by the Trusted Cloud in a Setup Phase, whereas the performance critical operations are performed on encrypted data by the payment gateway. This allows maximum utilization of the expensive resources of the Trusted Cloud, while high loads of

queries can be processed on-demand by the gateway. The Trusted Cloud requires only a constant amount of storage and is used constantly in the Setup Phase for pre-computing encryptions. The payment gateway provides switching in the time-critical Query Phase while processing encrypted user details in parallel with minimal latency.

More specifically, the client uses the Trusted Cloud as a proxy to securely outsource his data and computations to the gateway. The client communicates to the Trusted Cloud over a secured channel (e.g. SSL/TLS) and a clearly defined interface (e.g., a web service API) which allows the client to manage the outsourced data. We optimized the amount of data transferred between the client and the Trusted Cloud using symmetric cryptographic operations. We envisioned the Trusted Cloud to be either a private cloud (e.g, University existing IT infrastructure). The detail approach will be discussed in next section.

**b. Google App Engine Platform As A Service (GAEPaaS)**

With the emergence of new Cloud Providers, identifying one that best suits the business needs of an enterprise is a challenging and difficult task. Adopting a Cloud Provider requires a detailed study of parameters like data security, SLA's and options that address the reduction of capital expenditure.

Google App Engine (Http://appengine.google.com) allows a user to run Web applications written using the Java or Python programming languages. Other than supporting the Python standard library, Google App Engine also supports Application Programming Interfaces (APIs) for the data store, Google Accounts, URL fetch, image manipulation, and email services. Google App Engine also provides a Web-based Administration Console for the user to easily manage his running Web applications. Currently, Google App Engine is free to use with up to 500MB of storage and about 5 million page views per month. Again, this platform enables building and hosting of web applications on the same system that power Google application. The survey in (Http://appengine.google.com)shows that GAE offers the fastest development, deployment, simple administration with no issues about hardware, patches, backups and effortless scalability. Hence, our private cloud in this work is Google App Engine.

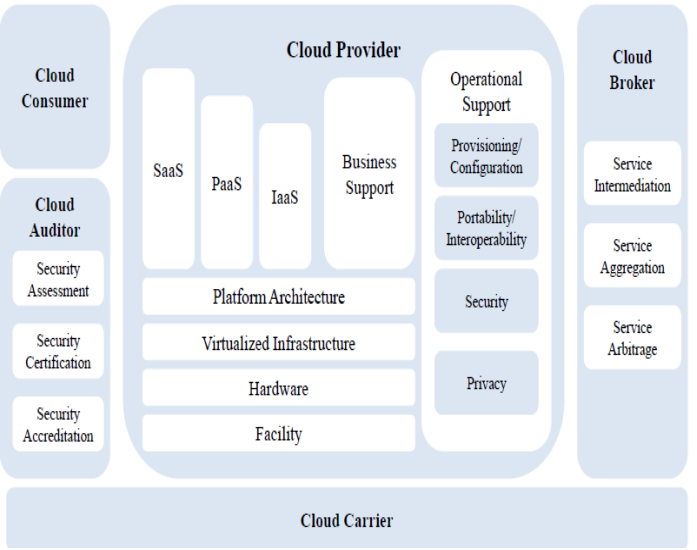



*Figure 9: TheConceptual Reference Diagram (www.en.wikipedia.org/wiki/file:cloudcomputing.svg).*

**c. Integration And Development Tools**

In this work, the following have been proposed in the prototype phase of the trusted cashless solution viz:

(i) Java Eclipse (Eclipse Helios 3.6)- IDE support
(ii) Google Secure Data Connector
(iii) Private gadgets
(iv) Google Visualization API
(v) Google Apps APIs
(vi) Google web toolkit
(vii) Google Pluggins for Eclipse
(viii) Google App Engine Java SDK 1.5.5
(ix) Google Web Toolkit SDK 2.4.0
(x) Programming Language Choice-Java.

Google App Engine runs Java applications using the Java 6 virtual machine (JVM). The JVM runs in a secured "sandbox" environment to isolate the trusted cloud application for service and security. The JVM can execute any Java bytecode that operates within the sandbox restrictions. The Administrative console provides the following details, viz: view access data

and error logs, and analyze traffic browse the application's data store and manage indexes view the status of the application's scheduled tasks.

The Supported Platform in GAE is Java Runtime Environment and Python Runtime Environment. Some of the features include:

(i) Integration with Google Accounts
(ii) URL Fetch
(iii) Mail
(iv) Memcache
(v) Image Manipulation
(vi) Scheduled Tasks and Task Queues
(vii) XMPP
(viii) Blobstore (which supports objects upto 50MB in size)

These makes for the easy implementation phase of the proposed cashless solution for the Nigerian educational sector.

### 3.2 SECURITY MODELING TRUSTED CASHLESS CLOUD.

One of the obvious and most commonly used forms of authentication in the portal is password; in the context of payment systems more commonly implemented as a personal identification number (PIN). Such a system has long been in place for authenticating users at cash-points prior to withdrawing money or processing an online form. The platform as a service infrastructure (GAE) must meet the security recommendations; also the data, application, and network security standards will be addressed in the implementation phase of this work.

### 3.3 SECURITY EVALUATION APPROACH: PROPERTIES AND REQUIREMENTS

*3.6.1. Requirements*

(i) Integrity: Sureness that information has not been altered after user forms has been processed in the portal and trusted cloud.
(ii) Authentication: Persons participating in a transaction are uniquely identified (the one they claim to be).
(iii) Fraud prevention and tolerance: prevention of parties from fraud and from financial losses in case the system crashes or the network fails.
(iv) Privacy: Information must not be revealed to unauthorized users.

*3.6.2. Cryptography and PKI*

In our cashless cloud model, to establish and efficiently implement both security and trust on Internet environment which is open, independent, heterogeneous and universal, cryptography represents the only way in which data trust can be realized. Secured Cryptographic methods ought to be trustworthy in order to generate confidence in the use of the cashless solution. Cryptographic methods considered in this work were developed in response to the needs and demands of our cashless solution.

Cryptography is represented in two forms. The first is called symmetric or secret key cryptography which uses one common key for both encryption and decryption and a second named public key cryptography or asymmetric, uses two different keys (a private and public) to transform plaintext into cipher text.

In symmetric schemes the sender and recipient of data, share a single encryption key, and the shared keys must not be revealed or exposed to unauthorized parties. In asymmetric schemes two keys are used; a ''public'' and a ''private'' key. Public keys can be freely distributed but recipients still require a way to know that a key can be trusted. To certify each public key, central Certification Authority (CA) is created. All cryptography schemes are based on the concept that only the users of the encrypted information should have the keys needed to decrypt it into something understandable. Public Key Cryptography is based on the principle that the two keys should be different, but related to each other. In a sense, they need to be inverses of one another. This form of cryptography relies heavily upon the assumption that it is computationally infeasible to determine the decryption key if the encryption key and algorithm alone are known.

Public Key Cryptography is implemented using trap-door one-way mathematical functions. These are functions which are easy to calculate in one direction but infeasible to calculate in the other direction unless certain additional parameters are known. With additional information, the inverse can be calculated easily. A product of Public Key Cryptography is the digital signature that both authenticates and guarantees that the message is original and is being sent by the person it was originally supposed to be sent from. Digital signature involves the reverse process of the encryption. The data are encrypted with the private key of an entity and anyone can decrypt it using the public key; since a public key can only decrypt the data from a corresponding private key, the identity of the sender is verified. Typical digital signatures attempt to solve the problem of tampering and impersonation in our model.

Unlike other underling technical mechanisms, cryptography scopes are to assure specific things not to happen.

Public Key Infrastructure (PKI) is a business enabling initiative that provides a means for both trusted digital identity verification and data encryption in transit. In our context, relationships and identification of parties will be realized via digital certificates. This addresses the problem of verifying the identity of the parties exchanging encrypted information over internet. Application security, Data security, Network security are to be taken care of in the trusted cashless cloud by the Google App Engine Platform as a Service (GAEPaaS). In order to ensure that data is secured (that it cannot be accessed by unauthorized users or simply lost) and that data privacy is maintained, Google cloud providers must attend to the following areas (Torry, 2009) as part of our submissions for our model:

(i) **Data protection**

To be considered protected, data from one client must be properly segregated from that of another; it must be stored securely and it must be able to move securely from one location to another. Google Cloud providers have systems in place to prevent data leaks or access by third parties. With Proper separation of roles, auditing and monitoring will be clearly consolidated.

(ii) **Identity management**

The trusted cashless cloud solution will have its own identity management system to control access to information and computing resources. Google Cloud providers integrate the client's identity management system into their own infrastructure, using federation technology

(iii) **Physical and personnel security**

Google Providers ensure that physical machines are adequately secured and that access to these machines as well as all relevant client data is not only restricted but that access is documented. The private cloud will only be managed by the institution and not outsourced. This eradicates the fears of security trust and assures greater confidence.

(iv) **Availability**

Google Cloud providers must assure clients of regular and predictable access to their data and applications. In our context (TCC)

(v) **Application security**

Google Cloud providers ensure that the application (TCC) available as a service via the cloud is secured by implementing testing and acceptance procedures for the packaged application code (Java code). It also requires application security measures (application-level firewalls) to be in place in the production environment.

(vi) **Privacy**

Finally, Google providers must ensure that all critical data (credit card numbers) are masked (key cryptography) and that only authorized users have access to data in its entirety. Moreover, digital identities and credentials must be protected as should any data that the provider collects or produces about customer activity in the cloud.

These recommendations serve to create integrity compliance and trust which will justify its adaption in the cashless strategy for the Nigerian Educational sector.

## 4. SOFTWARE DEVELOPMENT LIFE CYCLE (SDLC) METHODLOGY.

For a work of this magnitude, a fundamental process called the system development life cycle (SDLC) will be adopted. The SDLC starts with a planning phase, which identifies the business value of the proposed system, conducts a feasibility analysis, and plans the project. The second phase is the analysis phase, which develops an analysis strategy, gathers information, and builds a set of analysis models. In the next phase, the design phase, the implementers develop the physical design, architecture design, interface design, data base and file specifications, and program design. In the final phase, implementation, the system is built, installed, and maintained.

In this work, the choice of our methodology was influenced by factors like: clarity of the requirements; familiarity with the base technology; system complexity; need for system reliability; time pressures; and need to see progress on the time schedule. For our proposed model in figure 8, the rapid throwaway prototyping methodology will be used in realizing the system since it offer better options for the implementation.

### 4.1 ECONOMIC IMPLICATION OFTHE PROPOSED MODEL

The use of credit and debit cards is an established and popular alternative to cash. However, the advent of a new cashless solution that enables speed, trust and integrity compliance will be economically viable to the Educational sector as it has little cost implication in its implementation. The model is envisioned to have 95% improvement over existing security techniques which makes for successful tackling of problems of data verification, data repudiations, authentication, etc while giving greater confidence in its usage. With biometric techniques as part of the identity management interface, client authentication prior to making wire transfer will enhance its functionality. In our model, the cloud infrastructure is operated solely for an institution and may be managed by the institution or a third party and may exist on premise or off premise.

## 5 CONCLUSION AND FUTURE WORK

This paper has presented a proposed cashless solution for the Educational sector in Nigeria. Whilst technology continues to support the vision of a cashless strategy, it is believed that such alternative payment means will enhance flexibility in cashless transactions since with mobile wireless devices; users can complete cashless transactions very fast. Using Google App Engine with Java in the private cloud implementation, issues of trust, speed, security and performance are addressed our methodology (SDLC) facilitates the implementation and validations. With the current CBN policy in favour of the cashless strategy, it will only take a short time for society to fully give up on physical cash completely. This saves cost, enables productivity, flexibility and ease of migration. Future work will present our implementation results and model validations using unified modeling language (UML), Use case and vulnerability tests.

**REFERENCES**

Ahmed .A and Al-Mukaddim, "A Framework for Managing Cost Effective and Easy Electronic Payment System in the Developing Countries" unpublished)

Daniel. N, et al, 2009.The Eucalyptus Open-source Cloud-computing System ,*In 9th IEEE/ACM international symposium on cluster computing and the Grid*" Vol 10, pp.124-131Http://appengine.google.com [18 July 2008].

Http://www.en.wikipedia.org/wiki/file:cloud computing.svg.

Kalakota, R. andWhinston, 2000*"Frontiers of Electronic Commerce",* fifth indian reprint, Pearson Education Asia Pte. Ltd , pp. 295-331.

Leena.J and Sushil B, 2010. Enterprise CloudComputing: key Considerations for Adoption. *InInternational Journal of Engineering and Information Technology (IJEIT)* , vol 2 , No. 2,pp. 113-117.

PaulK.B,2006. *The cashless Society:Increased Usage of card-Based PayementSystems.*Publishers.Electronic&ComputerScienceECS,Universityof Southampton,Uk.

Rajkumar.B et al, 2009 "Cloud Computing and Emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility", *In Future Generation Computer Systems*, No.25 pp.599-616.

Srinivasa .R et al, 2009.Cloud Computing: An Overview.*Injournal of theoretical and applied information technology, JATIT* ,Vol 9, pp. 71-76

Theodosios. T. andSthephanides .G, 2005 "The concept of security and trust in electronic payments"*In Computers &Security* ,Vol 24, No.24, pp 10-15.

