e-Government 2013

nigeria computer society
www.ncs.org.ng

# Conference Proceedings

Theme>>

# e-Government & National Security

<Edited By>

Professor Charles O. UWADIA,
Professor Adesola ADEROUNMU, Dr. Adesina SODIYA

ISSN: 2141-9663

## FOREWARD

It is my great pleasure and delight to welcome all of us to the 11th International conference on e-Government and National Security which is holding at Iloko-Ijesa, Osun state, Nigeria from July 24 to 26, 2013. A total of 18 well-written and peer-reviewed papers have been slated for presentation at different sessions of the conference.

The programme for the conference has been threaded into 5 plenary sessions and 6 parallel sessions. Plenary sessions 1 and 2 focused more on issues relating to e-Government and National security. Session 3 incorporates a workshop on Public Key Infrastructure (PKI) which is a set of hardware, software, people, policies, and procedures needed to create, manage, distribute, use, store, and revoke digital certificates. The Minister of Communication Technology, Mrs Omobola Johnson will give the keynote address which is the focus in session 4. In plenary session 5, the workshop on introduction to computer forensic will be anchored by Professor Zacharian Tanko from Champlain College, Burlington, VT, United State of America. Parallel sessions 1 and 4 concerns governance through e-Government, Smart Government and Social Security, while parallel sessions 2 and 5 focused more on economic security, political security, and National database. As usual, the fourth edition of the Research Consortium on Information Technology Innovations **(RECITI 2013)** will provide an avenue for researchers to showcase their on-going research, hence parallel sessions 3 and 6 showcase on-going research in field of information and communication technology.

There would be lead paper presentation by eminent researchers and practitioners in the field which include the CTO and Vice President SWG, Africa and Middle East, IBM Software Group, Mr Ajamu Wesley, Dr. Adetoye Adedayo, Cyber Security Centre, University of Oxford, UK, Zachariah Tanko (Associate Professor), Champain College, Burlington, VT, USA, and Tope Aladenusi, Head, Information and Technology Risk, Akintola Williams Deloitte. Others are the CEO, Development Information Network, Mr Bankole Olubamise, Mr. Femi Williams, Deputy Managing Director, Chams Plc, Mr. Ayanda Dlamini, Business Development manager, LGR Telecommunication (Pty) Ltd., and Patience Akpan-Obong (Associate Professor), Arizona State University, USA.

Let me use this opportunity to express my appreciations to all spirited individuals, our collaborating partners, sponsors, and all those who have generously sponsored this year's conference. It is my prayer that together, we will move this country to a greater height. Finally, I wish to thank those that worked assiduously to make today a reality, Our President, Sir Demola Aladeokomo FNCS, members of the National Executive Council, Provost COF, Fellows of the society, conferences committee members, members of the State of Osun chapter of NCS and the local organizing committee for their commitment and dedication towards the success of this conference. I say a very big thank you to the secretariat staff.

**Professor Sola ADEROUNMU (FNCS)**
Chairman Conferences.

Full Paper

# A CLOUD-BASED PASSWORD MANAGER FOR MULTIPLE TRANSACTION ACCOUNTS

**D.O. Aborisade**
Department of Computer Science
Federal University of Agriculture, Abeokuta (FUNAAB), Nigeria
*aborisadeda@funaab.edu.ng*

**O.Y. Alowosile**
Department of Computer Science
Abraham Adesanya Polytechnic, Ijebu-Igbo, Nigeria

**K.O. Odunlami**
Department of Computer Science
Federal University of Agriculture, Abeokuta (FUNAAB), Nigeria

**A. Odumosu**
Department of Computer Science
Abraham Adesanya Polytechnic, Ijebu-Igbo, Nigeria

## ABSTRACT

*The emergence of Internet Technologies obviously has brought about several online transaction systems requiring authentication. These transaction systems require their users to supply access code (password) to authenticate them for any transaction to take place. Consequently, a number of password managers have been proposed and designed to assist users recollect their several passwords for transactions. Most users of online transaction systems keep many account passwords that must not be recorded and forgotten, but which they often find difficult. Hence, they are faced with the challenges of effectively managing their ever growing passwords for transacting on their systems. The existing password managers have been helpful mostly in the area of helping users recollect forgotten password on a particular account (platform) at a time, but not on multiple accounts (platforms). In this paper, an architectural framework for password manager on multiple accounts (platforms) was proposed and implemented. The architecture is composed of three modules namely login and account module, security module and the authentication module. The architectural design was implemented and tested with hundred networked systems. The results of implementation show that the proposed password system is effective and capable of assisting users easily recollect any of their multiple passwords for a particular transaction.*

**Keywords:** *Passcode management, Passcode security, Secured multiple accounts, Internet Technologies*

## 1. INTRODUCTION

A password is a string of characters used to login to a computer and other systems for files access, program access, and other resources (Melanie, 2012). They are used to ensure that people do not access any system unless they are authorized to do so (Melanie, 2012). Despite the argument by notable security researchers that the use of passwords as authentication method is vulnerable and characterized by security and usability drawback, it has continued to maintain its position as first line of system defense in every facet of our lives such as in home systems, office systems, to financial transactions systems. The reason for this is because of its incumbency, familiarity, and low cost. The number of passwords users use on their transaction systems in recent times has been on the increase (McCarney etal, 2012). Such systems are often found in online banking, web mail sites, and social media sites e.t.c. For example, it has been generally noted that an average Nigerian keeps about seven (7) to ten (10) passwords for their different systems at home, offices and for their financial transactions. This means that at every point in time, they are confronted with the problem of memorizing and recollecting all their unique passwords for the systems on which they want to transact at a particular time.

It has been observed that as the number of these passwords increase, users find it more difficult to recollect the appropriate password for a particular transaction at a particular time, hence, the need for this paper. Password managers are designed to relieve password fatigue and reduce login time (McCarney etal, 2012). They can also indirectly facilitate better password quality and a reduction in password reuse. There are three major classifications of password managers. These include Saving Logins in Your Browser (i.e IE, Firefox), Web-Based Password Managers (i.e Lastpass and Robofor) and Local (Desktop) Managers (i.e Keypass)(Melanie, 2012). Password managers have certain drawbacks. To use a password manager, existing accounts must be migrated into the manager and potentially replicated across multiple devices (McCarney etal, 2012). Major research efforts in this area have been found to include password managers, strengthening password quality and the use of alternative authentication mechanisms into passwords (i.e. graphical or object-based passwords). In this paper, we focus on developing a password manager for multiple accounts password. The remaining section is organized as follows; section 2 reviews a number of relevant literatures on password manager section 3 describes the methodology for the proposed system while section 4 and 5 describe the results and concludes the work respectively.

## 2. RELATED WORK

The proliferation and popularity of password as the commonest method of authenticating users to enhance security has attracted attentions of many researchers. A number of such relevant researches were reviewed in this paper. (Tam et al., 2010) examined five (5) password-management behaviours with the intention of investigating users knowledge of password quality, users motivation for password selection, and the effect of account type on password management behaviours. Their results showed that users understand the difference between good and bad passwords and their resulting consequences. They also found that the motives behind password selection and password behaviours are complex. Their research contribution provided a new way of looking at password management behaviour. (Tam et al., 2010) used Construal Level Theory to discover that trade-offs between security and convenience as an important determinant of password quality. They showed that this tradeoff could be positively influenced by imposing a time-frame factor. Their research efforts clearly provided a first step towards improving password management behavior, they however did not solve problem of managing multiple passwords that most users have.

Security threats that such approaches must address, known attacks, and methodological issues related to empirical evaluation were also discussed. Although further research and improved methodology were also identified this did not include multiple password scenario. (Boyen, 2007) revisited the venerable question of "pure password"-based key derivation and encryption, and expose security weaknesses in current implementations that stem from structural flaws in Key Derivation Functions (KDF). In this work, they advocated for a fresh redesign, named Halting KDF (HKDF), which was thoroughly motivated on the following grounds:

i. By letting password owners choose the hash iteration count, they gained operational flexibility and eliminate the rapid obsolescence faced by many existing schemes.
ii. By throwing a Halting-Problem wrench in the works of guessing that iteration count, they widened the security gap with any attacker to its theoretical optimum.
iii. By parallelizing the key derivation, they allowed legitimate users exploit all the computational power they can muster, which in turn further raises the bar for attackers.

(Boyen, 2007) submitted that HKDFs are practical and universal because they work with any password, any hardware, and a minor change to the user interface. As a demonstration (Boyen, 2007) offered real-world implementation for the a password generating object from their local collection or from the web, and then converts the password object (e.g. an image, a particular piece of music, excerpt from a book) to a (potentially) high-entropy text password that can be used for regular or secondary web authentication, or in local applications (e.g. encryption). Instead of requiring users to memorize an exact password, ObPwd only requires one to remember a hint or pointer to the password object used.

They implemented a prototype, and solicit feedback from the research community in regard to using digital objects as passwords (Mannan and Van Oorschot, 2008). (Sreelatha and Shashi, 2011) proposed user authentication using native language passwords was proposed whereby a user is expected to select a character from his native language and also submits the shape of that character in a grid when creating the password so that the user can be correctly authenticated using these information when there is need to login. This idea is based on their belief that users can remember their native language passwords better than passwords is any other language (Sreelatha and Shashi, 2011). The proposed scheme is found to be resistant to eavesdropping, brute-force attack, shoulder surfing and hidden camera. The research observation shows that although users are able to remember their character, they always find it difficult to remember the password shape. Another drawback observed is that password registration and login takes time in the proposed scheme. (Ross et al., 2005) described a simple browser extension called PwdHash, that transparently produces a different password for each site, improving web password security and defending against password phishing and other attacks.

Since the browser extension applies a cryptographic hash function to a combination of the plaintext password entered by the user, data associated with the web site, and (optionally) a private salt stored on the client machine, theft of the password received at one site will not yield a password that is useful at another site. While the scheme requires no changes on the server side, implementing this password method securely and transparently in a web browser extension turns out to be quite difficult. They describe the challenges faced in implementing PwdHash and some techniques that may be useful to anyone facing similar security issues in a browser environment (Ross et al., 2005). (Yee and Sitaker, 2006) described Passpet as a tool that improves both the convenience and security of website logins through a combination of techniques.