Whitepaper, 2011: Strawman Model v2,NIST Cloud Computing Reference Architecture and Taxonomy Working Group"*From NIST cloud computing Reference Architecture and Taxonomy Working Group* Google App Engine,

White paper: "Torry Harris, 2009" Cloud Computing Services – A comparison". *In http://www.thbs.com*

Yang. J.,2009. On-line Payment and Security of E-commerce", *Proceedings of the 2009 International Symposium on Web Information Systems and Applications (WISA'09), Nanchang, P. R. China, pp. 046-050.*

Http//www.wikipedia.org/wiki/HEBcashRegister)

# UNDERSTANDING FINANCIAL CONTAINER VULNERABILITY PARADOX IN A CASHLESS SOCIETY USING THE CYBER CRIME THEORY OF PSEUDO-OWNERSHIP

**O.B. Longe**
Fulbright Fellow & Research Scholar
International Centre for Information Technology & Development
Southern University System
Baton Rouge, Louisiana USA . 70813
longeolumide@fulbrightmail.org

***ABSTRACT***

*One of the major impetus for the proponents of cashless societies is the convenience of transacting businesses using digital financial containers (debit/credit/ATM cards). However, challenges with user privacy, network downtime and cyber fraud can impact on the use of digital financial containers. This paper x-rays the advantages and challenges of running a cashless society in the light of the new government initiatives in Nigeria. Criminological theories were used to explain possible cyber criminal activities and cyber victimization that can evolve in a cashless society. The theory of pseudo-ownership is proposed as a construct by which cyber victimization associated with digital containers can be explained. The paper concludes by advocating for more robust security measures that ties users to financial containers as a way of enhancing the security of consumers in a cashless society.*

***Keywords**: Cashless society, credit/debit/ATM cards, containers, Pseudo-ownership, security*

## 1. INTRODUCTION

Perhaps one of the major impetus driving the proponents of a cashless societies is the convenience of transacting businesses using digital financial containers (debit and credit cards) and online transactions without the need to carry cash (Marc, 2011). This ideal is therefore being encouraged in countries with weak currencies where consumers need to hold lots of cash for very basic transactions. However, the challenges a society face when running on cashless transactions are many and varied.

In the developed countries where over 80% of daily transactions are done using credit, debit and bank transfers, consumers are sometimes faced with the challenges of network failure and denial of service problems and privacy issues as a result of the fact that spending patterns are very open to the credit card companies. More challenges and concerns are the grim possibilities of credit and debit card fraud.

Financial containers are paradoxical because they confer a sense of ownership of the contents they (seem) hold on the user or owner. This is similar to what conventional financial instruments such as cheque books and passbooks do to banking customers. However, unless signatures can be perfectly copied or an insider is involved who compromised the verification and authentication process, it is difficult to access funds in an account using stolen cheque books or passbooks. Needless to say, the situation is different with digital financial containers(Philip, 2010; Sirota, 2012).

## 2. RELATED ISSUES

In the United States, the Payments Council already announced that by 2018 cheques would no longer be in use and paper payments will no longer viable. This is already evidenced by the number of trading institutional and consumer shops that accept cheque payment (LLBlynch, 2012 ) these days. In readiness for this future development, many organizations are migrating card payment systems. Payment for fuel, groceries and food can now be done through card payment systems. Arguments in support of a cashless society has centred on such advantages as the fact that cheques are things of the past, printing money is expensive, consumers are more comfortable with card payments and cards can assist in reducing crimes such as pick-pocketing as well as susceptibility to armed robberies (Arbak, 2005; Philip, 2010).

Online transactions are also becoming very popular even in the developing world. People now have the convenience of ordering for goods online, from electronic devices to household equipments, making purchases is just a click of the mouse away (Longe et al, 2012a). There is no doubt that some of these advantages are visible even in Nigeria within the last decade with the adoption of ATM transactions. However, the Achilles heel in the argument for a cashless society is the position that it is the intractability of cash that makes it a tool for crime and by extension if society does away with cash and we can do away with crime (Jen, 2011; Marc, 2012, Laseinde, 2012). This argument, is to say the least partial and incongruent. The proponents seem to be oblivious of electronic crimes such as card fraud, hacking, privacy invasion and identity theft online. In the same vein, financial containers confer a sense of ownership of the contents they seems hold on consumers such that long after contents have been taken fraudulently through different forms of cyber crimes already

mentioned, the card owner still carries the container around with the confidence that he can transact business with it when the need arise (David, 2012).

**a. Cashless Nigeria**

In a Nation with over 150 Million inhabitants, the proponents of a cashless society in Nigeria argued that it will aid in the drastic reduction in money laundering, terrorist financing and other economic and financial crimes (Abimbola, 2011). Others believe that a cashless society will encourage financial inclusion for most Nigerians since less than 30 per cent of bankable Nigerian adults own bank accounts. A larger percentage of the population rather keeps their money under their mattresses, in their pockets and probably in old cooking pots (Abimbola, 2012; Adana, 2011; Nahimah, 2012).

Scholars also opined that a cashless Nigeria will promote the implement realistic monetary and fiscal policies that will reduce inflation and encourage investments (Abimbola, 2012; Nnamdi, 2011).Ladeinde (2012) mentioned that the strike action in January of 2012 against the removal of fuel subsidy in Nigeria was a litmus test for how effective the cashless society will run. He mentioned that during the strike, Nigerians were left with no means to carry out financial transactions other than the use of ATM machines and electronic payments. The Central Bank of Nigeria (CBN) recently pegged daily cash withdrawals and lodgments by individual to N150,000 and corporate bodies N1m respectively with effect from the 1st of June 2012 (LAdehinde, 2012).

This move has continued to generate reactions from the generality of Nigerians. In a nation with high level of illiteracy and where most traders operate the "Cash and Carry" paradigm, it will take more than mere semantics to convince a groundnut seller or cocoa farmer to financially proceeds with all confidence in a "plastic card".

**b. Financial Policy Issues**

At the policy level, the Money Laundering Prohibition Act (MLPA) of 2004, presently before the National Assembly for update and amendment represents an effort made to move Nigeria towards a cashless society. Unfortunately, there were also incidences of ATM malfunctioning and citizens could not gain access to monetary. Worst are reported cases of card frauds and frustrations that besieged the banks on resumption of business at the end of the strike action.

In particular was a case in Ibadan, Nigeria of a bank customer who withdrew the sum of N10,000 to buy petrol for his household cars and generator (at black market rate), at the expiration of the strike action, he went into the banking hall to make another withdrawal using a cheque and discovered that on the same day he withdrew N10000 with the ATM card, an additional sum of N500000 was withdrawn from his account. Investigation into the incidence revealed that his debit card was cloned (duplicated) by fraudsters and used for the unauthorized fraudulent withdrawal.

Aladenusi and Azike (2012) opined that the security of electronic cash cannot be the sole responsibility of financial institutions. Claiming that the source of security breach on electronic cash over the decades points to sources such as from third-party processor of payment data, they said conscious efforts must be made by regulatory authorities to perform a security assessment of Point of sales devices and other information security measures must be installed at retailers' and third-party processor's end to ensure security of the transaction in the public.

## 3. CRIMINOLOGICAL THEORIES EXPLAINING CYBERCRIME AND CYBER VICTIMIZATION

Theories explaining cyber criminality can also double to provide insights into why people are victimized online. The routine activity theory and lifestyle exposure theory are criminological theories that explains cyber crime on the basis of proximity to motivated offenders, exposure to high-risk of crime, target attractiveness, and absence of guardianship (Cox & Richards, 2009; Cohen and Felson, 1979; Cohen, et al., 1981; Miethe& Meier, 1994; Yucedal, 2010). These theories state that for a crime to be committed, the following must be concurrently present:

(i) A suitable target is available: The suitable target here refers to a person, object or place.
(ii) There is lack of a suitable guardian to prevent the crime from occurring: The capable or suitable guardian refers to a deterrent like police patrols, security guards, neighborhood watch, door staff, vigilant staff and coworkers, friends, neighbors and CCTV systems.
(iii) A motivated offender is present: This presupposes that there can be no victim without the intentional actions of another individual.

Routine Activity Theory (Cohen and Felson, 1979) does not only offer some explanation on why cyber crime occurs, it can also suggest the fact that cyber-crime victimization will occur as a result of the variation in people's routine activities of everyday life which now revolves around the Internet and electronic communication.

These routine Internet usages definitely increase vulnerability and the probability that motivated offenders will converge with suitable targets in the absence of guardians (Bossler & Holt, 2009; Abdullah, 2005; Longe et al 2012b).

Opportunity Theory(Felson& Clarke, 1998) asserts that Opportunity to commit a crime is a root cause of crime. Also, they posit that no crime can occur without the opportunity and therefore opportunity plays a role in all crimes, not just those involving physical property but online crimes. For cyber crime to be successfully committed, the opportunity for crime is multiplied by the simple fact that the criminal is no longer "location-bound" and thus this anonymity creates more opportunity to victimize people online. Cornish (1986) rational choice theory argues that people make basic decision to commit a crime, or to not commit a crime, based on a simple cost-benefit analysis.

The rational choice theory focused on non-sociological factors that can influence the decision to commit crime. It is an

approach used by social scientists to understand human behavior, in the rational choice theory. "Rationality" means that an individual acts as if balancing costs against benefits to arrive at action that maximizes personal advantage. In relation to cyber crime for example, the criminal takes the decision to victimize based on his understanding of vulnerability to which victims are exposed online because of their shallow understanding of basic security measures that could be taken to safeguard them.

The crime displacement theory focuses primarily on reduction of the opportunity to commit crime. The efforts tend to displace or move the crime from one locale to another locale (Felson and Clarke 1998). Crime displacement may involve moving Crime from one location to the other, moving crime from one time to the other, moving crime from one target to the other, changing the approach to committing the crime and changing the type of crime that is to be committed. Cyber victimization is done by a calculated appraisal of each of the possible moves that yields the best result (Danquah & Longe, 2012).

A cyber predator may offer to assist a handicap user key in ATM pin or help an old lady with eyesight problems read an ATM card details in response to a phone request and by so doing scam the subject. Jaishankar (2008) proposed a state transition theory where he argued that persons with repressed criminal behavior (in the physical space) have a propensity to commit crime in cyberspace, which they would not otherwise commit in physical space, due to their status and position. It also implies that the status of persons in physical space does not transit to cyber space. Incidentally, the same notion applied to cyber victimization in the sense that individual behavior repressed in physical space that helps individuals avoid falling victim of crime may not be repressed in cyber space.

The Space transition theory argues that, people behave differently when they move from one space to another. This can make people who ordinarily are not vulnerable to physical assault because of their position or individuality in physical space become cyber crime victims in cyber space. Usually unethical behaviours are just a click of the mouse away in cyber space. Consider an individual who ordinarily will not visit or go to a brothel in the physical space. He can log into a sex site online, provide his credit card details for registration and by so doing get scammed.

## 4. THE CYBER CRIME THEORY OF PSEUDO-OWNERSHIP

Among all forms of cyber crimes such as cyber bullying, cyber espionage, cyber stalking, pedophiling and cyber terrorism, the most common form of cyber crime remains financial crimes (Longe and Osofisan, 2011). Most financial crimes on the Internet has been committed through the use of financial containers details such as ATM Pin numbers, credit or debit card numbers, log in details for these cards as well as just other details associated with this containers. We therefore state the Theory of Pseudo-ownership in respect of the foregoing that:

Financial Containers such as credit cards, debit cards, travel cards and ATM cards confer a sense of ownership on a human who carry digital financial containers and lowers their level of consciousness relative to their vulnerability to digital fraud.

Postulates of these theories are

(i) The sense of ownership conferred by financial containers on human carriers are Pseudo since most containers do not report transactions in real-time.

(ii) The perceived ease of use associated with containers makes them more vulnerable to cyber attacks as they become routinely dominant for financial transactions online

(iii) The perceived usefulness associated with containers makes lowers users consciousness level on the relative absence of strong guardianship for usage

(iv) The fact that usage of financial containers can easily be monitored and tracked makes users more vulnerable in online transactions

(v) Relative anonymity of users and usage makes it more difficult to tie financial containers to individual

The need to find appropriate basis for the explanation of cyber victimization is a motivation factor for this theory. What is now required is to empirically test the Longe's theory of Pseudo-Ownership. Generally speaking, pseudo-ownership is explained as the consciousness that container contents are the owners when they are already defrauded through cyber victimization. The owner or carriers of the content hold it – even as a legal tender carrier- until he realizes that the money in the container is gone. Since most ATM cards do not report transactions in real-time, there is no way or mechanism to inform the owner that he or she has been defrauded.

In a situation where there are message alerts to inform bank customers on transactions or activities in their accounts, network problems and denial of service constraints sometimes prevent the account owner from receiving report until long after the criminal act has been perpetrated ease of use and perceived usefulness also sets users in a mood that makes them transfer in their subconscious, the responsibility of security to the banking or financial institutions. These days, criminals cream off account by simply harvesting card details from unencrypted sources and selling such details to willing buyers. Current card designs do not tie usage to individuals. It is therefore very possible for close allies such as friends, colleagues and family members to obtain container details and use it to victimize authorized card owners.

## 5. CONCLUDING REMARKS

The increasing wave of migrating most transactions to an electronic platform will increase the pool of Internet users and by extension the volume of people exposed to cyber victimization. An understanding of cyber criminality and cyber victimization will go a long way in assisting the formulation of social, technical and legal policies to assist in dealing with the cyber crime and cyber victimization problem. Policing the cyberspace has remained a daunting task partly because of the

socio-technical dynamism introduced into crime detection and apprehension on electronic platforms.

While it is timely to adopt and enact new laws to meet the growing dimensions of cyber activities. Majority of the challenges in cyber space also has to do with the readiness and understanding of the cyber crime victims of the cyber space. This paper examined the pros and cons of moving towards a cashless society viz –a-viz the challenges posed to such an initiative by cyber crime and cyber victimization.