They reported that Password hashing helps users manage multiple accounts by turning a single memorized password into a different password for each account. They proposed new improvements to these techniques, discussed how they are integrated into a single tool, and compare Passpet to other solutions for managing passwords and preventing phishing. (Thomas, 2012) introduced Enterprise Random Password Manager (ERPM) which was designed to deal with the problem of privileged password management in cross-platform enterprise environments. In ERPM, when a user needs to login, he or she logs on to the ERPM web console and requests a password for the account. Depending on how the EPRM is configured, the request might be approved automatically, or the user might need to wait for approval. Either way, when the request is approved, ERPM will issue the user a complex temporary password for the account. This password can be displayed on the screen, sent through email, or transmitted though a text message. ERPM ensures that the password has been synchronized on the related system before issuing it to the user. Unlike typical administrator passwords, this password is valid for a limited time only, before it expires and the password is reset.

Administrators also have the option of checking in a password, at which point the password will be reset ahead of schedule. (Bonneau et al., 2012) evaluated two decades of proposals to replace text passwords for general-purpose user authentication on the web using a broad set of twenty-five usability, deployability and security benefits that an ideal scheme might provide. The scope of proposals surveyed was also extensive, including password management software, federated login protocols, graphical password schemes, cognitive authentication schemes, one-time passwords, hardware tokens, phone-aided schemes and biometrics. Their comprehensive approach led to key insights about the difficulty of replacing passwords. They concluded that many academic proposals have failed to gain attraction because researchers rarely consider a sufficiently wide range of real-world constraints. Beyond the analysis of current schemes, their framework provided an evaluation methodology and benchmark for future web authentication proposals (Bonneau et al., 2012).

## 3. METHODOLOGY

### 3.1 Proposed Architectural Framework Design

The Architectural framework for the password manager proposed in this paper as described in Figure 1 is designed based on the text-based password authentication scheme. According to the figure, the architectural framework is divided into three major modules, namely; user's accounts and login module, the security module and the authentication module.

User's accounts and login module: This module depicts all users activities involving attempts to gain access to the password manager, supply of minimum number account owned by the user and culminating in the display of all the accounts owned by the user. In this module the user loads the password manager, create accounts and supply minimum information about the accounts owned by him/her. Then the system displays all the accounts owned by the user.

Security module: This module is the second module in the architecture. It consists of the integrated database (Security Level 1) and the cloud database (Security Level 2). It is the engine house of the password manager because it houses all the repositories of various accounts passwords and passcode information and helps to secure these information. It is called the security module because it provides two levels of security for the passwords in a manner that all users accounts passwords are encrypted and stored in Level 1 and each time any of these passwords are changed, a copy of all these passwords is made in the cloud database to ensure their security. This is the reason why it is called the second level of security for the passwords.

Authentication module: This is the module where a particular user account password meant for a particular transaction at a time is located, compared with the copy in the cloud database before it is authenticated for the transaction to take place.

### 3.2 Methodology for System Operational Design at Interface Level

With the proposed password manager system S running and invoked through the user login, the system demands for the password for the desired transaction accounts. Two assumptions are made at this point. First, it is assumed the user has forgotten his password for transacting on that account. It is also assumed that the user would be able to remember at least one or two of his/her several transaction account names. Therefore, the user is expected to supply at least one of his multiple transaction account name. When the account name is supplied, the proposed password manager system displays all the names of all the transaction accounts owned by the user. With this, the user is reminded of all his/her account names. The user would then be expected to select the name of the transaction account on which he intends to transact at that particular time. Once this is done, the password manager system automatically generates the password meant for that particular account chosen by the user for instant transaction to take place. In case the transaction account password is changed, the password manager system facilitates the transfer and replacement of the new password as encrypted data between the Level 1 security (local integrated database) and the Level 2 (cloud database).

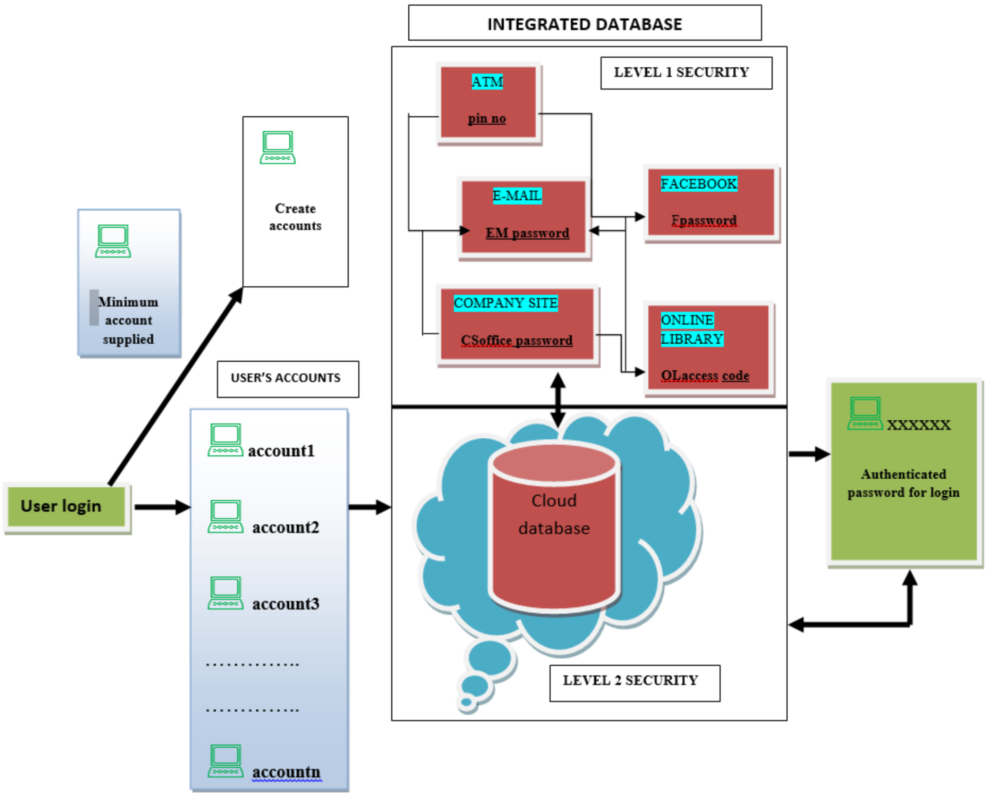


*Figure 1: Architectural framework for the proposed Password Manager System*

### 3.3 Methodology for the proposed System at Operational Level

At operational level of the proposed password management system *S*, every user is made to have a **name code** and for every **transaction account** created by the user a passcode is given called **acct code** so that when a user is creating a new transaction account the system allows him to supply his name (**name code**) and a pin code (called the **actual code**) among other information like his/her saddest moment. Let the password structure be defined as **αβPwd** where **α = name code** (as unique and known to all transaction accounts ($T_A$ ) in the system, **β = acct code** is the unique code that is created and assigned to a particular transaction account ($T_A$)), and **Pwd =** is the actual code (password) created by the user for a particular transaction account such that

**workingcode=** $\prod_{\square\square\ \square}^{\square}$ **$\alpha_i\beta_i Pwd_i$ .......**equation (1)

where n= number of passwords owned by the user and there exists a symmetric relationship between passwords in the integrated database and the cloud database as defined by

**($\alpha_i\beta_i Pwd_{iLevel1}$) Ɽ ($\alpha_i\beta_i Pwd_{iLevel2}$) if ($\alpha_i\beta_i Pwd_{iLevel2}$, $\alpha_i\beta_i Pwd_{iLevel1}$) ϵ Ɽ** for **all $\alpha_i\beta_i Pwd_{iLevel2}$, $\alpha_i\beta_i Pwd_{iLevel1}$ ϵ Level1 and Level2** such that **$f^{-1}$((exC$_i\alpha_i\beta_i$Pwd$_i$)$_{Level2}$))** $_=$ **(exC$_i\alpha_i\beta_i$Pwd$_i$)$_{Level1}$.** and **exC** stands for extra code for login. The system is designed in such a way that when a user creates a transaction account, he is asked to supply a number of other information including information about the user "most unhappy moment". To use the password manager system, the user is expected to supply the name of any of his transaction accounts he could recollect and information about his most unhappy moment" as supplied when creating the account. At the time the transaction account is being created, the system generates a **name code** and **acct code** for the account name and account code respectively and attach to **password (actual code)** supplied by the user to form the **working code**. These are encrypted and stored in the integrated local database (Level 1 security). A copy of this is immediately made on cloud database (Level 2 security) associated with the local integrated database. In the same manner, the date value supplied by the user as his most unhappy moment is evaluated using a Hash function technique and copied on the cloud database.

Whenever a user forgets his password for any of his transaction accounts, the only thing he has to do is to select the option for the transaction of choice at the time and supply correct date value for his most unhappy moment. Once these are correctly supplied, and because his **name code** is made unique and known to all his transaction accounts while his **acct code** is unique to every transaction account he keeps and these two code are embedded in the **working code** the account name supplied by the user is compared with the working code encrypted in the database and the hash values for the transaction account is reverted from the cloud database and also compared with the most unhappy value for a match, once they match, the user required password is auto-generated and authenticated for the transaction to take place.