Existing criminological and social theories are used to explainscyber crime and cyber victimization and by extension a new theory is proposed to explain cyber victimization with respect to financial containers. Furthermore, the paper provided insights on the dynamics of financial containers and how the new theory can be used to explain causation in cybercriminal activities. In future we shall conduct empirical research to validate the assumptions of the Longe's Cyber Crime Theory of Pseudo-ownership in order to justify its application to the domain of cyber security

## REFERENCES

Abdullah, A. 2005. Cyber-Crime Fear and Victimization: An Analysis of A NationalSurvey. http://www.cse.msstate.edu/~dampier/study%20materials/NationalCrimeStats.pdf

*Abimbola, A. 2012. The Imperative Of A Cashless Society. The NEWS .* http://thenewsafrica.com/2011/05/23/the-imperative-of-a-cashless-society/

Adanna, A. 2011.Nigeria Moves towards a Cashless Society.FACE2faceAfrica. http://face2faceafrica.com/article/nigeria- moves-towards-being-a-cashless-society

Aladenusi, A. &Azike, A. 2012. Cashless Society – Is Nigeria ready for the information security challenges http://www.businessdayonline.com/NG/index.php/business-intelligence/30952- cashless-society--is-nigeria-ready-for-the- information-security-challenges Friday, 16 December 2011 00:00

Arbak, E. 2005.Social status and crime. Documents De Travail – Working Papers W.P. 5-10, November 2005, GATE Grouped'AnalyseetTheorieEconomiqueEcully – France

Bossler Adam M., Holt Thomas J., 2009. Online Activities, Guardianship, and Malware Infection: An Examination of Routine Activities Theory, International Journal of Cyber Criminology (IJCC) ISSN: 0974 – 2891 January-June 2009, Vol 3 (1): 400–420

Cohen L. E., and M. Felson. 1979. Social change and crime rate trends: A routine activity approach. American Sociological Review 44: 588-608

Cox, J. & Richards, K. (2009), Routine Activity Theory and Internet Crime, Crimes of the Internet, Pearson, p.302-316

Danquah, P & Longe, O.B 2012 Cyber Deception and Theft – An Ethnographic Study on Cyber Criminality from a Ghanaian Perspective. Vol. 11, No. 3 Journal of Information Technology Impact www.jiti.net

David, S., 2012.Should We Fear A cashless Society. The Open Salon.http://www.salon.com/2012/03/12/should_we_fear_a_cashless_society/singleton/

Jaishankar K., 2008., Space Transition Theory of Cyber Crimes, Crimes of the Internet, Pearson, ISBN-13:978-0-13-231886-0 pp.283-299

Jen, E., 2011. Cashless Society: The Way Forward for Nigeria. http://www.cp-africa.com/2011/10/08/cashless-society- the-way-forward-for-nigeria/

Ladehinde, K. 2012. CASHLESS SOCIETY: Lessons From Subsidy Removal Strike.http://businessnews.com.ng/2012/01/23/cashless-society-lessons-from-subsidy- removal- strike/

LLBlynch, K. 2012. Is a cashless society likely. http://debatewise.org/debates/1582-is-a-cashless-society-likely

Longe, O.B, Danquah, P. &Ebem, D.U. 2012.Deindividuation, Anonymity and Unethical Behavior in Cyber Space – Explorations in the Valley of Digital Temptations. Computing & Information Systems Vol. 16. Issue 3 No. 1. http://cis.uws.ac.uk/research/journal/index.html

Longe, O.B, Danquah, P &Totimeh, F. 2012. An Empirical Evidence of Deviant Cyber Space Behavior: The Case of a Website Trap. The 86th Annual Conference of the Louisiana Academy of Science – March, 2012, Alexandria, Louisiana, USA.http://www.laacademy.org/status.html

*Longe, O.B. &Osofisan, O.A. 2011. O*n the Origins of Advance Fee Fraud Electronic Mails: A Technical Investigation Using Internet Protocol Address Tracers," The African Journal of Information Systems: Vol. 3: Iss. 1, Article 2. http://digitalcommons.kennesaw.edu/ajis/vol3/iss1/2

Marc, B. 2011. The Perils of a Cashless Society - http://www.forbes.com/sites/alexknapp/2011/11/29/the-perils-of-a-cashless-society/

Miethe, T. D., & Meier, R. F. 1994.*Crime and its social context : toward an integratedtheory of offenders, victims, and situations*. Albany: State University of New York Press.

Nnamdi, O., 2011. Cashless society is possible in Nigeria Intermarc boss. http://www.vanguardngr.com/2011/11/cashless-society-is-possible-in-nigeria-intermarc-boss/

Nahimah, A.N. 2012. Attaining cashless society in Nigeria. Lagos. Daily Trust Newspaper Monday, 06 February 2012 0

Philip, A. 2010. Is a Cashless Society on the cards http://www.telegraph.co.uk/finance/newsbysector/banksandfinance/6968143/Is-a- cashless-society-on-the-cards.html

Sirota, D. (2012): Should We Fear A cashless Society. The Open Salon. http://www.salon.com/2012/03/12/should_we_fear_a_cashless_society/singleton/

Yucedal, B. 2010. Victimization in Cyberspace: An Application of Routine Activity and Lifestyle Exposure Theories. PHD, Kent State University, College of Arts and Sciences / Department of Political Science, 2010.http://etd.ohiolink.edu/view.cgi/YUCEDAL%20BEHZAT.pdf?kent127929 0984

# SURVIVABILITY IN E-PAYMENT SYSTEMS: A HOLISTIC APPROACH

**D. Dawodu**
Forestry Research Institute of Nigeria,
Jericho, Ibadan.
dotundawodu@yahoo.com

**G. M. M. Obi**
International Business Systems,
12 Moleye St, Alagomeji, Yaba Lagos.
gmm.obi@consultant.com

***ABSTRACT***

*The increasing adoption of e-payment and the criticalness that it be possible to carry out payments for goods and services at all times, even in adverse conditions, make it imperative that e-payment systems be survivable. Therefore vectors that impede the realization of mission goals of such systems must be identified, analyzed and appropriate mitigating strategies to possible untoward incidents put in place. However, a close look at works that have been done in this area reveals gaps: (1) in the underlying security assumptions being no longer valid in the contemporary environment, (2) in the works not taking a holistic view of the e-payment system and hence being one dimensional analyses, and (3) in focusing on the traditional e-payment model and not taking into account developments in the e-payment landscape - possible multiplicity of the interacting entities in the aforementioned model, or new entrants into the e-payment calculus. This work seeks to fill the observed gap. It presents a multidimensional consideration of security issues in e-payment systems based on the security paradigm of survivability, and the pragmatic perspective of an e-payment system being a multi-layered entity composed of new entrants into the e-payment calculus, and a possible multiplicity of one or more of the interacting entities of the traditional model.*

***Key Words**: Survivability, multi-layered, unbounded system, value robust. self-confiaurina.*

## 1. INTRODUCTION

The huge growth of e-commerce in terms of the volume of goods and services that are being traded on-line, induce a corresponding growth in e-payment. This is understandable for, in order to complete an e-commerce transaction, payment must be fully integrated into the on-line dialogues. Thus just as the complexity of conventional commerce has led to the evolution of many different payment instruments so also has e-commerce brought about a range of electronic payment methods. The deployment of information systems and networks and the entire infomation technology environment have changed the face of e-commerce and hence that of e-payments dramatically, and it is the prediction that this will continue to be. The unstoppable growth of unbounded systems (an unbounded system is any system in which participants have incomplete or imprecise information about the system as a whole and the system boundaries are not known, Fisher and Lipson (1999)), including the Internet, and the attendant tidal wave of e-commerce in its wake indicate that the seemingly inseparable duo of e-commerce and e-payments will represent an enormous industry worldwide, an impetus that will continue to inject dynamism into the industry in the years to come so that, as larger numbers of organizations and individuals come on-line, there is plenty of scope for growth.

The attainment of the aforementioned development on e-payment is nevertheless dependent on the security of the payment systems. According to the Central Bank of Nigeria, Central Bank of Nigeria (2009), the total volume and value of online POS transactions in 2009 showed decreases of 23.1% and 31.5 %.respectively, compared to those in the preceding year. The decline was attributed "to the fears expressed by customers over the increased numbers of fraud associated with card transactions". A recent study shows that the growth of m-commerce, an aspect of e-commerce, is being stifled by security issues in the e-payment systems. The study report concludes, "If security concerns can be eradicated, the m-commerce market may finally reach its long-anticipated exponential growth." These reports corroborate a Ponemon Institute's study, Ponemon (2005) which shows that not only do consumers expect that there are safeguards and procedures in place to protect them from untoward acts, but also that if it becomes obvious that those safeguards are not working, they will churn, Ponemon (2005). Thus, although the emerging growth of e-commerce over the unbounded networks and systems such as the Internet is bringing exciting opportunities for organizations and individuals through the corresponding growth of e-payment, the security risk to the latter is also imminent. These continuing changes offer significant advantages but also require a much greater emphasis on security.

Ever more powerful personal computers, converging technologies and the widespread use of unbounded systems such as the Internet have replaced what were modest, stand-alone systems in predominantly closed networks. Today, the e-payment environment is increasingly interconnected, with the connections in some cases crossing national borders. The nature and type of technologies that constitute the e-payment infrastructure have also changed significantly. The number and nature of infrastructure access devices have increased to include fixed, wireless and mobile devices with a growing percentage of access being through "always on" connections. Each of the interacting entities possibly has plural multiplicity and the possible connectivity scenarios have quadrupled. Consequently, the nature, volume and sensitivity of e-payment

information that is exchanged have expanded substantially. As a result of increasing interconnectivity, e-payment systems and networks are now exposed to a growing number and a wider variety of threats and vulnerabilities, thereby raising new issues for security.

This work responds to this dynamics by advocating a holistic appreciation of the changes taking place in the e-payment system and its environment, and the attendant security issues. It takes the position that there be a focus on security, in terms of ensuring that the system fulfills its mission despite attacks, failures or accidents, in the development of e-payment systems and associated networks - a clear break with a time when security was too often afterthoughts treated as a separate thread in an e-payment system engineering process. The e-payment system needs to be reliable and secure, to fully enjoy the benefits of which, the security vectors must be identified, analyzed and appropriate mitigating strategies to possible untoward incidents put in place.

The work is organized as follows: In section 2 is presented related works and the contribution of this work. The proposed approach to security is presented in Section 3, followed by the conclusion in section 4.

## 2. RELATED WORKS AND CONTRIBUTIONS OF THIS WORK

Most of the studies that have been undertaken on security issues in e-payments have been based on two perspectives: the traditional e-payment model, and the fortress security model, both limiting.

### 2.1. CONSIDERATIONS BASED ON THE TRADITIONAL E-PAYMENT MODEL

First, adopting the traditional e-payment model loses sight of developments in the e-payment landscape in which there are now possibly more than the traditional five interacting entities of client, merchant, payment system provider, the issuer and the acquirer, as there are now new entrants of the mediators/intermediaries and e-payment enhancing mechanisms, with possible multiplicity of some or all of the interacting entities.

The traditional model assumes that each of its five entities consist of a single element; one client buying from one merchant with one issuer, one acquirer and one payment system provider. The flow of messages in the traditional e-payment model is shown in Figure 1.

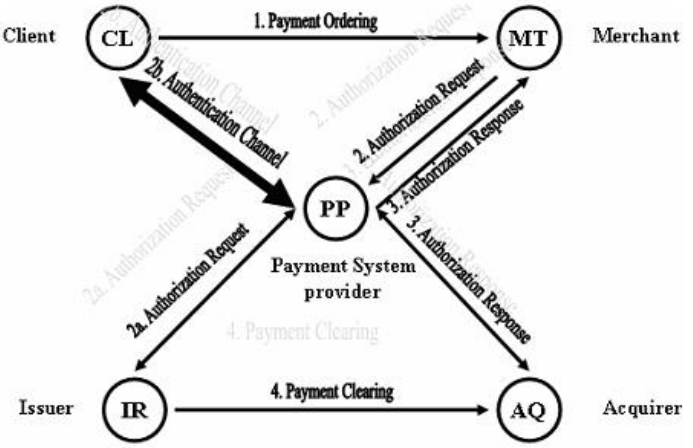



*Figure 1: Flow of the messages in the traditional e-Payment system (adapted from Carbonelliet al., 2007)*

In a practical e-payment there are possibly mediators/intermediaries or clients' agents who source the goods and negotiate on behalf of the clients thus providing many value adding functions that cannot be easily substituted or 'internalized' through direct supplier-buyer dealings. There possibly are as well, enhancing mechanisms (entities that have network node capabilities, e.g. net work smartcards). Beside there are now possible multiplicity of these interacting entities, for example those in the client and merchants arising from demand aggregation and supply aggregation respectively) [Carbonell, et al (2007), Odokumo& Obi (2012)], and more connectivity scenarios (32 in the practical e-payment model compared to 8 in the traditional model). From the foregoing, traditional topologies such as (one-to-many, ring, mesh, many-to-many) now need to be considered in the payment model, and also, need to be integrated with the other previous aspects in order to represent real applications. This has security implications and exacerbates the security concerns. The flow of messages arising from the extension of the principal entities is as shown in Figure 2. The plain arrows indicating direct connection while dotted arrows are indicative of the connections being direct or indirect.

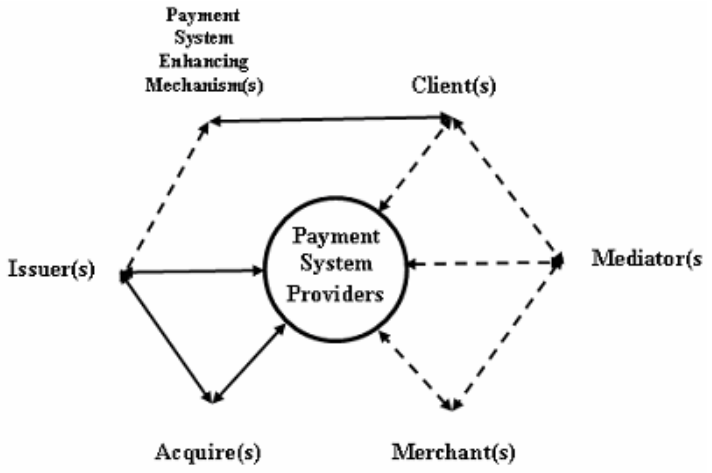



*Figure 2: The flow of messages in the e-payment system's interacting entities*

### 2.2. CONSIDERATIONS BASED ON THE TRADITIONAL SECURITY PARADIGM

On the security side the focus of the existing works is on the protection of the system by hardening defences against penetration to intruders, dealing with the e-payment system transaction without due account, if any, being taken of the security of the underlying technology infrastructure. As will be shown shortly, this fails to recognize the nature of the e-payment system as a multi-layered entity, requiring a holistic multi-layer adhering approach to the consideration of its security. Some of these studies that propose some form of a security layered framework for mobile payment systems [Zheng& Chen (2005), Lal Das, et al, 2005, and Agarwal et al, 2007 ], apart from being based on the traditional e-payment model did not adopt a multi-layer coordinated and integrated approach which is more appropriate to the e-payment system. For example Agarwal et al (2007) investigated vulnerabilities in four dimensions: in the choice of hardware/software platform, in technology, in the cell phone operating system and in the security threats posed by mobile worms. This was however done for each of the layers independently and from the perspective of only protecting the system from compromise in transacting payment through a cell phone. Other works focused on one aspect or the other and are not holistic. For example, Godbol and Pais [Godbol and Pais (2008)] worked on challenges facing service providers such as interoperability, security and infrastructure of the mobile payment system, and propose architecture for micropayments which addresses these issues, while Min.& LI (2008) discussed critical factors which affect usability, and Ondrus et al. (2006) proposed a multi-actor multi-criteria framework to facilitate the assessment of mobile payments for the Swiss public transport industry. In the same vein, Meng and Ye, (2008) discussed security requirements and solutions for mobile commerce and proposed a mobile payment model based on Wireless Application Protocol, while Liu et al.,(2005) proposed an innovative model for mobile payment which focuses on enhancement of privacy and non-repudiation.

These initiatives being based on the traditional security paradigm are primarily focused, as characteristic of such initiatives, on the detection and prevention of intrusions and attacks rather than on all the security considerations, including continued correct operation while under attack. A major goal of these traditional security considerations is fault tolerance, usually concerned with redundancy that is required to detect and correct up to a given number of naturally occurring faults. Beside nature not being malicious, conventional failure models make significant assumptions, in particular, assuming faults to be independent and random. These assumptions are no longer valid in the contemporary environment of the e-payment systems, for example, the presence of intelligent adversarial attacks can significantly challenge these conventional models, and software and protocol vulnerability often become more important considerations in the presence of an adversary. In what follows are proposed the adoption of a security paradigm and in a manner that is appropriate to the nature of e-payment systems.

### 2.3. CONTRIBUTIONS OF THIS WORK

This work presents an e-payment system as a multi-layered entity and proposes a holistic approach to the consideration of its security. This is a coordinated and integrated approach that provides complementary mechanisms at the different layers, drawing on the benefits of each mechanism, and takes into account developments in the practical e-payment - possible new entrants with each interacting entity being of possible multiplicity..

## 3. THE PROPOSED APPROACH

The proposed approach is based on two very vital considerations: First, the e-payment system should satisfy the critical requirement that payments for goods and services be possible at all times even in adverse conditions. Second, it should be adaptive as changes occur in its components and environment. Taking these two together, the e-payment system has to be value robust, i.e. have the ability to continue to deliver prescribed stakeholder value in the face of changing contexts and needs. This is the challenge confronting systems architects in the contemporary environment of unbounded and large-scale systems - the specification, development, procurement, operation, and maintenance of systems with critical security requirements supportive of a new paradigm: value robustness. This is what survivability is about, and it leads to the first consideration for e-payment security.

### 3.1. ADOPT SURVIVABILITY AS THE SECURITY PARADIGM

Survivability is traditionally defined in military systems as the capability to avoid or withstand a hostile environment. For example, Ball (2003) analyzes design techniques, armaments, and tactics for combat aircraft survivability. In Ball's framework, survivability is enhanced by both reductions in the susceptibility of systems to disturbances (*e.g.*, stealth, maneuverability) and reductions in the vulnerability of systems to disturbances (*e.g.,* redundant flight controls and surfaces, independent fuel feed tanks).

In this paper, survivability is viewed as the ability of a system to continue to achieve specified value delivery in spite of disturbances - the ability of a system to satisfy and to continue to satisfy certain critical requirements (e.g., specific requirements for security, reliability, real-time responsiveness, and correctness) in the face of adverse conditions. Such adverse conditions might typically include hardware faults, software flaws, attacks on systems and networks perpetrated by malicious users, and electromagnetic interference. Thus, survivable systems can prevent a wide range of systemic failures as well as penetrations and internal misuse, and can also in some sense tolerate additional failures or misuses that cannot be prevented.

Formally, survivability is defined as the ability of a system to continue to fulfill its mission despite attacks, failures or accidents, Lipson and Fisher (1999). Unlike Ball's formulation, a three-part constituent of survivability is considered in terms of reducing susceptibility, reducing vulnerability, and recovery from the impact of, and the adaptation to, the disturbance. These are the three R's which attributes are hallmarks of survivability and which the e-payment systems must have: Recognition, Resistance, Recovery and adaptation. The first

two, recognition and resistance relate to preventing the occurrence of untoward incidents. Current security approaches to protect information systems have focused on preventing attacks from being successful, primarily on improving component and system reliability, by hardening defenses with authentication, encryption, and a variety of layer-violating network devices (i.e., firewalls, network address translators, intrusion detection systems). What is not being captured is the restoration of affected components, the survivability of an **entire** system as a whole unit to failures or attack. While security approaches may protect one layer of an e-payment system they often introduce single-point-of-failure vulnerabilities in other layers. Survivability fills this gap. It is the **sum**of the parts, not **some**of the parts.

Therefore, rather than focus on hardening systems to make them impenetrable to intruders, the focus of survivability is on systems mission, imbuing systems with the capability of continuing to fulfill mission goals despite attacks failures or accidents - being able to recognize and resist untoward incidents as well as being robust during, and recovering from, the incidents and adapting to them.

**a. Build Survivability Into The E-Payment System**

The second consideration is that survivability should be built into the e-payment system at the system engineering stages, not retrofitted or considered as a separate thread in the system engineering process. This encompasses all the layers of the e-payment system described below, not just the application component.

Typical system life-cycle models, particularly software systems, do not focus on creating secure systems, and fall short when the goal is to develop systems such as the e-payment system, with a high degree of assurance, Marmor-Squires and Rougeau (1998). If addressed at all, security issues are often relegated to a separate thread of project activity, with the result that security is treated as an add-on property. This common misconception of isolation of security considerations from primary system-development tasks typically results in an unfortunate separation of concerns, as observed in Mead and McGraw (2001), and a significant amount of security flaws. Some of these flaws can involve serious architectural issues. In a best case scenario, developers can expect to invest an immense amount of time and effort to fix these flaws. Worst case, the application may require recoding and an overhaul of its architecture. Performing application security in this manner is of course, incredibly expensive and time consuming. Integrating survivability into the early phases of the software development life cycle neutralizes this cost and produces more secure applications in far less time. Survivability should be integrated and treated on par with other system properties to develop systems with required functionality and performance that can also withstand failures and compromises, Mead & McGraw (2001). An approach to achieving the integration of survivability into the system engineering process, in the case of software systems is SQUARE, discussed in Mead (2008). In Richards, et.al (2008) a set of seventeen survivability design principles were presented, spanning susceptibility reduction, vulnerability reduction, and resilience enhancement strategies. In a 2009 work by the same authors, Richards et al (2009), a process is described for applying the survivability design principles to a system analysis methodology integrating decision theory with model-based design. This initiative of applying the design principles serves both to augment the creativity of system designers by ensuring consideration of a broad trade-space of design alternatives and to quickly screen a large number of candidate design variables before proceeding to concept evaluation.

**b. Adopt Security Engineering**

Overtime the security and survivability of the e-payment system or any system for that matter, degrades. This arises from changes in the environment or usage of the system, or changes to the elements that compose the system, which often introduce new or elevated threats that the system was not designed to handle and is ill-prepared to defend itself against.

A way to addressing this is to adopt security engineering for the e-payment system. Security Engineering focuses on the tools, processes, and methods needed to design, implement, and test complete systems, and to adapt existing systems as elements of their constituents or the environment of the systems evolves The e-payment system must be imbued with the capability to evolve to meet new threats to its security and survivability, to recognize changes in security and survivability risks that trigger the need to enter the evolution phase of the system's life cycle. Possible approaches to achieving this for software and engineering systems are presented in Lipson (2006) and Anderson (2008) respectively.

Figure 3 illustrates the flow of a systems engineering process in which survivability is integrated

**c. Appreciate That The E-Payment System Is Multi-Layered**

Composed of a combination of legacy and emerging technologies, the e-payment environment, broadly viewed, is heterogeneous and multi-layered (specifically, 3-layered, with a backbone running through these). This has to be appreciated for the survivability initiatives to be effective. At the top is the 'application/service' layer, which uses network services for end system processes and provides interface to the user. In the middle is the 'traffic/transport layer', which provides routing and congestion control for connections across the network that supports the e-payment system. It consists of the networking environment such as circuit-switching, packet-switching (TCP/IP), ATM, and virtual private networks (for special services). The bottom layer is the "transmission/physical layer". It typically consists of a mixed technology infrastructure containing fiber and non-fiber wire based systems as well as wireless components (microwave, cellular, satellite, etc.). The forth and administration component provides the administration required for the e-payment system. This forth has been included because of the vulnerabilities arising from malicious insiders due to inappropriate administrative related countermeasures. Thus, an e-payment service may traverse several interconnected networks with different physical layer and network layer components.

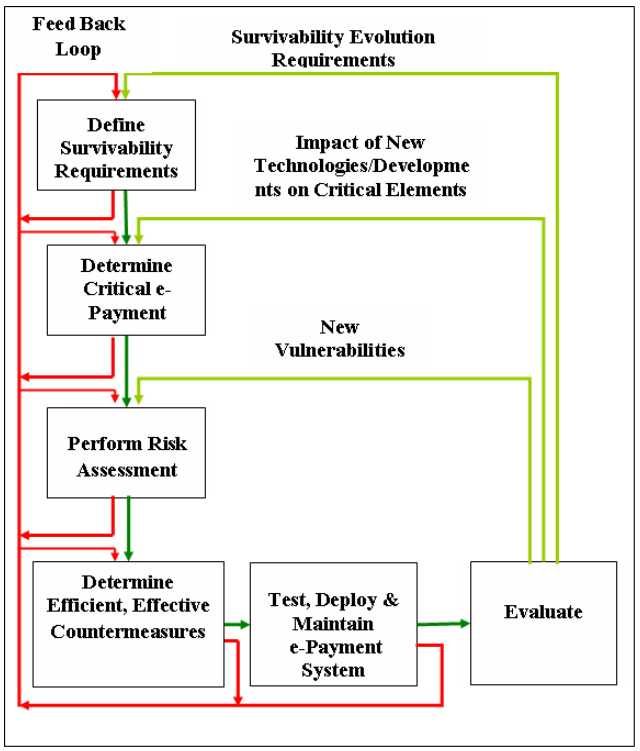



*Figure 3: Survivability Integration Approach (Adapted From Obi(2010))*

A number of vulnerabilities arise at each of these layers: from the ATM's, POS's, and other devices that come into play in e-payment to the technologies and standards and the applications – the platforms for their creation and the operating systems. The layers and the attacks/faults in the multi-layer survivability setting are shown in Figure 4.

| Layers | Attacks/Faults |
|---|---|
| Application/User Interface | Malware/Viruses<br>Application Platform, bugs<br>Operating system intrusion<br>Cryptography faults/flaws<br>Quality of service degradation etc. |
| Traffic/Transport | Circuit/Trunk interface fault<br>Routing corruption<br>Hw/sw switch fault<br>DNS corruption/hijack<br>DoS/DDoS<br>Network management corruption<br>Traffic monitoring etc. |
| Transmission/Physical | Cable – cut/mishap<br>Spectrum – jamming/fading<br>Sniffing<br>Electromagnetic pulse (EMP) etc. |

Malicious Insider

*Figure 4: Payment System Attacks/Faults in the multi-Layer Survivability Setting*

Although some of these attacks/faults are specific with respect to each layer, there are, never-the-less, some that occur in two or more layers, as the malicious insider attack shows. Therefore, the e-payment security considerations should not be singular focused at each layer independent of other layers but should be holistic. This is dealt with in the next section.

**d. Adopt A Holistic Coherent, Coordinated, And Integrated Approach**

Given the multi-layered environment of the e-payment system, survivability and hence restoration can be addressed at the multiple layers.

Different restoration techniques can occur independently at each of these e-payment network layers. For instance as a result of some fault at the application layer a wireless telephone handset may automatically switch from a call over an analog infrastructure to a call over a digital infrastructure or vice versa. Given some other fault, or even the same fault as before, the traffic layer connections may be transparently routed around link or switch failure using disjoint paths; while at the physical layer 1:N trunk protection switching can provide a hot-standby for back hoe cable cuts. In this multi-layer perspective results may extend from conventional attacks which kinetically destroy links and nodes at the physical layer to virtual attacks which destroy or corrupt computer operating systems, application software, and databases at the application layer.