### 3.4 The proposed system as a Decision Tree

To show that the proposed system *S* is capable of effectively generating the password for the desired transaction at a particular time, decision tree is used to model the system. To do this, we have to first establish that if the proposed system S with *m-ary* structure of height *h* has *l* $T_A$, then *h* ≥ Ɔlog$_m$ *l*Ƈ and also establish that if the system *m-ary* tree is full and balanced, then h= Ɔlog$_m$ *l*.Ƈ . Taking logarithms to the base m shows that log$_m$ *l* ≤ *h* because h is an integer, we have *h* ≥ Ɔlog$_m$ *l*Ƈ. Now suppose that the system is balanced. Then each $T_A$ is at level h or h-1, and because the height is h, there is at least one $T_A$ at level i. It follows that there must be more than $m^{h-1}$ leaves ($T_A$). Because $l \leq m^h$, we have $m^{h-1} < l \leq m^h$. Taking logarithms to the base m in this inequality gives $h\text{-}1 < log_m\ l \leq h$. Hence, *h* = Ɔlog$_m$ *l*Ƈ. Suppose there are nine (9) transaction accounts with the same degree of probability for selection as a desired transaction account to make a total of ten transaction accounts. To determine which of the transaction accounts is to be selected at a time, we need to determine the number of comparisons that are necessary using the proposed system. Since, there are ten transaction accounts of the same probability for selection. There are three (3) possibilities for each comparison of two password at a time namely; two passwords are right or the first password is right while the second password is wrong or the first password is wrong while the second password is right. Therefore, the proposed system *S* adequately models the decision tree for the sequence of comparisons is a *3-ary* tree. Therefore, there are at least ten leaves ($T_A$) in the in the system *S* because there are ten possible outcomes (because each of the ten $T_A$ 's can be selected and each possible outcome must be represented by at least one $T_A$. The largest number of comparisons needed to determine the right password for transaction is the height of the decision tree (*S*) as represented in Figure 2. From (Alberto et al., 2002) , it follows that the height of the decision tree ( ie. *S*) is at least Ɔlog$_3$ 10Ƈ=3. Hence, at least three (3) are needed to select the right transaction password in the proposed system S.

## 4. VALIDITY PROOF FOR THE PROPOSED SYSTEM

### 4.1 Mathematical Induction step of Proof

To prove the validity of the proposed system S, it is modeled with a rooted tree so that it can shown that it is balanced if all its transaction accounts $T_A$ are at levels *h* or *h-1*. Since a rooted *m-ary* tree of height *h* is balanced if all it leaves are at levels *h* or *h-1*(Kenneth, 2007). To prove this, we need to prove that there at most $m^h$ transaction accounts $T_A$ in the proposed system S, using mathematical induction on height. First we consider a system S of height 1. This system consists of a root with no more than m children, each of which is a transaction. Hence, there are no more than $m^1$=*m* transactions in a system S of height 1. This is the basis step of the inductive argument. We then assume that the result is true for all systems (*m-ary* trees) of height less than *h*, this is the inductive hypothesis. Let S be an *m-ary* tree of height *h*. The transaction accounts $T_A$ of S are the $T_A$ of *subS* obtained by deleting the edges from the root to each of the vertices at Level 1 as shown in Figure 3. Each of these *subS* has height less than or equal *h-1*. So, by the inductive hypothesis, each of these rooted tree (system S) has at most $m^{h-1}$ transaction accounts $T_A$, because there are at most m such *subs*, each with a maximum of $m^{h-1}$ transaction accounts $T_{A,}$ there are at most $m.m^{h-1}$ = $m^h$ transaction accounts $T_A$.

### 4.2 Evaluation Results

The proposed password manager system design is implemented with Miscrosoft Visual C#.NET with Microsoft SQL Server and MongoDB as the back-end. The password manager system is deployed on one hundred (100) networked systems for 100 different users to test at the same. Each user is allowed to use ten (10) different transaction accounts for the test. Response from the users indicate that the proposed system is capable of using the password manager at the same time on the same network. Some of the sample implementation snapshots are as indicated in figure 4,5,6,7 and 8.

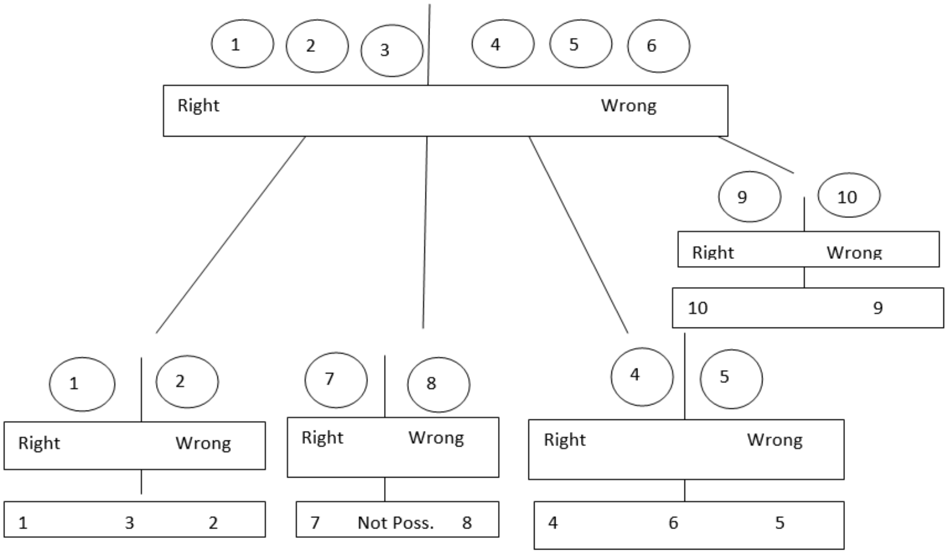


*Figure 2: A decision tree for generating the right password for transaction*

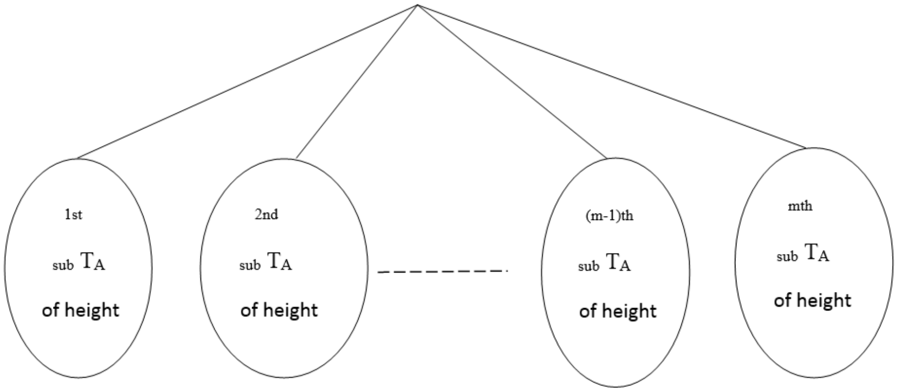
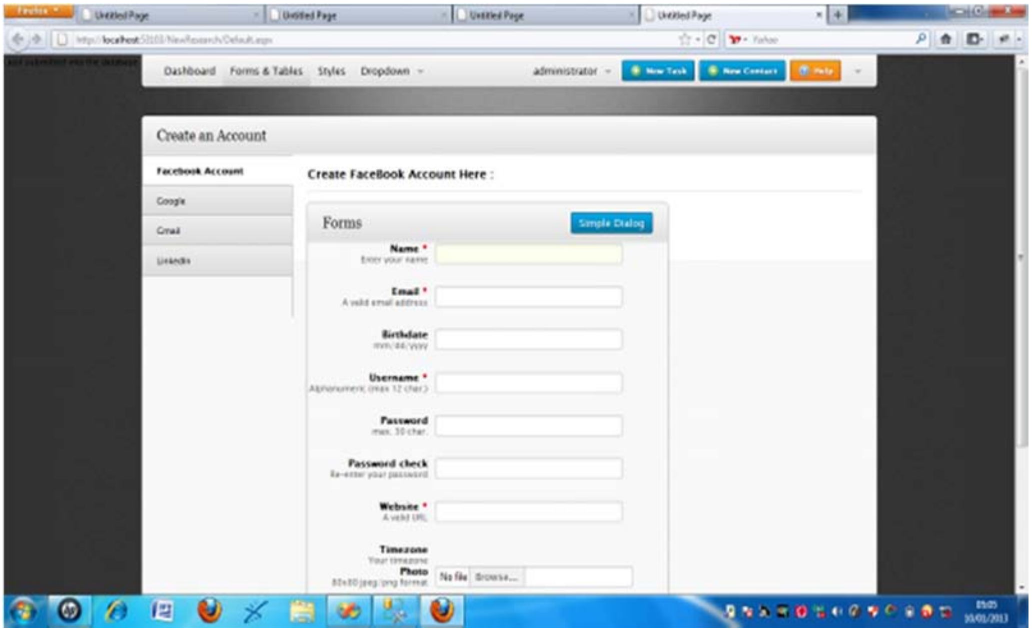


*Figure 3: Steps for the Inductive Proof*



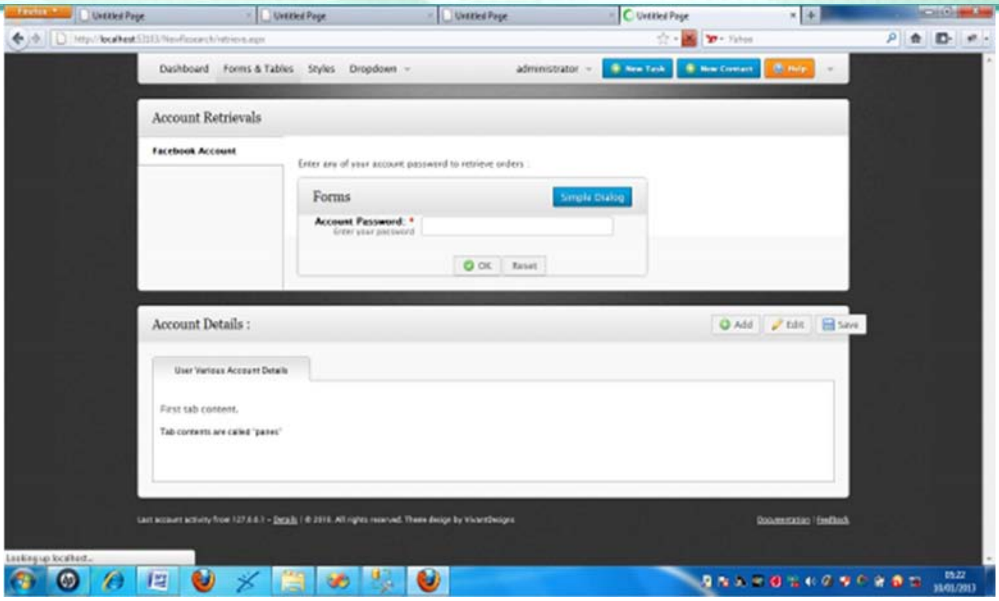
Create an Account

Create FaceBook Account Here :

Forms

| | |
|---|---|
| Name *<br>Enter your name | |
| Email *<br>A valid email address | |
| Birthdate<br>mm/dd/yyyy | |
| Username *<br>Alphanumeric (max 12 char.) | |
| Password<br>max. 30 char. | |
| Password check<br>Re-enter your password | |
| Website *<br>A valid URL | |
| Timezone<br>Your timezone | |
| Photo<br>80x80 jpeg/png format | No file |

*Figure 4: Interface for password account in Facebook site*



Account Retrievals

Enter any of your account password to retrieve orders :

Account Password: *
Enter your password

Account Details :

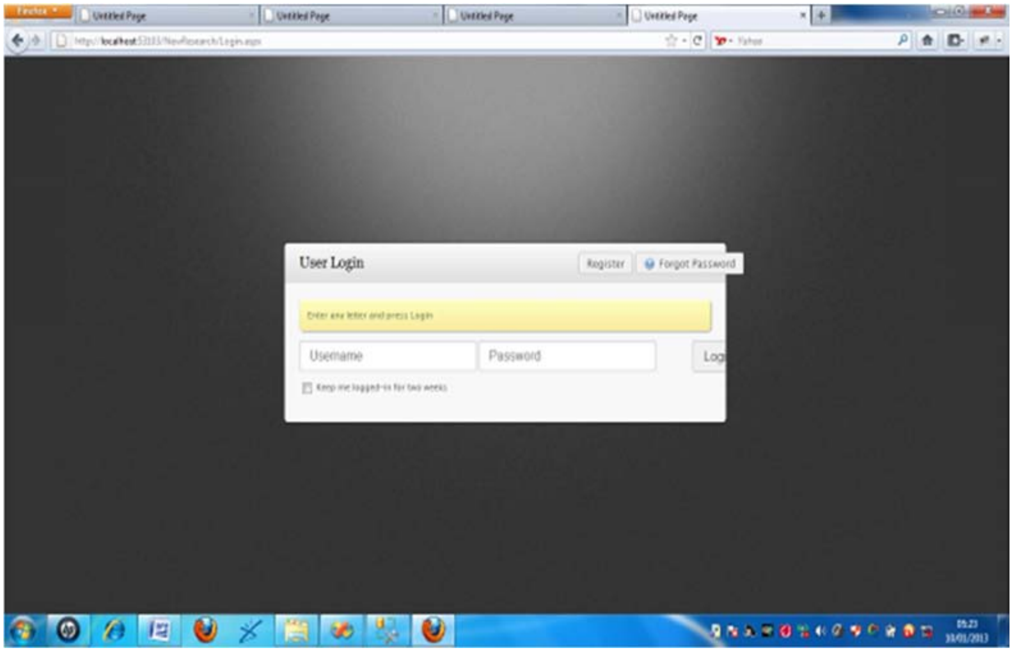
First tab content.

Tab contents are called "panes"

Last account activity from 127.0.0.1 - Details | © 2010. All rights reserved. Theme design by VivantDesigns

Looking up localhost...

Figure 5:  Interface for retrieving for password information in the system



User Login

Enter any letter and press Login

Username
Password

□ Keep me logged-in for two weeks

Figure 6: Interface for auto generate password for transaction

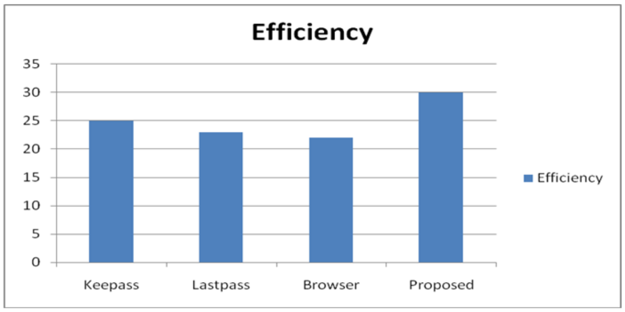


Figure 7: Graph Analysis of measure of systems efficiency

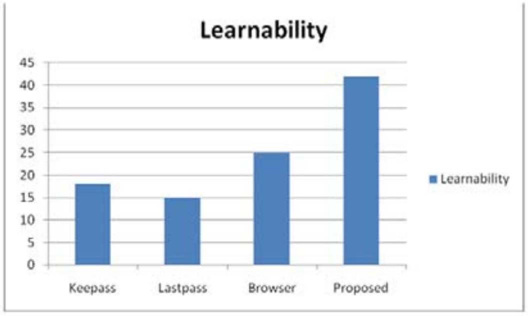


Figure 8: Graph Analysis of measure of systems Learnability

To evaluate the extent to which the proposed password manager system can be used by users to achieve specified goals, and since usability is associated with the measure of functionalities of a product, usability attributes like Learnability, Efficiency, Memorability, Errors, and Satisfaction (Alberto et al., 2002) information are obtained from 100 users. The information obtained from the users are represented in the Tables 1-5 and analyzed in figures 7, 8,9,10 and 11

*Table 1: User's measure of password managers in terms of their Efficiency*

| Usability Attribute | KeePass | Lastpass | Browser-based | Our Proposed System |
|---|---|---|---|---|
| Efficiency | 25 | 23 | 22 | 30 |

*Table 2: User's measure of password managers in terms of their Learnability*

| Usability Attribute | KeePass | Lastpass | Browser-based | Our Proposed System |
|---|---|---|---|---|
| Learnability | 18 | 15 | 25 | 42 |

*Table 3: User's measure of password managers in terms of their Learnability*

| Usability Attribute | KeePass | Lastpass | Browser-based | Our Proposed System |
|---|---|---|---|---|
| Memorability | 10 | 10 | 5 | 75 |

*Table 4: User's measure of password managers in terms of their Satisfaction*

| Usability Attribute | KeePass | Lastpass | Firefox | Our Proposed System |
|---|---|---|---|---|
| Satisfaction | 20 | 25 | 20 | 35 |

*Table 5: User's measure of password managers in terms of errors they contain*

| Usability Attribute | KeePass | Lastpass | Firefox | Our Proposed System |
|---|---|---|---|---|
| Errors | 25 | 60 | 10 | 5 |

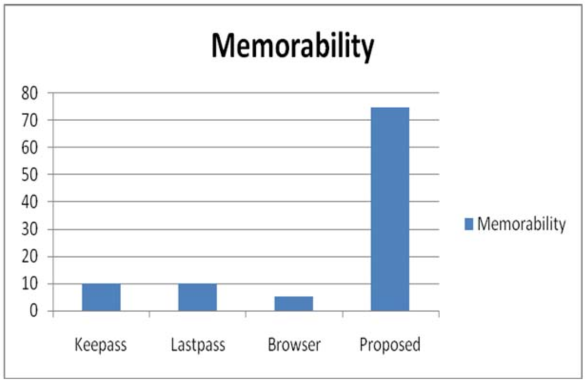


*Figure 9: Graph Analysis of measure of systems Memorability*

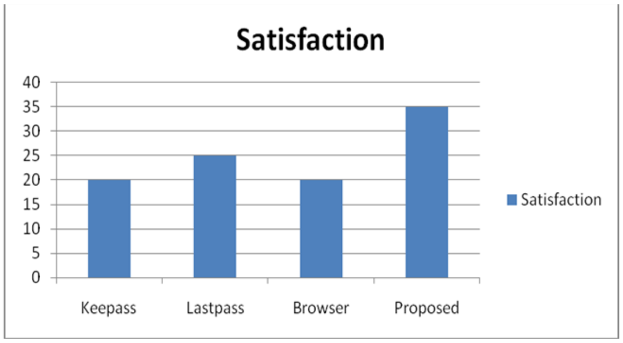


*Figure 10: Graph Analysis of measure of systems Satisfaction*

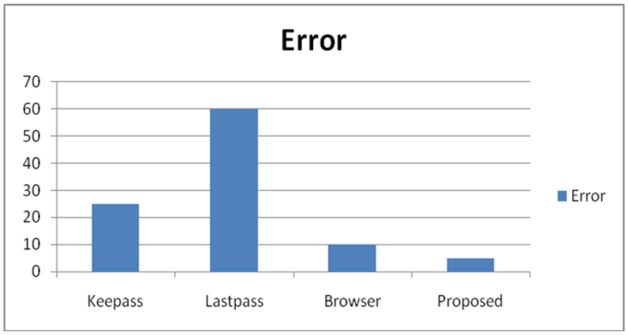


*Figure 11: Graph Analysis of measure of systems errors*

The foregoing data and analysis as obtained from 100 users during testing show that the proposed password manager system is highest in efficiency, learnability, memorability, and satisfaction but lowest in occurrence of error(s) when compared with other existing password managers.

## 5. CONCLUSION AND FUTURE WORK

The trend in every society of the World is fast moving towards a situation where the number of passwords that an average user has continue to increase on daily basis owing to their participation in transaction accounts ranging from online banking systems, web mail sites, to social media sites. Although a number of password managers already exist, the idea proposed in this paper is meant to bring to fore another unique perspective to the development of password manager. This paper presents a unique perspective to the development of password manager that affords a user to have automatic access to any of his passwords amongst several others across his multiple transaction accounts. The evaluation report of this research shows this proposed system promises to be the best password managers when implemented. Future research effort would be geared toward improving the system to handle up to about twenty (20) transaction accounts password.