*i. Coordinate between,and syncretize survivability engendering mechanisms at, different layers*

Although it may be possible to address untoward events in each layer of the e-payment system completely independently, it is more appropriate and desirable to adopt a multi-layer, holistic, coordinated and integrated approach. The singular focus on each layer independent of the others has actually contributed to the fragility of systems, from a holistic perspective. For example, authentication schemes that are dependent on a certification authority invariably introduce a one point of failure to the entire system, just as cryptographic protocols that rely on secure base station hosts. Firewalls which break end-to-end protocols for network management while allowing trivial insider attacks once circumvented, and more, are cases that show that the layer violating approach of focusing on protecting layers independently do not capture the survivability of the entire system as a whole unit to attacks, failures or accidents. That a restoration mechanism performs well at a single layer does not imply that it would perform well when applied to all the layers of the entire system.

*ii. Engender survivability adaptively*

In 3.3 the security engineering approach was proposed for the creation of the e-payment system so that the system is capable of adapting to the dynamics of its environment. This approach provides restoration algorithms at each layer that are suitable for automatic invocation by the e-payment network components, resulting in a self-configuring system that adapts to the changing fault environment. Combined with the coherent coordination it eliminates the danger of focusing on a particular type of attack at a single layer, as attackers can easily adapt to a different vulnerability at another layer. It is known that in the extant practice of focusing on the protection solutions, while security engineers harden defences against

anticipated attacks, the successful attacks are usually the unknown ones - those that the engineers never thought about Anderson (1993), Schneier (1999)]. For example a physical attack with a strategically positioned traffic-level denial-of-service attack may prove unrecoverable at the application layer despite operating system defences. Thus e-payment systems must be flexible so as to be able to reconfigure transparently given that incidents of previously unknown and unanticipated attacks are inevitable. The optimization problem of how this can be achieved efficiently is considered in Yurcik and Tipper, (2000).

The multi-layer perspective of the e-payment system provides a unified approach that not only addresses the survivability of the fragile e-payment infrastructure but also defends against malicious attacks. This unified approach is needed across the layers. It includes a syncretism of mechanisms at different layers, complementary and coordinated, with appropriate trade-offs and based on the engendering survivability adaptively. This also has the benefit of the maximum use of available resources, of account being taken of the underlying technology infrastructure so that evolving survivable e-payment network architectures can be generated, and of focus on four key aspects that can significantly enhance e-payment survivability: (i) an application that evolves to meet new threats to the e-payment system's security and survivability (ii) establishing and maintaining survivable topologies that strive to keep the e-payment network connected even under attack, (iii) design for end-to-end communication in challenging environments in which the path from source to destination is not wholly available at any given instant of time, (iv) the use of technology to enhance e-payment survivability - such as adaptive networks and satellites.

## 4. CONCLUSION

In this work, an approach to the consideration of security issues in the e-payment system was presented. It proposes that in view of the critical nature of these systems:

(i) They should not be merely secure but be survivable.

(ii) Survivability should be adopted as their security paradigm, and should be built into the system at the system evolution stages, adopting security engineering, not retrofitted.

(iii) It should be appreciated that the e-payment system is multi-layered and rather than focus on protecting each layer independently a holistic, coherent, coordinated and integrated multi-layered approach should be adopted in dealing with issues of security of e-payment systems, as the former could introduce vulnerabilities in some other component or layer.

The work provides an insight which should be helpful in better analyzing the survivability of e-payment systems and in their design and deployment.

## REFERENCES

Agarwal S, Khapra M, Menezes B and Uchat N, (2007) Security Issues in Mobile Payment Systems, *Proceedings of ICEG 2007: The 5th International Conference on E-Governance*, Hyderabad, India, December, 2007, pp 142-152

Anderson, R., (1993), Why Cryptosystems Fail, *1st Conf. on Computer and Communications Security,* 1993, pp 215-227.

Anderson, R. J., (2008), Security Engineering: *A Guide to Building Dependable Distributed Systems 2nd Edition,* Wiley Publishing Inc. Indianapolis

Ball, R., (2003), *The Fundamental of Aircraft Combat Survivability Analysis and Design, 2nd Edition*. Reston: AIAA Education Series, 2003.

Carbonell, M., Sierra, J., Torres, J. and Izquierdo, A., (2007) Security analysis of a new multi-party payment protocol with intermediary service. In: *DEXA Workshops 2007,* pp. 698–702 (2007)

Ellison, R.J, Fisher, D.A., Linger, R.C., Lipson, H.F., Longstaff, T.A., and Mead, N.R., (1999), Survivable Systems: An Emerging Discipline, *Proceedings of the 11th Canadian Information Technology Security Symposium (CITSS)*, Ottawa, Ontario Canada, pp 138-143.

Fisher, D.A. and Lipson, H.F., (1999), Emergent Algorithms – A New Method for Enhancing Survivability in Unbounded Systems, *32nd Hawaii International Conference on System Sciences* (HICSS-32), 1999, pp 7043.

Godbol R. and Pais A., (2008), Secure and efficient protocol for mobile payment.*10th international conference on electronic commerce (ICEC)' 08, Austria*, ACM 2008, Art icle 25.

Lal Das M., Saxsena M. and Gulati V. (2005). A security framework for mobile to mobile payment network.*Proceeding of the ICPWC'05*, IEEE computer society 2005, pp 420-423.

Liu J., Liao J. and Khu X..(2005), A system model and protocol for mobile payment.*Proceeding of IEEE international conference on ebusiness engineering (ICEBE'05)*, IEEE computer society 2005, pp 438-442.

Lipson, Howard, (2006), Evolutionary Systems Design: Recognizing Changes inSecurity and Survivability Risks, *Technical Note CMU/SEI-2006-TN-027*

Lipson, H.F.; and Fisher, D.A.; (1999), Survivability- A new Technical and Business Perspective on Security, *Proc. Of the New Security Paradigm Workshop, IEEE Computer Society press* 1999, pp 33-39

Marmor-Squires, A.B., and Rougeau, P.A., (1998), Issues in Process Models and Integrated Environments for Trusted Systems Development, *Proc. of the 11th National Computer Security Conference. Fort George G. Meade*, MD, Oct. 17-20, 1988: 109-113.

Mead, N. R, (2008), Incorporating Security Quality Requirements Engineering (SQUARE) into Standard Life-Cycle Models, *Technical NoteCMU/SEI-2008-TN-006*

Mead, N.R. and McGraw, G. M., (2001), "Managing Software Development for Survivable Systems." *Annals of Software Engineering* 2(2001): 45-78.

Meng J. and Ye L., (2008), *Secure mobile payment model based on WAP*. IEEE computer society 2008, pp 1-4.

Min Q. and LI S.. (2008), From usability to adoption – a new m-commerce Adoption study framework. *International conference on communication and mobile computing* ,IEEE computer society 2009, pp 309-313.

Obi, E. E, (2010), A Survivable Enterprise Website Design, *M.Sc Thesis Napier University*

Odokumo, E. E., and Obi, G. M. M., (2012), A Model of a Pragmatic Secure e-Payment System, Preprint.

Ondrus J., and PigneurY.. (2006), A multi stakeholder multi criteria assessment framework of mobile payments: an illustration with the swiss public transportation indsurry. *Proceeding of the 39th Hawaii international conference on system science* , IEEE computer society 2006, pp 42a.

Ponemon Institute, LLC, (2005), Report Issued, April 5, 2005, *Privacy Trust Survey for Online Banking*

Rhodes D.H., (2004), Report on the Air Force/Lean Aerospace Initiative Workshop on Systems Engineering for Robustness, Massachusetts Institute of Technology, July 2004.

Richards, Matthew G., Ross, Adam M., Hastings, Daniel E., and Rhodes, Donna H., (2008), Empirical Validation of Design Principles for Survivable System Architecture, Proceedings of the 2nd IEEE Systems Conference, Montreal, Canada pp 1-8

Richards, Matthew G., Ross, Adam M., Hastings, Daniel E., and Rhodes, Donna H., (2009), Survivability Design Principles for Enhanced Concept Generation and Evaluation, Proceeding of the19th INCOSE Symposium, Suntec City, Singapore., July 20-23, 2009, pp 1055-1070

Ross A.M., (2006), Managing Unarticulated Value: Changeability in Multi-Attribute Tradespace Exploration, Doctor of Philosophy Dissertation, Engineering Systems Division, MIT, June 2006.

Schneier, B. (1999), Risks of Relying on Cryptography, Comm. of the ACM, pp. 144, October 1999.

Yurcik, W. and Tipper, D., (2000), Survivable ATM Group Communications: Issues and Techniques, 8th Intl. Conf. on Telecom. Systems, pp. 518-537, 2000.

Zheng X. and Chen D.. (2005), Study of mobile payment System. Proceedings of the IEEE International Conference on E-Commerce (CEC'03), IEEE computer society 2005, pp 376-381.

# AN EXPLORATORY STUDY ON ELECTRONIC RETAIL PAYMENT SYSTEMS: USER ACCEPTABILITY AND PAYMENT PROBLEMS IN NIGERIA

**G. O. Ogunleye**
Redeemer's University(RUN)
Department of Mathematical Sciences
(Computer Science Programme)
KM 46, Lagos-Ibadan Expressway, Redemption Camp, Mowe, Ogun State
ope992000@yahoo.com

**O.S. Adewale**
Department of Computer Science
The Federal University of Technology, Akure
adewale_olumide@yahoo.co.uk

**B.K. Alese**
Department of Computer Science
The Federal University of Technology, Akure
kaalfad@yahoo.com

***ABSTRACT***

*Payment for goods and services in Nigeria is characterized by long queues, long distance traveling and time wasting that negatively affect business activities and ultimately economic development. Settling utility bills, payment for goods and services, and money transfers has been a major headache for individuals and firms in Nigeria resulting in declined business activities and huge debt to most of the utility services providers. Indeed, most Nigerians are yet to fully realize the benefits of the technological advances made in banking services like networking of business branches, electronic transfers and use of automated teller machines. The few payment mechanisms that are available are not being well patronized by bank's customers. The focus of this paper is to assess the issue of user acceptance in the existing electronic retail payments and also to ascertain the impact in solving some of the problems in retail payment for goods and services in Nigeria.*

***Keywords****: Retail Payment, Electronic Payment, Customers, Nigeria*

## 1. INTRODUCTION

In recent times, there has been an urged clamour for the replacement of cash as an exchange for goods and services to accommodate a host of online services. As buyers and sellers increasingly transact business miles away from each other, there has been an increased demand by both parties for alternative means of payment.

The introduction of the internet has transformed the world into a global village. The world has witnessed an upsurge of electronic payment instruments meant to facilitate trade and simplify payments (Abor, 2004). Before the introduction of electronic payment into the Nigerian banking system, all customers had to walk into the actual bank to do transaction of all kinds. Customers had to queue up and spend more hours to talk to a teller to make their transactions. The inconveniences caused by these long queues can discourage someone to make payment. For many years, bankers, technology specialists, entrepreneurs, and others have advocated for the replacement of physical cash and the introduction of more flexible, efficient and cost effective retail payment solutions. Countless conferences and seminars have been held to discuss the concepts of cashless and "chequeless" society. Electronic retail payment has been designed to help individual customers and companies as well as the banks itself in eliminating or reducing some of the problems inherent in the settlement and payment process (Federal Reserve Bank of New York, 1996). Customers can pay their bills without having to actually move to the bank's premises. They may also have access to their account information and even transfer money to other accounts in the comfort of their homes.

Nigeria banks are making huge investments in technology to upgrade their infrastructure in order to provide new electronic information-based services. Electronic services such as online retail
banking are making it possible for individuals and small institutions to take advantage of new technologies at quite reasonable costs.

In Nigeria, electronic retail payments are being continuously developed, to replace or reduce paper-based payments. Many new payment services have come into existence in recent years, most of which are based on technical innovations such as card, telephone and the Internet.

Payment for goods and services in Nigeria is characterized by long queues; long distance travelling and time wasting that generally affect business activities and ultimately economic development. Settling utility bills, payment for goods and services, and money transfers have been a major headache for individual and firms in Nigeria resulting in declined business activities and huge debt to most of the utility providers. In fact, the country has not yet realized the full benefits of the technological advances in electronic payment such as the use of cards, automated teller machines (ATM), the Internet, mobile phones, and etc. The payments and clearing system in

the country is under developed. For instance, cheques drawn in Lagos against accounts held in banks in Lagos could take three days whilst cheques drawn on different regions can take several weeks. There is no central clearing system to clear debit card transactions between banks. The banking halls continue to be immersed with the long queues as people troop into the bank hall en masse to collect their monthly wages or salaries. Many people have been holding large sums of money outside the banking system as a result of the ordeal one has to go through before withdrawing money or making payment (Sarpong, 2003). However, faced with such problems in the payment process, only a few payment solutions have been introduced so far in Nigeria to solve them. Cash still remains the most popular retail payment instrument, despite the increase in the introduction of electronic payment schemes in the country. Whether consumers are adopting the current and emerging payments mechanisms is another issue confronting the banks.

The purpose of this paper is to tackle different electronic payment schemes available in Nigeria, discuss patronage and to ascertain its contribution to the elimination or reduction in problems inherent in the payment process in Nigeria. The paper described and briefly analyzed recent and potential future trends in electronic payments in Nigeria. It also assessed issues of user acceptability of the current payments systems. Furthermore, the paper also investigated attempts that have been made by some of the banks to introduce such a system, and the successes and failures.

It is also meant to assist consumers, businesses and service providers in Nigeria to understand the various electronic payment alternatives. It is also in response to the growing need in Nigeria to develop non-cash payment products and clearing systems in order to reduce the over-dependence on cash payments. We concentrate on those electronic payment systems that make use of the banking system since that is where these services are mostly being offered currently in Nigeria. We discussed some electronic payments products in some countries like Sweden and other countries for comparative analysis. With any new payment product, it is important that the key features of the product are clearly explained to the consumers and ensuring that the product actually works as described. Customers who fail to fully understand how the system work and the benefits to be derived from its use may take inadequate precautions in using the product. For this study, the following are the major research questions:

(i) Can electronic payment system replace existing payment systems and solve payment problems?
(ii) How are customer attitudes about electronic payments changing?
(iii) What are the impediments to market development and innovation in electronic payments?