## REFERENCES

Alberto A., Jan B., Avratoglou C., Robert C.,Xavier F. E., Natalia J., Jeff M., Stavros M., AnaM.P. 2002. STATUS: Software Architecture for Usability".Information Societies Technology (IST) Pprogramme. D.2. v.1.0 Usability Attributes affected by Software Architecture.

Biddle R., Chiason S., and Van OorschotB P.C. 2012. Graphical passwords: Learning from the first Twelve years. ACM Computing Surveys, 44(4):1–41, 2012.

Bonneau J., Herley C., Van Oorschot P.C., and Stajano F. 2012. The Quest to replace Passwords: A framework for Comparative Evaluation of Web Authentication Schemes.InIEEE Symposium on Security and Privacy.2012.

Boyen X. 2007. Halting Password Puzzles–Hard-to-break Encryption from Human- Memorable keys. In USENIX Security.

Kenneth H. R. 2007. Discrete Mathematics and Its Applications Sixth Edition. McGraw-HillInternationalEdition. Pages. 691-699.

McCarney D., Barrera D., Clark Chiasson S., Van Oorschot, P.C. 2012. Tapas: Design, Implementation,and Usability Evaluation of a Password Manager. ACSAC '12 Dec. 3-7, 2012, Orlando, Florida USA 2012 ACM 978-1-4503-1312-4/12/12.Pg. 9-98.

Mannan M., and Van Oorschot P.C. 2008. Digital Objects as Passwords. In HotSec.

Melanie P. 2012.Which Password Manager is the Most secure online:http:lifehacker.com.

Ross B., Jackson C., Miyake N., Boneh D., And MitchellJ.C. 2005.Stronger Password Authentication Using Browser Extensions. In USENIX Security, 2005.

Sreelatha M and Shashi M. 2011. User Authentication using Native Language Passwords.International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.6, November 2011, 149-160.

Tam L., Glassman M., and Vandenwauver M. 2010. The Psychology of Password Management: A tradeoff between Security and Convenience. Journal of Behaviour & Information Technology. Vol. 29, No. 3, May–June 2010, 233–244.

Thomas O. 2012. Enterprise Random Password Manager. Penton Media, Inc.Pg 55.

Yee K.P. and Sitaker K.. 2006. Passpet: Convenient Password Management and Phishing protection. In SOUPS.

Full Paper

# A COMBINED APPROACH TO SECURING INFORMATION USING STEGANOGRAPHY AND ASYMMETRIC CRYPTOGRAPHY

**Okure U. Obot**
Department of Computer Science
University of Uyo, Uyo
okureobot@uniuyo.edu.ng

**Mercy E. Edoho**
Department of Computer Science
University of Uyo, Uyo.
edohojnr@yahoo.com

**ABSTRACT**

The study describes a technique for integrating a simple steganography technique of hide and seek with asymmetric cryptography algorithm such as RSA into a hybrid system. The hide and seek method of hiding information in another information though simple and robust lacks adequate security since it works without a key making it prone to attack. On the other hand, an asymmetric cryptographic technique such as RSA works with both public and private keys generated by the potential receiver of a message to his sender. This feature gives such a system a high degree of invulnerability. These motivate the integration of the two methods within a hybrid system. The combination of the two techniques tends to minimize the limitations of individual method while enhancing their strengths. The study presents a framework of the combination whose implementation is bound to be very useful in information security in applications such as banking, government, commerce and their likes where some administrative documents categorized as 'classified' need to be properly secured against unauthorized access.

**Keywords:** *Steganography, Cryptography, LSB, RSA, Asymmetry.*

## 1. INTRODUCTION

Government establishments are daily challenged by leakages of information to the public at unusual time. Such leakages sometime pose great setbacks in the running of government programmes. Some documents marked 'classified' or 'confidential' are discussed in the public domain before they get to the people they were meant for. This becomes more challenging in electronic governance where despite its openness must of necessity still have classified or confidential documents in its websites. The issue of security of data and information in electronic governance is therefore of great concern to its practitioners.

The art of hiding a message in another message from its potential receiver until some manipulations are done to reveal it is referred to as steganography. Steganography is one of the measures taken to enhance security and integrity of data. It is a form of information hiding which encompasses other techniques such as watermarking and fingerprint. Messages could be hidden in various formats such as, text, images, audio, video and file protocol. In all these, the most suitable format is the format whose bits can be altered without the alteration being noticed or detected easily (redundant bit). Image and audio files have high degree of redundant bits, so are the most used formats in stegonagraphy. In image steganography a message is hidden in an image such as a picture that the potential receiver is known to be fond of.

The first requirement of a steganographic system is its undetectability. According to (Kharraze et al, 2004), a steganographic system is considered insecure if an intruder is able to differentiate between a cover object and a stego object. A cover object is an object used as the carrier to embed a message into, and a stego object is the object carrying a hidden message. A steganographer needs a cover object and a message to produce a stego object which carries the message. In encoding the message, the steganographer has to indentify the redundant bits of the cover object before a message is embedded into the cover object to form a stego object. During decoding, an estimate of the message must be obtained from the stego object. A key is needed by an intruder or potential user (receiver) of the message to unlock the stego object to obtain the message. The key is usually kept secret between the sender and the receiver of the message. The general model of a steganographic system is depicted in Figure 1.

The model shows that a steganographer needs a key, a message to be sent, a cover object and an algorithm to form a stego object. Some approaches using the LSB however can be operated without a key. This object is sent to an intended receiver who is expected to have a key to unlock the stego object using a decoding algorithm. In case an intruder gets hold of the stego object, all he needs is a key to unlock it and get the message. A stego object must therefore be constructed in such a way that it is difficult to manipulate a key to unlock it, it must also be constructed in such a way that it is difficult to differentiate it from the cover object. In an algorithm like the hide and seek algorithm which needs no key, an intruder needs to be able to manipulate the encoding and decoding algorithms in order to unlock the stego object.

The study is aimed at designing a system that keeps not only the existence of a message secret but also brings out a meaningless message to an intruder if he detects the existence ( a stego object) of the message and unlocks it. This is done by integrating the steganographic technique with an asymmetric cryptographic technique. The combination though more complex offers a better security approach to data. In (Obot et al, 2012) an enhanced Playfair cipher is proposed for data security and integrity while (Chandrammouli and Memon, 2001) analysed LSB based image steganography techniques, (Chandrammouli et al, 2003) discussed the concepts and practice of image steganography and steganalysis, and in (Moulin and Mihcak, 2004) a framework for evaluating the data-hiding capacity of image sources is presented.

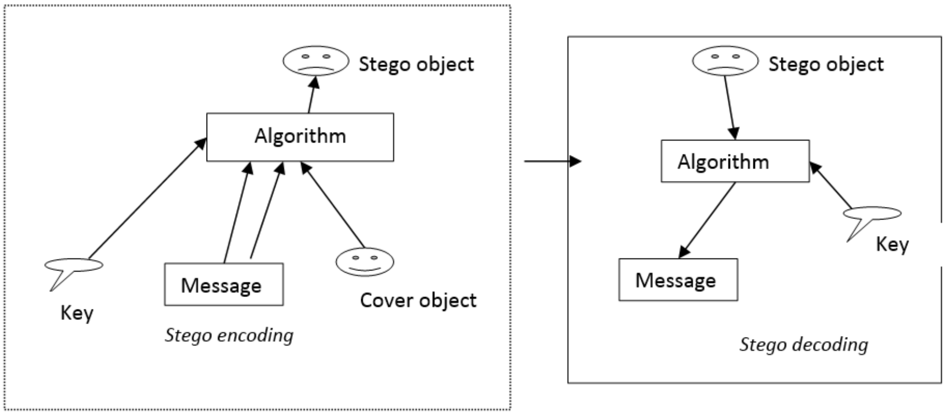


*Fig 1: General Model of Steganography*

In (Benabdellah et al, 2006), a Faber-Schauder Multiscales Transformation (FMT) and a Data Encryption Standard (DES) algorithm are combined to encrypt and compress still images while (Mohamed and Abbes, 2007) describe a robust watermarking schema based on logo embedding using image normalization to assist in embedding codes in an image. (Juneja et al, 2009) present the results of image compression and the LSB steganographic techniques using a 24-bit colour optimized to a 8-bit colour. (Kavitha et al, 2012) implement the LSB algorithm to hide data into image through the Microsoft.NET framework while (Sharma and Shrivastava, 2012) develop an improved LSB substitution and use it to hide an image in another image. In (Gupta et al, 2012) the operations of pure steganography, combined steganography and RSA algorithm and combined steganography and Diffie Hellman algorithm are compared.

In Section 2, the different methods of steganography are presented. Asymmetry cryptography is presented in Section 3 while the combined approach is presented in Section 4. Discussion on the strengths of the combined approach is presented in Section 5 where a conclusion is also drawn.

## 2. THE HIDE AND SEEK ALGORITHM

The hide and seek technique is one of the earliest techniques used in steganography. It uses the principles of Least Significant Bit (LSB) substitution. Alteration of the least significant bit in the cover object by the message bit should not pose serious changes in the cover object, that is, the change in the cover object is not easily detected or noticed. The hide and seek technique is a technique that replaces the LSBs of pixel values with the bits from the message bit stream. The algorithm does not require a key to implement and is implemented both sequentially and randomly. The sequential and randomized techniques (Bateman, 2008) are presented in algorithms 1-4 for encoding and decoding processes. In the sequential embedding, the algorithm starts at the first pixel of the cover image and embeds the bits of the message in order until there is nothing left to embed. The randomized embedding scatters the locations of the pixel values that will be modified to contain the bits of the message. A pseudo random number generator is employed in shuffling the data in the cover image.

**Algorithm1**: The encoding process of the Hide and Seek algorithm in sequential mode.

```
1. For i =1,….,l(m) do
2.     PŶ  LSB ($c_i$)
3.     If P ≠ $m_i$ then
4.         $C_i$ Ŷ  $m_i$
5.     End if
6. End for
```

**Algorithm 2**: The decoding process of the Hide and Seek algorithm in sequential mode.

```
1. For i = 1, … l (s) do
2.     M'$_i$ Ŷ  LSB ($s_i$)
3. End for
```

**Algorithm3**: The encoding process of the Hide and Seek algorithm in randomized mode.

```
1. Generate randomized sequence C using data c and seed k
2. For i =1,….,l(m) do
3.     PŶ  LSB (Ci)
4.     If P ≠ $m_i$ then
5.         $c_i$ Ŷ  $m_i$
6.     End if
7. End for
8. Generate original sequence c using data C and seed k
```

**Algorithm 4**: The decoding process of the Hide and Seek Algorithm in randomized mode

```
1. Generate randomize sequence  s using data S and seed K
2. For i = 1, … l (s) do
3.     M'$_i$ Ŷ  LSB (Si)
```

4. End for

The counter in the algorithm loops through the length of the message (l(m)), then the LSB in the first pixel of the cover object is evaluated and assigned to variable p. LSB is obtained by calculating the modulus 2 of the pixel, that is, finding the remainder when dividing the pixel value by 2. For an odd number, the LSB value is 1 and 0 for an even number. For example, the number 15 (odd) in binary is 1111, so the LSB value is 1 while the number 14 (even) in binary is 1110, so the LSB value is 0. The LSB value is then compared with the message bit mi that is to be embedded, if the LSB value of the cover object is the same as that of the message then the value is retain otherwise, if they are different then assign the message bit mi to the cover object bit (ci). The process continues in the entire length of the message. This is the same for both the sequential and randomized embedding except that in the randomized embedding the data in the cover object must first of all be shuffled using the pseudo random number generator and reshuffled after the decoding process.

One obvious weakness of the hide and seek algorithm is that it works without a key, anyone that can understand and manipulates the encoding and decoding processes can unlock the stego image and get the message. There has been series of improvement on this over the years resulting in algorithms such as jSteg, Outguess, F3, F4 and F5 algorithms using the transform domain techniques. These techniques come with some complexities into the algorithms without appreciable security proof in the design of the keys. The transform domain techniques have advantages over the LSB techniques in the area of embedding messages as they could be used to embed messages in file formats like the jPEG which are more compressed and readily used.

## 3. ASYMMETRY CRYPTOGRAPHY

Some cryptography techniques have good key design that is difficult to manipulate. One such technique is the asymmetry cryptography which uses a private key and a public key generated by the potential receiver of a message to his potential sender. 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, Ke and Kd and keeps the decryption key Kd a secret. The encryption key Ke 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 Ke and Kd for encryption and decryption respectively. For example, if B expects to receive secret information from other agents, B generates a pair of keys Ke and Kd. and publish Ke and keeps Kd secret. It may do this either by sending Ke 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 Ke and uses E(Ke, M) to produce (M)Ke before sending it to B. Only B knows Kd and can apply D(Kd,{M})Ke) to decrypt the message (Coulouris, et al, 1994). This is depicted in Figure 2.

El Gamal algorithm is based on the Diffie-Hellman key and consists of the key generator, the encryption algorithm and decryption algorithm. The key generator generates both the public key and private key using a random number. Similarly, the Rivest, Shamir, Aldeman (RSA) algorithm is asymmetry cipher that offers both encryption and decryption algorithms and generates both public and private keys (Stallings, 2001). These algorithms and their keys though effective are not invulnerable as recent development has come to prove. Cryptography algorithms are mostly used to encrypt text files while steganography algorithms could be used to hide text, image and audio files. Cryptoanalysts work hard to break security systems secured with these algorithms of late. This calls for concerted effort to design a system that integrates two or more algorithms or techniques.

## 4. THE COMBINED SYSTEM

The combined system consists of two levels of security; the encrypting of the message before encoding it on a cover object to form a stego object, the decoding of the stego object to obtain an encrypted message which will not be meaningful to the receiver until he decrypts it. In steganography, the message is hidden in a cover object using LSB substitution method such as the hide and seek encoding algorithm or any of the algorithms the steganographer may be familiar with. The stego object which is the output of the encoding process is sent to a potential receiver of the message which on receipt manipulates it using the decoding algorithm to get the original message. An intruder who gets the message in transit and is familiar with the decoding algorithm can as well manipulates the stego object and get the message.

The combined system offers another level of security in the sense that the intruder needs to obtain a key to decrypt what he has been able to uncover. What an intruder uncovers will not make any meaning to him since it is encrypted and needs to be decrypted using a private key which is known only to the receiver. The steganographic system is relevant and a good security measure too because the object comes in a form that may not be of interest to the intruder so he may not make an attempt to hack. Figure 3 shows a simple combined model of the stego-crypto system.

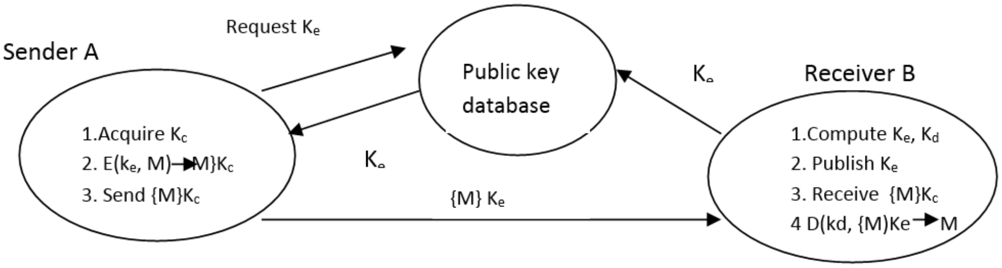


*Figure 2: The process of encryption and decryption with public and private keys*

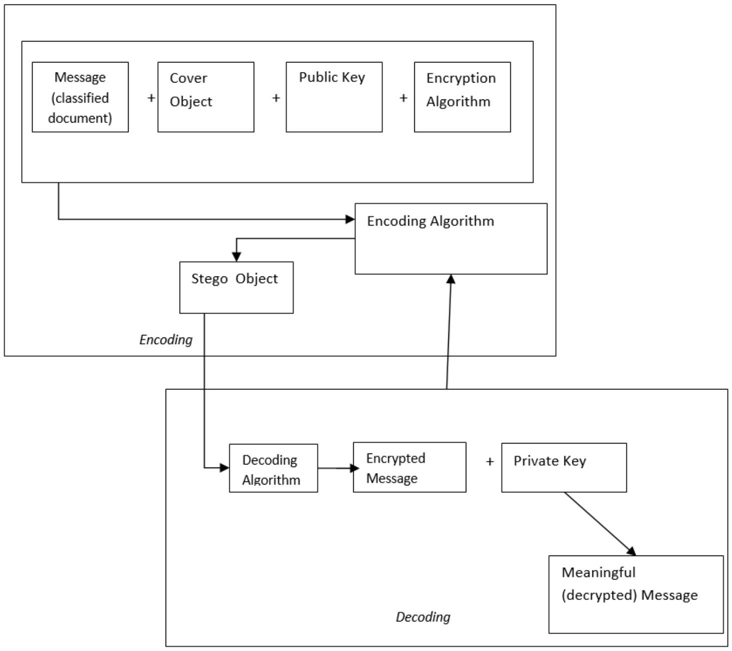


*Figure 3: A Combined Model of a StegoCrypto system*

## 5. DISCUSSION AND CONCLUSION

Various methods of ensuring that information is available to only authorized users abound in computing. These methods try to ensure the security and integrity of data, but there are always people out to make a living in hacking by breaking through the security. There has never been a perfect information security system; a system that is considered secured now could be broken into in no time. Cryptography which started with the manual system of managing information has grown into computing with various ciphers. As these methods are devised, so are the methods of attack. The same goes with steganography and others.

In studying the two security techniques of cryptography and steganography, it was discovered that they share certain attributes with the sole aim of hiding information from an unauthorized recipient. Cryptography hides the contents of a message from an unauthorized user while steganography conceals the existence of the message. Keeping the contents of a message secret may not be enough so it is necessary to conceal the message from potential intruders. The asymmetry method of cryptography does well in key management where there is a public key known to both the sender of information and the receiver and a private key known only to the receiver. On the other hand, steganography has its weakness in key management but triumphs in its ability in hiding information in a form that only the authorized receiver will find fascinating. Cryptography hides information in a form that will arouse the curiosity of an intruder.

In order to overcome the limitations of each of the approaches and enhance their individual strengths, an integration of the two methods is proposed in this study. In the hybrid, a simple LSB technique using the hide and seek algorithm integrated with an asymmetry cipher is proposed. One of the strengths of the LSB technique is the simplicity in embedding the bits of the message directly into the LSB plane of the cover object (Chandramouli and Memon, 2001). Modulating the LSB does not result in a human perceptible difference because the amplitude of the change is small, so the resulting stego object will look identical to the cover object. These attributes of LSB technique are combined with the private-public key technique of a cipher like RSA to give the hybrid a high degree of invulnerability. An intruder who finds a stego object and knows how to unlock it will get disappointed when he finds a meaningless message as the product of his endeavour. Attempting to decrypt the meaningless message requires a private key that is not available at his disposal and which he may not be able to manipulate. He has to sweat it out to cryptanalyse before getting a meaningful message.

The new approach may not be impossible to break, but will take a lot of resources which at the end will not worth the effort. If an intruder stumbles on a strange object containing a confidential message such as classified information on government policy that needs not be made public he may not find this fascinating so would not engage himself trying to unveil it. If because of certain reasons he opens it, he will find some strange codes that require a key to decode. The resources put in doing this may not worth the while at the end of the exercise. The time complexity of the exercise is enormous but the security achieved is significant. Efforts are being intensified to design an asymmetric steganography algorithm using the F5 algorithmic approach.

## REFERENCES

Bateman P(2008) Image Steganography and Steganalysis, MSC Thesis, Department of Computing, University of Surrey, Uk

Benabdellah M, Gharbi M, Zahid N, Regragui F and Bouyakhf E (2006). Encryption-Compression of Still Images using the FMT transformation and the DES algorithm. Georgian Electronic Scientific Journal: Computer Science and Telecommunication 4(11), 22-31

Coulouris G , Dollimore J and Kindberg T (1994). Distributed Systems, Concepts and Design, 2nd Edition, Addison Wesley, London.