While there are many emerging types of electronic retail payment schemes, special emphasis will be given to payment methods that utilize the services of banks. Such schemes include ATMs, the Internet, mobile phone, debit and debit cards, etc.

## 2. LITERATURE SURVEY

### 2.1. DEFINITIONS OF ELECTRONIC PAYMENT SYSTEMS

Due to the nature of electronic payment systems, there have not been a widely or universal definition for it. But we have attempted to bring some few notable definitions given some writers. These range from now-familiar automated teller machines (ATM) to Internet bill payments.

According to Humphrey et al (2001), electronic payment refers to cash and associated transactions implemented using electronic means. Typically, this involves the use of computer networks such as the Internet and digital stored value systems. The system allows bills to be paid directly from bank accounts, without being present at the bank, and without the need of writing and mailing cheques. E-payment can be defined as 'payment by direct credit, electronic transfer of credit card details, or some other electronic means, as opposed to payment by cheque and cash' (Agimo, 2004).

According to Kalakota and Whinston (1997), "electronic payment is a financial exchange that takes place online between the buyer and the seller. The content of this exchange is usually the form of digital financial instrument (such as encrypted credit card numbers, electronic checks, or digital cash) that is backed by a bank or an intermediary, or by a legal tender." For the purpose of this paper, the term "electronic payment" refers to as convenient, safe, and secure methods for payment of bills and other transactions by electronic means such as card, telephone, the Internet, EFT, and etc. Electronic payment gives consumers an alternative to paying bills and debts by cash, cheque, money order, etc. Its main purpose is to reduce cash and cheque transactions.

According to Pariwat&Hataiseere (2004), for the achievement of effective and efficient retail payment systems, the following considerations that shape the choice of payment method for consumers and businesses should be taken into account; the convenience, reliability and security of the payment method, the service quality, involving such features as the speed with which payment are processed; the level and structure of fees charged by financial institutions; taste and demographic; and technological advances which have improve the speed, convenience and flexibility of different payment systems.

### 2.2. FACTORS AFFECTING PAYMENT CHOICE

#### *2.2.1. Customers' Wealth/Levels of Income*

Consistent with Kwast and Kennickell (1997) research, wealth has an important role to play in terms of consumer's decisions on payment choice. Consumers' wealth may influence payment choice and the availability of payment instruments that one can choose. For instance, while wealthy consumers may be able to fund their obligations generally, consumers that experience brief financial shortfalls may not find electronic bill payment desirable as a payment instrument (Mantel, 2000). In such a situation, the consideration of the risk factor will let some consumers to avoid using pre-authorized electronic bill payment.

*2.2.2. Educational Level*

On the bank customers' survey, we also focused on education, because this might affect the demand for electronic banking products. For example, Kwast and Kennickell (1997) have illustrated how education play important role in determining household use of e-money products.

Kwast and Kennickell concluded that the US market for such products is still highly specialized, with the demand coming almost entirely from higher income, younger, and more educated households that have accumulated significant financial assets.

Educational levels of customers determine whether consumers will adopt electronic payment or not. Studies have shown that highly-educated people patronize electronic payment products than less-educated people. The technicalities involved in some electronic payment transactions discourage less educated customers to patronize its use (Annon, 1999).

*2.2.3. Employment Levels*

Those employed who receive their pay through the banks are more likely to use electronic means of payment. Employees, through their constant contacts with banks are more exposed to payment products, and are therefore, likely to patronize the products. According to Ferguson (2000), more than half of the workers in the US, in 2000 receive a direct deposit of their pay through the Automated Clearing House (ACH).

*2.2.4. Transaction-Specific Factors*

Transaction-specific is another factor that influences consumer decision-making in payments.

This relates to the specific nature of the payment being made, where it is being made, and how the consumer views their relationship with the merchant (Mantel, 2000). The use of a particular payment instrument may depend on the value of the bill (whether it is large or small). Also the availability of payment infrastructure determines the choice of payment instrument.

**2.3. RECENT TRENDS IN ELECTRONIC PAYMENTS**

In this section, we provided a brief background to some of the rapid emergence of methods which used electronic means to make payment. Some of the new techniques represent automation of existing methods of payment, whereas others are new or revolutionary.

*2.3.1. Card Payments: Automated Teller Machine (ATM)*

ATM is a combined computer terminal, with cash vault and record-keeping system in one unit, permitting customers to enter the bank's book keeping system with a plastic card containing a Personal Identification Number (PIN). It can also be accessed by punching a special code number into the computer terminal linked to the bank's computerized records (Rose, 1999). Mostly located outside of banks, it can also be found at airports, shopping malls, and places far away from the home bank offices, and offering several retail banking services to customers.

First introduced as cash dispensing machines, it now provide a wide range of services, such as making deposits, funds transfer between two or more accounts and bill payments. (Abor, 2004).

*2.3.2. Electronic Purses/Wallets*

There are two categories of e/wallet, these are;

(i) E-wallets that store card numbers. This is a virtual wallet that can store credit card and debitcard information. Other information that can be stored on this card is passwords, membership cards, and health information. Some of the e-wallets make it easier for consumers to buy goods using the card.

(ii) E-wallets that store card numbers and cash. The second category of a digital wallet is where consumers store digital cash, which has been transferred from a credit card, debit card or virtual cheque inside their e-wallets. It operates like having a virtual savings account where charges are made for ongoing purchases, particularly micro-payments.

*2.3.3. Electronic Funds Transfer at Point of Sale (EFT/POS)*

EFT/POS is an online system that involves the use of plastic cards in terminal on merchants' premises and enables customers to transfer funds instantaneously from their bank accounts to merchant accounts when making purchases. It uses a debit card to activate an EFT process (Chorafas, 1988). It actually comprises two distinct mechanisms: debit and credit cards.

*2.3.4. Credit Cards*

This is a plastic card that assures a seller that the person using it has a satisfactory credit rating and that the issuer will see to it that the seller receives payment for the goods or items delivered. This represents the automated capture of data about purchases against a revolving credit account (Pierce, 2001).

*2.3.5. Debit Cards*

These were a new form of value-transfer, where the card holder after keying of a PIN, uses a terminal and network to authorize the transfer of value from their account to that of a merchant. Introduced more recently, debit together with credit cards represent the most rapidly growing method of payments in several OECD countries (Pierce, 2001).

When a payment is made through a debit card, the funds are immediately withdrawn from the purchaser's bank account. The advantage is that the buyer has the funds to make the purchase and paid for right away, so there's no credit card shock when the statement arrives in the mail

*2.3.6. Smart Cards*

A smart card is a plastic card with a computer chip inserted into it and that store and transacts data between users(Smart Card Basics, 2004). The data, in a form of value or information is stored in the card's chip, either a memory or microprocessor. "Smart card-enhanced systems are in use today throughout several key applications, including healthcare, banking, entertainment and transportation." One of the features of this card is that it improves the security and convenience of transactions. The system works in virtually any type of network and provides security for the exchange of data.

### 2.4. MOBILE

According to Zika (2005), "a mobile payment is an electronic payment made through a mobile device (e.g., a cell phone or a PDA). In the field of payments, mobile phones opportunity is seen in the embedded SIM (smart) card used to store information of users. The advantage of not needing to use other devices such as modems, point of sale terminals, and card readers for mobile payments is also quite clear.

Costello (2003) envisaged that further developments in the mobile payments content were inevitable in the near future. Mobile devices might be used in micro-payments such as parking, tickets, and charging mobile phones.

### 2.5. TELEPHONE BANKING

Telephone banking or telebanking is a form of virtual banking that deliver financial services through telecommunication devices. Under this mechanism, the customer transacts business by dialing a touch-tone telephone connected to an automated system of the bank. This is normally done through Automated Voice Response (AVR) technology (Balachandher et al, 2001).

Telebanking has numerous benefits for end users. For the customers, it provides increased convenience, expanded access and significant time saving. Instead of going to the bank or visiting an ATM, retail banking serves the same purpose for customers to get the services at their offices or homes. This saves customers time and money, and gives more convenience for higher productivity (Leow, 1999).

### 2.6. HISTORICAL CHANGES IN PAYMENT USE IN OTHER COUNTRIES

Japan has been known to have a high cash holding, low non-cash use, and a high percent of electronic payments. High cash use for point-of-sale transactions while non-cash payments are largely electronic and almost entirely for bill payment and employee payroll disbursements (Humphrey and Hancock, 1997).

Norway, in 1996 has about 60% of non-cash payments in an electronic form compared to 1987 figure of 90% non-cash payments. Robinson and Flatraaker (1995) study of Norwegian postal and commercial banks found out that the total of payor bank and payee bank costs of an electronic bill payment through a giro was $0.49 while its paper-based substitute averaged $1.34 (Humphrey and Hancock, 1997).

In Finland, Sweden and Denmark, customers can use several different payment methods for transacting business. The mobile phone sector in Finland is developing rapidly. Some purchases can be paid for via a mobile phone with such costs included in the customer's monthly mobile phone bill. Also tickets for tram, underground Finland line ferry traveling in Helsinki can be paid for by sending a text message to a service number. The customer gets his ticket as a reply text message after 30 seconds and can show it to a controller if necessary. These purchases are later included on the mobile phone bill (The Banker, 2004) threat to civil liberties.

## 3. METHODOLOGY

This section describes the methodology used for this paper and suggests different barriers to retail payment systems in Nigeria.

### 3.1. QUALITATIVE ANALYSIS OF USERS EXPERIENCES WITH E-PAYMENT

To analyze the survey data obtained from the survey questionnaire, we employed descriptive statistics to ascertain the level of customer's reaction to e-payment products. We analyzed the results of the survey questionnaire administered.

### 3.2. SURVEY PARTICIPANTS

Data were gathered from the questionnaire sent to customers, bank staff, and corporate bodies.

A total of 150 questionnaires were sent to bank employees, customers and corporate bodies. 5 questionnaires were sent to each of the 10 banks studied, while 50 questionnaires were given to customers and 50 questionnaires were also given to corporate bodies to solicit for their view. Of the 50 questionnaires sent to the banks, all of them responded representing approximately 100% response rate. Out of the 50 questionnaires given to bank customers to answer, 49 responded given a response rate 99.8%, and this was due to the presence of those who administered the questionnaires – making sure that customers have actually responded. All those who agreed to respond to the questionnaires were made to provide instant answers, and those questions that they found it difficult to understand were explained to them.

Most of the respondents to the questionnaire who have initiated payment using electronic means valued more than one preference, but it appeared that most were primarily driven by just one or two preferences across different payments they were making. For instance, 33% confirmed that their desire for e-payment includes the ability to review, initiate, stop, and record payments as well as customer service if problems arise. 22% indicated that using e-payment will minimize cost, while 14% felt that error resolution are convenient and are tailored to meet their needs. For privacy/security, 11% indicated that for e-payments' ability to withhold information that may be detrimental if disclosed, they prefer making payments by electronic means.

### 3.3. PERSONAL PREFERENCES

#### *3.3.1. Customers Personal Preference for E-Payment*

Another factor influencing payment instrument choice pertains to customers' personal preferences. Based on the survey questionnaires, five general consumer preferences were identified: (1) control and customer service; (2) budgeting and record keeping; (3) incentives and low cost; (4) convenience; and (5) privacy and security.

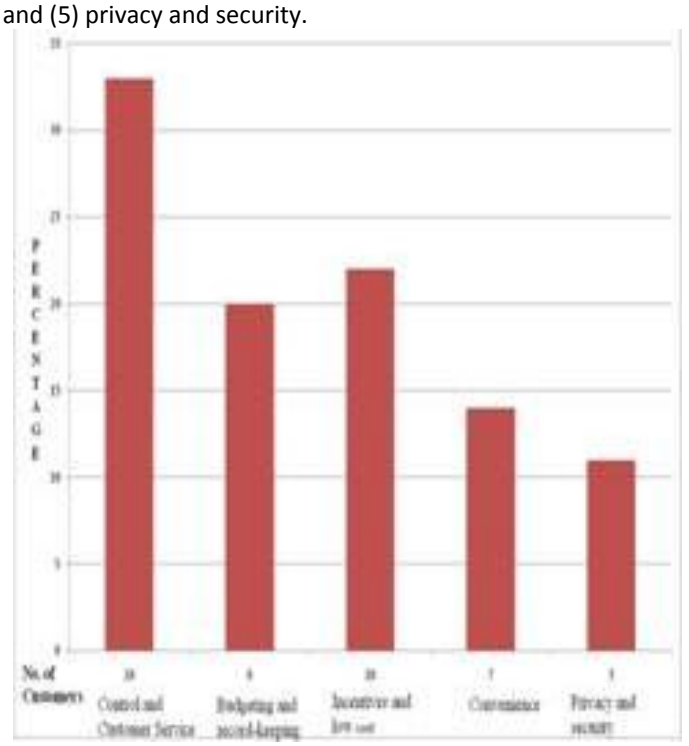



*Figure 1: Customers Personal Preference for E-Payment*

A series of questions were designed to examine the perception of bank customers about the different payment services. Customers were asked to rank the various means of payment available to them, and as expected, cash was overwhelming favourite. Maybe this was due to maturity of cash usage and the fact that other payment products are not well-developed in Nigeria. The results are shown in figure 2.

The reasons given were that it is easy, carries no interest and payment are resolve immediately.