Chandramouli, R and Memon, N (2001). Analysis of Least Significant Bits Based Image Steganography Techniques, IEEE International Conference on Image processing vol 3 pp 1019-1022

Chandramouli, R, Khaarrazi and Memon N (2003). Image Steganograhy and Steganalysis: Concepts and Practice. Proceedings of the second International Workshop on Digital Watermarking.

Gupta S, Goyal A, Bhushan B(2012).Information Hidding using Least Significant Bit Steganography and Cryptography. International Journal of Modern Education and Computer Science (6) 27-34.

Juneja M, Sandhu P. and Walia E(2009).Application of LSB based Steganogarphic Technique for 8-bit Color Images. World Academy of Science, Engineering and Technology, (26) 423-425

Kavitha K, Koshti A, and Dunghav P(2012). Steganogrpahy using Least Significant Bit Algorithm. International Journal of Engineering Research and Applications; 2(3) 338-341

Kharrazi M, Sencar, H, and Memon N(2004). Image Steganography: Concepts and Practice, WSPC/Lecture Notes pp1-49

Mohamed F and Abbes R(2007). RSTRobust Watermarking Schema based on Image Normalisation and DCT Decomposition. Malaysian Journal of Computer Science 20(1) 77-90.

Moulin P and Mihcak M (2004). AFramework for Evaluating the data hiding capacity of Image sources. IEEE Transactions on Image Processing vol 2 pp 1029-1042.

Obot, O. Ekong, V and Okon M (2012).Enhanced Playfair Cryptography System for Data Security and Integrity in a Cashless Society. Proceedings of NCS National Conference on Towards a Cashless Nigeria: Tools and Strategies, Uyo, Nigeria. Vol 23 pp 56-60.

Sharma V and Shrivastava(2012). A Steganography Algorithm for Hiding Image in Image Improved LSB substitution by minimize detection. Journal of Theoretical and applied Information Technology, (36)(1) 1-8.

Stallings, W (2001) Cryptography and network security: principles and practice, 2nd ed., Pearson education, USA.

Full Paper

# A CONCEPTUAL DESIGN OF A LOW COST IDENTIFICATION MANAGEMENT SYSTEM FOR NIGERIA

**O. Osunade**
Dept. of Computer Science,
University of Ibadan, Nigeria
osunade@mail.ui.edu.ng

**B. S. Olanrewaju**
Dept. of Computer Science,
University of Ibadan, Nigeria
bs.olanrewaju@gmail.com

**O. F. Phillips**
Dept. of General Studies,
Ladoke Akintola University, Ogbomosho, Nigeria
folushophillips@yahoo.co.uk

## ABSTRACT

The National Identification program in Nigeria has faced numerous challenges over the years. Every attempt by government to make the program acceptable and functional has not been successful. The computer and data network, on which the program depends, needs to be well designed, developed, responsive and transparent to users. A low cost corporate system which could be easily implemented without too much investment on required infrastructure is adopted to marshal the benefit of information technology to design a viable identification management system for Nigeria. The system incorporates the concept of distributed computing with various interactive input devices at each points linked to centralized secured database via reliable broadband communication technology. This paper presents this low cost identification management system for the acquisition of citizens' data, verification of the data collected and distribution of the national identity card in Nigeria. The business and logistic implications of the system will be presented in future research publications. The system is sustainable and applicable for the Nigerian environment because it is built on existing infrastructures and would only need some customisation for it to work.

**Keywords:** *data, identification management, information technology, Nigeria*

## 1. INTRODUCTION

Nigeria, the most populous nation in African, gained independence in October 1st 1960 from the British and since that day, Nigeria remained a federation of distinct regions. According to National Bureau of Statistics (2008), Nigeria is situated between 30 and 140 East Longitude and 40 and 140 North Latitude; the area of Nigeria is 923,769 square kilometres and is made up of 909,890 square kilometres of land area and 13,879 square kilometres of water area. Located in western Africa, Nigeria borders countries namely Benin with a distance of about 773 km, Cameroon with a distance of 1,690 km, Chad with a distance of 87 km, and Niger with a distance of 1,497 km. With a population of over 150 million people, about 250 ethnic groups spread across the six geo-political zones; Nigeria has many languages such as Yoruba, Hausa and Igbo with English being the official language.

Having a reliable national identification system and citizens register is a good compliment for national planning, election, census board, law enforcement, banking, tax collection, pension board, education and in fact the judiciary (Akinlabi, 2006). Without functional identification systems, citizens of many developing countries miss out on the benefits of official identification. In many poor countries, not only is there no consistent identity system but at least half of the people don't have records of birth at all (MacDonald, 2011).

### 1.1 History of Identification System in Nigeria

The idea of a national identification card system in Nigeria was originally conceived in 1977 but was eventually executed in 2003 after several controversies and bottlenecks (Obi, 2006). In 1978 under the Department of National Civic Registration (DNCR), which was charged with registering and issuing a National Identity Card to every citizen of Nigeria who was then 18 years or older, an attempt was initiated to document the identity of Nigerians and non-citizens using biographic data. The aim of this scheme then as stated in the National Identity Management System Handbook on Business Processes, Standards and Specifications (2011) was to use the program as an effective tool for controlling illegal immigration, to validate other civic documents like travel passports, and to set up a reliable personal identification system for securing commercial transactions with financial institutions and the like.

In 2007, National Identity Management Commission (NIMC), established by the NIMC Act No. 23 of 2007, was given the mandate to establish, own, operate, maintain and manage the National Identity Database in Nigeria. A key requirement of the National

Identity Management System (NIMS) is the capture of biometrics and necessary demographic data in a standardized manner that would facilitate identity authentication and verification using the unique National Identification Number (NIN) (NIMC, 2011). National Identity Management Commission, in discharging of its duties, on July 2009 constituted a body to be known as the National Identity Management and Harmonization Committee (NIMHC) to become the custodian for setting standards for National Identity Management System. By the extension of the National Identity Management Commission Act, Section 5, part (j), NIMHC established rules and standards that shall be binding on all subjects, agencies, organizations, and entities that are collecting, disseminating, or consuming identity data in Nigeria (NIMC, 2011).

### 1.2 Present State of Identification System in Nigeria

Presently, Nigeria has a national identity programme that is incomplete because not every Nigerian participated in the last National identity (ID) Card project which means that not everybody is uniquely identified. That is why the critical private sectors are doing their own identification (Obi, 2006). The NIMS Handbook stated that there is currently no centralized national identity database and no system of National Identity Management which efficiently links public and private sector identity schemes. While the financial services sector has been most proactive in the deployment of identification schemes for delivery of its services, several different identification schemes and databases by the various institutions offering services to that person has led to the duplication of an individual's identity. Government agencies also hold a number of databases with no viable integration of access or interoperability to enhance the delivery of services within these government institutions. A reliable national identification system for verification and secure authentication of an individual's identity is still being fashioned out with the plan introduction of the NIN project, which is a means of having a dependable data base of its citizens (Omoniyi, 2012). Therefore, there is need for contributions to have viable national network architecture (deployment map) for an identification management system in Nigeria.

For the national identification management system, a low cost deployment map that allows building on existing technology to create highly efficient, integrated systems that collect, manage, organize, and disseminate information throughout different sectors in both public and private organization is proposed by this paper for the nation.

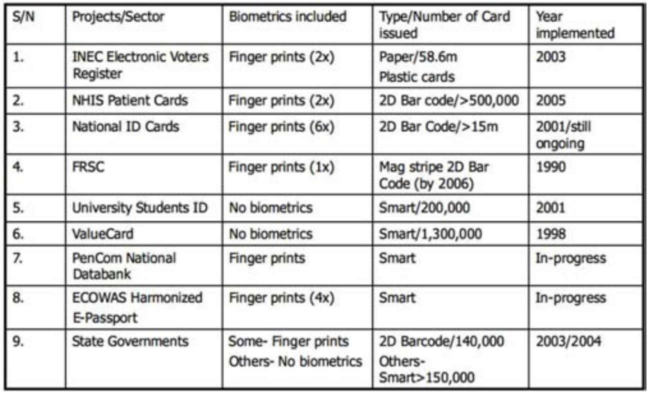
## 2. LITERATURE REVIEW

There have been different intended approaches to achieve the national identification project among which is the talked about synergy among Nigerian Communications Commission (NCC), NIMC and the Federal Road Safety Commission (FRSC) to deliver a national database, which will effectively capture the details of Nigerians (Aginam, 2008). The outcome of this has not been seen, though NCC is to transfer the data compiled during the SIM card registration to NIMC. Other approaches are highlighted in Table 1.

### 2.1 Processes to have Identification Card

The idea of national ID card is now matured as NIMC has initiated processes for the issuance of the unique NIN and General Multipurpose Smart Cards (GMPC) to all Nigerians and Legal Residents (NIMC, 2011). This will now serve the purpose of national ID card. There have been many challenges delaying the take off of the project which has led to series of postponement. The process, which was planned to begin by August 1, 2011 but was later shifted to May, 2012 then to September 2012 is yet to take off (Oketola, 2012). The NIMC had engaged two consortia, Chams and Onesecurecard, in July 2010 to serve as the Front End Partners to the project to carry out data capture, personalization of smart ID cards and deployment of smartcard verification devices for the National Identity Management campaign and also responsible for the financial and other risks in relation to the design, financing, construction, completion, commissioning, maintenance, operation, management and development of the works and registration centres for the purpose of the national ID project (Oketola, 2012). However, after signing the agreement, the consortia had been unable to raise the necessary funds to execute their mandates (Oketola, 2012).