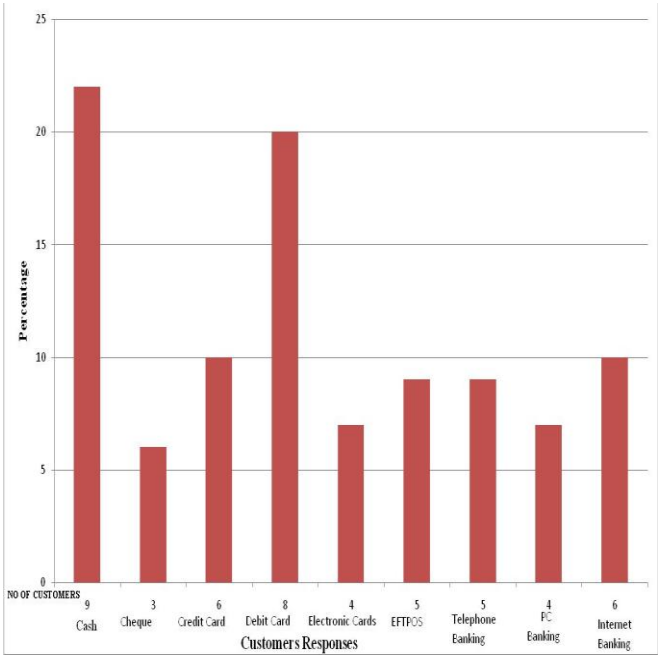



*Figure 2: Ranking of Payment Methods*

Over 22% of the respondents ranked cash as their most preferred method of payment. Debit card was the next preferred method of payment (20%), followed by Internet Banking (10%), Credit Cards ( 10%) and Telephone Banking (9%).

Most respondents were of the view that they are not used to the electronic payment methods, but majority indicated that they would like to shift into e-payment if the banks will introduce more of them with enough education. 20% indicated they prefer to use debit cards since it can be used to make purchases, at the same time to pay bills. 6 respondents indicated that they prefer creditcards, because that would allow them to make purchases even if they are not present at the point of sale.

### 3.4. CUSTOMERS IN FAVOUR OF ELECTRONIC PAYMENT PRODUCTS

Customers were asked to indicate whether they are in favour of a nation-wide introduction of e-payment products in the country. In all, 45 respondents answered in the affirmative, with the rest indicating that they disfavour its introduction. Specifically, 33 out of 36 (representing 90 %) with senior secondary school certificates and above were more in favour of e-payment instruments while those with education below SSS were less in favour of e-payments (figure 3).

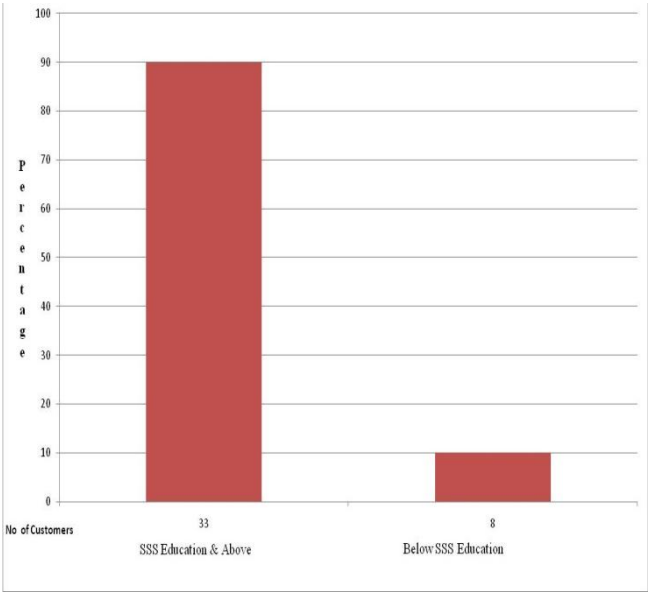



*Figure 3: Customers in Favour of Electronic Payment Products*

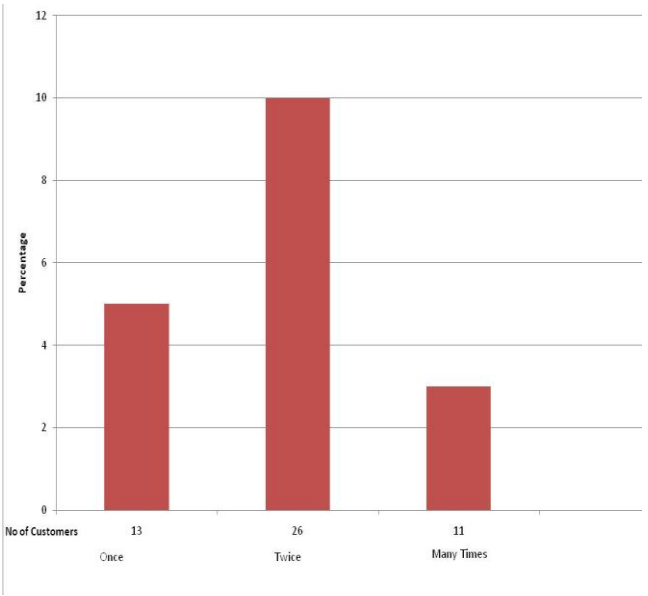



*Figure 4: Use of Electronic Payments by Customers*

### 3.5. ACTUAL USAGE OF ELECTRONIC PAYMENT METHODS BY CUSTOMERS

It was surprising to find out that over 80% responded indicated that they have not used any of the electronic payment mechanisms to make payment.

Only 18% confirmed that they have actually used one or more of the electronic channels for payment.

This shows that the number of customers who have embraced the use of electronic payment is low in Nigeria(figure 4).

Customers were asked to enumerate some of the problems confronting them in bills payment, payment for goods and services, and settlement of debt. Customers' response to this part of the survey was very revealing. Problems range from bad nature of bank notes to long queues at bank and utility payment premises.

Of the 50 response received from bank customers, majority cited long queues and time wasting at bank premises and at utility collection point as a major problem that needs a critically look.

The most common problems that the respondents cited are long queues and time wasting at bank premises and utility collection points. Out of the 50 customers surveyed, 40% and 20% cited long queues and time wasting at bank premises respectively as the major problems confronting them.

### 3.6. LONG QUEUES AND TIME WAITING

Even though the introduction of computers and ATMs has improved waiting time at the banks, many customers still complained about the long waiting time. 15 of the respondents indicated that they had to wait about 30 minutes to 2 hours to get served at the banks. Most of the respondents indicated that there were no proper queuing systems at many of the banks. The majority of the respondents indicated that the absence of queuing system has at times led to confusion about the order of customers to serve. Some customers also bypass the queue and receive services from the tellers (figure 5).

### 3.7. BAD ATTITUDES OF BANK TELLERS

Some of the respondents felt that the behaviours of some bank tellers leave much to be desired. Nine (9) of the respondents representing 15% indicated that some of the bank tellers' behaviour does not match with the overall goals of the banks, and that this needs to be checked. They cited this is the main reason why they prefer other mode of payment such as e-payments to avoid encounters with bank tellers. Some of the reasons they gave are that some of the bank tellers are slow, unduly delay customers, always attend to other social or private matters, and sometimes allows other customers to bypass the queue to be served (figure 5).

### 3.8. ARMED ROBBERY ATTACKS

15% of the respondents cited armed robbery attacks as the main reason why they prefer e-payment to cash or cheque. Recent incidents of armed robbery attacks on customers who withdraw huge sums of money from the banks have heightened customers' fears about withdrawing large sums of money from the banks. It is uncommon in Nigeria to find a whole business organization withdrawing physical cash to pay workers wage manually. Some of them end up being attacked on their way from the banks resulting in huge losses to those organizations (figure 5).

### 3.9. BANKING HOURS

In terms of banking hours, 10% indicated that they found the banking hours very inconvenient (figure 5). Of those who expressed dissatisfaction with the banking hours, over 64% indicated their preferences for longer hours from 8:00 a.m. - 6:00 p.m.

Furthermore, 36% indicated their preference for bank opening hours on Saturdays as in other developed countries.

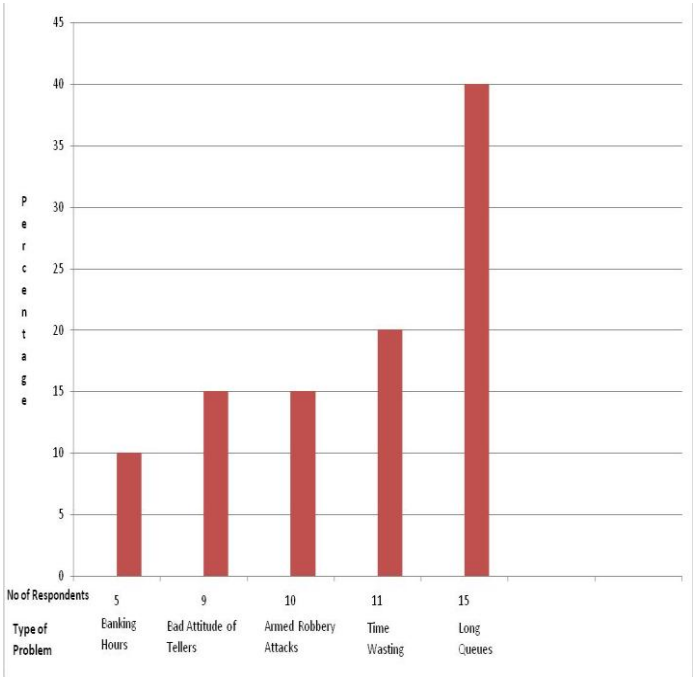



*Figure 5: Payment and Settlement Problems*

### 3.10. E-Payment has helped to solve Retail Payment Problems

The introduction and use of electronic payment instruments holds the promise of broad benefit to both business and consumers in the form of reduced costs, greater convenience and more secure, reliable means of payment and settlement for a potentially vast range of goods and services offered worldwide over the Internet or other electronic networks. One such benefit is that electronic payments enable bank customers to handle their daily financial transactions without having to visit their local bank branch. E-payment products could save merchants time and expense in handling cash The resource cost of a nation's payment system can account for 3 percent of its GDP. Since most electronic payments cost only around one-third to one-half as much as paper-based non-cash payment, it is clear that the social cost of a payment system could be considerably reduced if it is shifted to electronics. Automating could increase operational efficiency. Automating and streamlining electronic payments made from self-serve channels such as ATMs, branch office terminals, and point-of-sale (POS) systems can reduce paper-based errors and costs. New payment mechanisms have enhanced consumer convenience. Bill-payment over the Internet is growing in popularity among people who have adopted other new technologies, such as computer and ACH credit (debit deposit). New payment arrangements, such as the government's Electronic Benefit Transfer system (EBT) or payroll cards, enable people without bank accounts to use ATM services or POS debit services. For consumer-to-business point-of-sale and bill payments, electronic payments will reduce the need for business working capital associated with the delay in processing paper-based non-cash payments.

### 3.11. BARRIERS TO RETAIL PAYMENT SYSTEMS IN NIGERIA

#### *3.11.1. Confidence and Security*

There is lack of adequate security with the use of certain electronic payment devices like card payments. The lack of security when processing transactions over the Internet is posing a great threat to its adoption. Security, confidence, reliability and efficiency are fundamental features of any electronic payment solution. Security makes consumers more inclined to trust and to use a newly developed electronic payment solution. It was only after the credit card industry assured users that their exposure to criminal misuse of cards was limited that confidence in that form of payment developed." Since electronic retail payments relies heavily on credit cards for identification and payment, the credit card companies refusal to insure its customers against fraud will inhibit its adoption.

#### *3.11.2. Telecommunication Infrastructure*

The telecommunication infrastructure in Nigeria is under-developed. But for electronic retail payments to thrive, this infrastructure is a primary requirement. The telecommunication services are generally of poor quality, which impedes against the development of retail payment technologies. The speed and quality of line is unsatisfactory, especially outside metropolitan areas.

#### *3.11.3. Lack of Knowledge and Skill*

Both consumers and business enterprises have limited knowledge of what services exist, how they operate and what benefits to be derived. Due to high level of illiteracy, most of the people do not recognize the economic importance of electronic retail payments. Most Nigerians especially the aged, lack the skills and knowledge required to ensure efficient and effective use of the system.

Our investigation showed that only a few number of the adult population have computer knowledge and skills. The low level of knowledge in the payment devices and how each of them works has led to low patronage of the existing retail payment products. Information on practical issues with regard to handling, confidence-related issues on security, integrity and consumer law issues concerning internal and external trade are necessary to increase patronage.

#### *3.11.4. Attitude to New Products*

The problem of reaching a critical mass is explained by the reluctance of people to use new schemes until a sufficient relative number of their associates use them. It is difficult to convince customers to switch providers especially if they are not particularly dissatisfied with the systems they have been using.

## 4. CONCLUDING REMARKS

This study has covered some issues associated with payment transactions, instruments, and systems prevailing in Nigeria. It contains a description and analysis of various

electronic payment instruments from the viewpoint of end-users. Furthermore, it looked into the trend and the use of electronic payment in some selected countries. Finally, it included a description of innovations in electronic retail payments in Nigeria.

As elaborated earlier in this study, the retail payment systems in Nigeria during the past few years have undergone progressive technological developments, but have also remained highly paper-based and inefficient. The outcome of the study shows that cash transactions continue to play a significant role in almost all countries and in particular Nigeria. Even the developed countries are making every effort to ensure a cashless society and Nigeria cannot wait to embrace this concept.

As consumers seek out new ways to do business, the market must provide innovative electronic payment solutions that can eliminate or reduce some of the problems they faced. Banks will have to determine what kind of electronic payments services best fit their customers' needs, and which could lead to smooth operating payment systems. There are also numerous problems in processing cash and cheques that electronic payments can eliminate. Both cash and cheques are labor-intensive – must be physically transported and counted, and risk loss or theft throughout their processing. We are convinced that many people are going to flock to electronic payments as it becomes easier to use. Because of its ease of use and familiarity, it has made it easy for consumers to focus on electronic bill payment in developed countries. If electronic payments can carry the broader

**REFERENCES**

Abor, J. (2004). Technological innovation and banking in Ghana: An evaluation of customers' perceptions, American Academy of Financial Management.

Agimo (2004).Better Practice Checklist for ePayment. Australia Government Information Management Office (online), available: http://www.agimo.gov.au/publications/2000/04/better_practice_checklist_for_epayment (2005-01-14).

Annon (1999). Survey of retail payment systems: Consumer payment options grow. ABI/INFORM Global, p. 4A-13A.

Balachandher, K. G., Santha, V., Norazlin, I. and Prasad, R. (2001). Electronic banking in Malaysia: a note on evolution of services and consumer reactions. *Journal of Internet Banking and Commerce*, vol. 5, no. 1.

Chorafas, D. S. (1988).Implementing networks in banking and financial services. Macmillan, Houndmills, 242 s.

Costello, D (2003). Mobility and micropayment (online) June, Zafion, available: http://www.epays.com/downloads/zafion_WP.pdf (2005-03-24).

Ferguson, J. W. (2000). Electronic commerce, bank and payments, 36th Annual Conference on Bank Structure Competition, Chicago.

Humphrey, D. B. and Hancock, D. (1997). Payment transactions, instruments, and systems: A survey. Journal of Banking and Finance 21, p. 1573-1624.

Humphrey, D. B., Kim, M. and Vale, B. (2001). Realizing the gains from electronic payments: cost, pricing, and payment choice. *Journal of Money, Credit, and Banking*, vol. 33, No. 2, pp. 216-234.

Kalakota, R., and Whinston, A. B. (1997). Electronic commerce: A manager's guide, Reading, MA: Addison Wesley Longman.

Kwast, M. and Kennickell, A. (1997). Who uses electronic banking? Results from the 1995

Leow, H. B. (1999). New distribution channels in banking services. *Banker's Journal Malaysia*, no.110, p. 48-56.

Mantel, B. (2000). Why do consumers pay bills electronically? An empirical analysis.

Economic Perspectives, Federal Reserve Bank of Chicago, Iss. Q IV, p. 32-48.

Pariwat, S. and Hataiseree, R. (2004). The use of cash, cheques and electronic payment services in Thailand: Changes and challenges for efficiency enhancement. Working paper, Payment systems Groups. (p.2-73).

Pierce, Michael. (2001). Payment mechanism designed for the Internet (online), available: http://ganges.cs.tcd.ie/mepeirce/Project/oninternet.html (2004-12-11).

Robinson, P. &Flatraaker, D. (1995). Income, costs, and pricing in the payment system, Norway Bank Economic Bulletin 66, p. 321-332.

Rose, P. S. (1999). Commercial banking management, 4ed., Irwin/McGraw-Hill, Boston

Sarpong, S. (2003). Banking system fails the test. (online), available: http://africa.peacelink.org/newsfromafrica/articles/art_781.html (04-12-15).

Smart Card Basics (2004). Smart card overview (online), available: http://www.smartcardbasics.com/overview.html (2005-02-02).

The Banker (2004). Will mobile get moving? (online), available: http://www.thebanker.com/news/fullstory.php/aid/2346/Will_mobile_get_moving_ht...(2005-02-22).

Zika, J. (2005). Retail electronic money and prepaid payment instruments, Institute of Economic Studies, Charles University in Prague, Prague

## PROFILES OF TECHNICAL AUTHORS

**Survivability in E-Payment Systems: A Holistic Approach** – G.M.M. Obi

**A Model of a Pragmatic Secure e-Payment System** – G.M.M. Obi

**Dr. Gabriel M. M. Obi** is a 1969 Ist Class honours graduate of Mathematics of the University of Ibadan, Nigeria. He also holds a Masters Degree in Computer Science of Oregon State University, Corvallis, Oregon, a Masters Degree and a Doctorate Degree, both in Mathematics, of Cornell University Ithaca, NY 1973 and 1974 respectively. He was at various times between 1970 and 2000, a lecturer (1970) then a Senior Lecturer (1978) in Mathematics and Computer Science at the University of Benin, Benin City Nigeria , Controller Data Processing at Ibru Organization, Lagos Nigeria (1985), and Deputy General Manager/Head of the IT Division of the First Bank of Nigeria (1998). His higher degrees were obtained while he was on study leave from the University of Benin. He is currently the Lead Research consultant at the International Business Systems Limited Lagos. He has several publications to his credit with the current research interests being IT Governance and IT security (Distributed Cryptography and Systems survivability). A Fellow of the Nigeria Computer Society and Chartered as a Fellow of the IT Profession by the Computer Professionals (Registration Council of Nigeria), Dr Obi is a Past Registrar/Secretary to Council, a Past President of the aforementioned Council, a recipient of the Best Paper Award of the Nigeria Computer Society National Conference 2001, and the Award of Professional Excellence of the Association of Professional Bodies of Nigeria 2011.

---

**Addressing Privacy in Online Banking and Transactions in Nigeria's Cashless Society –** B.K. Olorisade

**A Privacy Control Option For Call Centers In Nigeria's Cashless Economy –** B.K. Olorisade

**OLORISADE Babatunde Kazeem,** an Assistant Lecturer at Fountain University, Osogbo. He is currently pursuing PhD studies in Empirical Software Engineering at the University of Ibadan. He had M.Sc (double) degree in Software Engineering from the Universidad Politécnica de Madrid (UPM), Spain and Blekinge Tekniska Högskola (BTH), Sweden. He was sponsored for the master program under the prestigious Erasmus Mundus Scholarship scheme financed by the European Commission. He had first degree in Computer Science from Nigeria's premier university – University of Ibadan. His areas of research interest are: Software Quality, Software Measurement, Process Improvement, Cloud computing, ICT4D and internet applications.

---

**Users' Password Selection And Management Methods: Implications For Nigeria's Cashless Society –** A.S. Sodiya PhD

**SODIYA Adesina Simon,** Ph.D, Department of Computer Science University of Agriculture, Abeokuta, Ogun state, Nigeria.
Sodiya at present is working oncyber security planning and management, adaptive IRS, hierarchical access control architecture, authentication systems and generally improving the security of enterprise network. He is also a member of Computer Professional (Registration council) of Nigeria (CPN) and International Institute of Electrical and Electronic Engineering (IEEE). Sodiya has published in both international and local journals.

**Secured Banking By Automated Signature Verification and Face Recognition – T.S. Ibiyemi PhD**

**Development of Iris And Fingerprint Biometric Authenticated Smart ATM Device and Card – T.S. Ibiyemi PhD**

**Professor IBIYEMI T.S**. obtained Ph.D degree in 1982 from University of Bradford, Bradford, UK. He is a full Professor of Electrical Engineering (Information Technology & Automation) at Department of Electrical and Electronics Engineering, University of Ilorin, Ilorin, Nigeria. His research interest is principally in biometrics signal processing, and embedded system development.

---

**Trusted Cashless Cloud: A Flexible Approach For The New Cashless Society – Engr. Dr. M.C. Ndinechi**

**Engr. Dr. Michael C. NDINECHI** is the Director and Chief Executive of the *Electronics Development Institute (ELDI), Awka*, Anambra State. He holds the *B .ENG degree (Second Class Honours Upper Division)* from the Federal University of Technology, Owerri and M.Sc degree of the same University in 1988 and 1991 respectively. In 1995, he obtained the University of Greenwich London postgraduate certificate in *Data Communications.* He obtained his Ph.D degree in 2008 from the Federal University of Technology, Owerri where he specialized in *Communications Engineering*.

His working career started at the Federal University of Technology, Owerri where he rose to the position of Associate Dean of Engineering Faculty and was promoted to the rank of *Associate Professor of Electrical and Electronics Engineer* in 2009 with more than 30 journal publications and conference proceedings.

He is a Registered Engineer with the *Council for the Regulation of Engineering in Nigeria COREN* and a corporate member of the Nigerian Society of Engineers (NSE). He is a member of Institute of Electrical and Electronics Engineers (IEEE), Member Communications Society of the Institute of Electrical and Electronics Engineers (IEEE), Member Nigerian Institute of Management (NIM). His research interest is energy conservation and embedded systems programming.

---

**Retail Electronic Banking Quality (EBQ) In Nigeria: A Performance Evaluation** – DAVID-WEST Olayinka

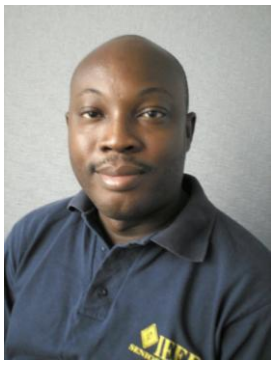
Dr. Olayinka **David-West**, a senior lecturer of Information Systems at Lagos Business School, Pan-African University, has over 20 years experience in the IT industry. She recently completed a doctorate in business administration (DBA) at Manchester Business School, University of Manchester; she holds an MSc in Business Systems Analysis and Design from City University, London; and a BSc in Computer Science from the University of Lagos.

In addition to systems development practices, Olayinka's research interests span the adoption of information systems in business. She has presented papers in local and international conferences and has authored numerous teaching case studies. She combines her teaching and research interests with industry consulting engagements in the areas of Strategic IS Planning, IT Personnel Selection, IT Assessment & Review/Due Diligence, E-Business, Business Planning, Software Selection & Management, Systems Implementation, Project & Change Management, Process Improvement and Systems Design. Her research interests include information systems in organisations, performance of e-business, electronic service quality and IT governance.

Olayinka is also the academic director at the Enterprise Development Services (EDS) Centre of Pan-African University and academic advocate to the Information Systems Audit and Control Association

(ISACA). She is a Certified Information Systems Auditor (CISA) and Certified in the Governance of Enterprise IT (CGEIT).

---



**Open Source Entrepreneurship in a Cashless Society** – Seyi Osunade

**Seyi OSUNADE** is a senior lecturer in the Department of Computer Science, University of Ibadan, Nigeria. He is a computer engineer and instructor with research interests in data communication systems, mobile agent technology, computer networks, computer education and open source software. Seyi obtained his bachelor's degree in computer engineering and masters in computer science from Obafemi Awolowo University, Ile-Ife, Nigeria. He obtained his doctoral degree from University of Ibadan, Nigeria. He worked as a graduate assistant at Obafemi Awolowo University, Ile-Ife before joining the University of Ibadan as an Assistant Lecturer. Dr Osunade has numerous publications in local and international journals. At the University of Ibadan, he was the Assistant Director, Management Information Systems (MIS) unit and currently the Sub-Dean(Physical – Undergraduate) of the Faculty of Science. He is a Member of the Nigerian Computer Society and member of the Computer Professionals Registration Council of Nigeria. He is married and has children.

---

**An Exploratory study on Electronic Retail Payment Systems: User Acceptability and Payment Problems in Nigeria –** G.O. Ogunleye

**OGUNLEYE, Gabriel Opeyemi** is a Lecturer in the Department of Mathematical Sciences (Computer Science Programme), Redeemer's University, Mowe, Ogun State, Nigeria. He holds B.Tech in Computer Science from Ladoke Akintola University of Technology, Ogbomoso, Oyo State, Nigeria; M.Tech Computer Science from Federal University of Technology, Akure, Ondo State, Nigeria. His research area includes Knowledge Management, Distributed System, Computer Security and Operating System. He is a member of Nigeria Computer Society. He has published papers in reputable international and local journals.

---

**A Flexible Envelope System For Tracking And Reporting Overspending In Cashless Transactions** – O.B. Olumide
**Understanding Financial Container Vulnerability Paradox In A Cashless Society Using The Cyber Crime Theory Of Pseudo-Ownership** – O.B. Longe

**Dr. LONGE Olumide** is on Faculty at the Department of Computer Science, University of Ibadan, Nigeria. His research has focused on using social theories and computer security theories to explain causastion and apprehension of cyber crimes. He is currently a Fulbright Fellow at the International Centre for Information Technology & Development, College of Business, Southern University' , Baton Rouge, LA, USA

---

**Survivability in E-Payment Systems: A Holistic Approach** – O.O. Dawodu

**Oladotun O Dawodu** is a Computer Analyst with the Forestry Research Institute of Nigeria, Ibadan. She holds a Bachelor of Science (Honours) Degree in Computer & Electronic Engineering, of the Lagos State University, Lagos Nigeria, (2007) and is currently pursuing a Masters degree programme in Computer Science at the University of Ibadan, Nigeria. Her research interest is in the survivability of e-payment systems. She is a member of the Nigeria Computer Society and is Chartered as an Associate member of the IT Profession by the Computer Professionals (Registration Council of Nigeria).

**A Model of a Pragmatic Secure e-Payment System** – E.E. Odokuma

**ODOKUMA Elizabeth** heads the Information Technology Department at Biotic Technology & Consulting Services, Port Harcourt, Nigeria. She holds a Bachelor of Science (Honours) Degree in Computer Science (1996) and a Masters Degree in the same discipline and from the same University in 2007. She is currently pursuing a Computer Science Ph.D programme at the University of Port Harcourt, Nigeria. Her current research interests include requirements engineering, trust and privacy preserving systems and electronic payment systems. She is a Microsoft Certified Professional, a member of the Institute of Electrical and Electronics Engineers (IEEE), the Nigeria Computer Society (NCS) and is chartered as a Member of the IT Profession by the Computer Professionals (Registration Council of Nigeria)


cpn

NATIONAL INFORMATION TECHNOLOGY DEVELOPMENT AGENCY
NITDA

ISPON
INSTITUTE OF SOFTWARE PRACTITIONERS OF NIGERIA

ITAN
NIGERIA
Information
Technology
Association
of Nigeria