*Table1: Highlights of the Nigerian Experience*



| S/N | Projects/Sector | Biometrics included | Type/Number of Card issued | Year implemented |
|---|---|---|---|---|
| 1. | INEC Electronic Voters Register | Finger prints (2x) | Paper/58.6m<br>Plastic cards | 2003 |
| 2. | NHIS Patient Cards | Finger prints (2x) | 2D Bar code/>500,000 | 2005 |
| 3. | National ID Cards | Finger prints (6x) | 2D Bar Code/>15m | 2001/still ongoing |
| 4. | FRSC | Finger prints (1x) | Mag stripe 2D Bar Code (by 2006) | 1990 |
| 5. | University Students ID | No biometrics | Smart/200,000 | 2001 |
| 6. | ValueCard | No biometrics | Smart/1,300,000 | 1998 |
| 7. | PenCom National Databank | Finger prints | Smart | In-progress |
| 8. | ECOWAS Harmonized E-Passport | Finger prints (4x) | Smart | In-progress |
| 9. | State Governments | Some- Finger prints<br>Others- No biometrics | 2D Barcode/140,000<br>Others-Smart>150,000 | 2003/2004 |

*(Source: Onyemenam, C. E., Identity Management Systems in Africa: Nigeria's Experience, www.nimc.gov.ng)*

### 2.2 National Identification Number

The unique NIN is principally meant to give the country a dependable data base of its millions of citizens, a process that has never been entirely completed in any programme in the past. The NIN is a non intelligent set of numbers assigned to an individual upon successful enrolment. Enrolment consists of the recording of an individual's demographic data and the capture of the 10 fingerprints, head to shoulder facial picture and digital signature which are all used to crosscheck existing data in the national identity data base, to confirm that there is no previous entry of the same data. Once this process is completed the data is then stored with the unique number known as NIN (Omoniyi, 2012). When the numbers are issued, they will be uploaded on chip-embedded multifunctional smartcards alongside citizens' personal information (Oketola, 2012). This number when issued to a person cannot be used again, even if the person to whom it is issued dies. It is the number that ties all the relevant records of a person in the data base and is used to verify diverse identities. Access to the database is secure and graduated and that every resident from 16 and above would soon be mandated by law to register their NIN or they would be deprived of access to basic day to day commercial transactions (Omoniyi, 2012).

It is a unique identification number that every citizen and legal permanent resident must have. It helps the government to plan. It is to differentiate two or more people with the same names. This makes identification easier. A lot of other information like home address, phone number, date of birth, parent's information, DNA information, criminal record, driving record, marriage information and even employment record of people are stored with the number. Hence, a complete life history of a person can be pulled from the computer (by authorized government officials) with his social security number (Omoniyi, 2012).

### 2.3 Present Attempt to Have Identification System

Presently, Nigeria Interbank Settlement System (NIBSS) is working in collaboration with NIMC to integrate the Nigeria Central Switch, NCS, operated by NIBSS with the NIMS. This integration will enable banks to conduct identity verification on NIMS through NIBSS to issue NIN as well as a General Purpose Identity Card (Komolafe, 2012).

The front-end partners (FEP), of the NIMC had agreed with NIMC, CBN, and NIBSS that starting from 1st of September 2012, they would commence an enrolment exercise for all banks' customers nationwide with a view to capturing their biometrics, issuing them the National Identity Numbers (NIN) and the General Multi-purpose Identity Cards (GMPC), as well as providing verification infrastructure for linking their bank accounts to the issued NIN within the NIMC data base. This enrolment exercise was planned to be completed by the 31st December 2012 (Komolafe, 2012). This is yet to take off.

### 2.4 Identification Management in Other Countries

Many countries around the world have either implemented, or are in the process of embarking on national ID projects. The key motives behind such initiatives is to improve the identification and authentication mechanisms in order to reduce crime, combat terrorism, eliminate identity theft, control immigration, stop benefit fraud, and provide better service to both citizens and legal immigrants (Al-Khouri, 2006). Many countries around the world have national identification cards, although the type of card and the purposes for which it is used varies (Wang, 2003). The majority of cards in developed nations contain name, sex, and date of birth and some with photographs and fingerprints (Wang, 2003). Some nations have much more data on their cards. Wang (2003) cited examples and the purpose of identification card management in some countries. In Korea, the card has name, birth date, permanent address, current address, military record, issuing agency, issued date, photograph, national identification number, and prints of both thumbs. The Italian card contains identity number, name, photo, signature, fingerprint, date and place of birth, citizenship, residency, address, marital status, profession, and physical characteristics. In Spain, when someone works under contract the identification must be used to demonstrate work eligibility, and it also is used for the health care system.

In Kenya, the national identity card is required to get a job, get married, purchase or sell land, or register to vote. In Belgium, everyone over the age of fifteen is required to carry the identification card at all times. The card is used for banking, billing, rental agreements, proof of age when buying alcohol and cigarettes, or entering an adult-only business. A police officer can ask to see the card of anyone in a public space and does not need to have any particular justification (Wang, 2003). As a result of the rapid growth of the economy as well as the population over the past few years in the United Arab Emirates (UAE), the project which was kicked off in June 2003, aimed to develop a modern identity management system with two strategic objectives addressing security and economical requirements (Al-Khouri, 2006).

## 3. METHODOLOGY

This work was carried out using qualitative analysis on available information and personal experience with the various national identification card registration program of the country. The network design being proposed is based on existing infrastructures that are functional in the country as at the time of this study. The National Identity Management Commission (NIMC) is made to be the central coordinating agency as it has the mandate and established Acts as stated earlier to handle matters relating to national identity management issues. The study also uses human psychological and sociological concepts in the design of the architecture. The architecture has a three layer structure as shown in Figure 1.

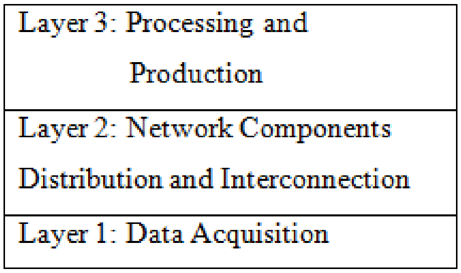

Layer 3: Processing and Production
Layer 2: Network Components Distribution and Interconnection
Layer 1: Data Acquisition

*Figure 1: Layer Structure of the Architecture*

Layer 1 is the access point where bio-data and other necessary documents are acquired; layer 2 is the distributing layer for the network facilities for acquiring peoples' data from each of the affiliated branches (in layer 1) of institutions partaking in the processing of ID card. Also, layer 2 interacts with layer 3 in a coordinated and controlled manner to exchange information and authenticate connections. Layer 3 is where the processing of data and production of NIN and GMPC takes place; it also, has facilities to authenticate every connection to it.

The following assumptions were taken in this work: (1) Nigeria is interested in having a national identification management system, (2) a communication system will be used for data transfer, access, verification and authorization (3) data acquisition can be carried out using a variety of information technologies and (4) there is a data verification mechanism available.

The design depends on different computer networks and communications technologies available at different input centres with the integration at NIMC. At every data collection point, network devices to capture citizens' biometric data, photographs, their ten finger prints as well as scanners to scan any supportive documents submitted should be available. Most agencies and financial institutions suggested as participants in the process might have the computer network and communication technology infrastructures needed. However, for others without such facilities, and for interoperability between different agencies or institutions, a distributed computing system that ensures that government can collect the knowledge that resides within the country to respond with creativity and speed to changes in the citizens' data for up to date information stored for every individual. Distributed computing is needed because the process requires the use of a communication network that connects several computers and also the data produced in one location will be needed in another location. The system is designed to have multiple contact points and offline capability in case there is any problem with the system connection.

The relationship/communication between various sectors for the national identification management is shown in Figure 2.

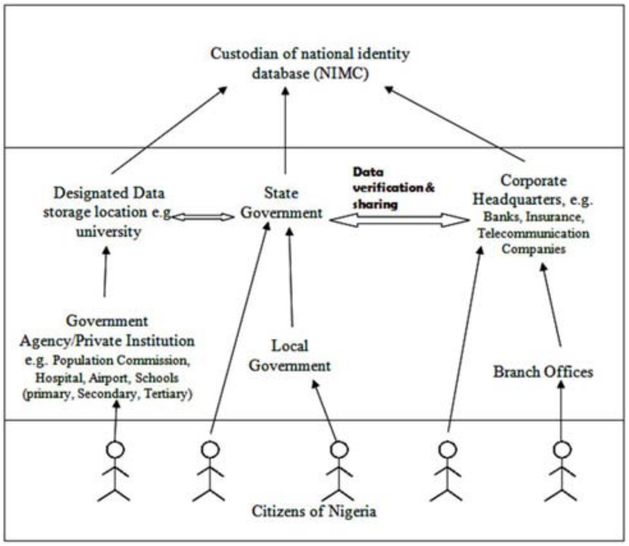

Custodian of national identity database (NIMC)
Designated Data storage location e.g. university
State Government
Data verification & sharing
Corporate Headquarters, e.g. Banks, Insurance, Telecommunication Companies
Government Agency/Private Institution e.g. Population Commission, Hospital, Airport, Schools (primary, Secondary, Tertiary)
Local Government
Branch Offices
Citizens of Nigeria

*Figure 2: relationship/communication between various sectors*

The figure shows that citizens of Nigeria at layer 1 of the architecture could submit their biometric data to anyone of government agencies or private institutions. The local government being the closest level of government to the people and also rendering services like birth registration and the likes is also recommended for citizens' data collection points. Bio-metric data could also be collected at state government level and also at corporate headquarters of financial institutions and their branches. In these contact points, the system would allow citizens' data to be sent through web pages, e-mail anytime from anywhere to head offices of agencies or institutions.

Layer 2 of the architecture makes use of the existing functional infrastructures of institutions partaking in the program for data sharing, transfer, access, verification and authorization.

At the top level of the architecture is the processing and production of the National ID card. National Identity Management Commission provides the NIN that is unique to each Nigerian that has registered with the Commission. Only NIMC can assign the NIN which cannot be re-assigned to a subject once it is assigned to a subject and it can never be changed or altered in any form. NIN does not expire and is valid for the entire life span of the subject biometrics that it was assigned to. NIN shall be the basis of which the Federal, State, and Local government shall interact with a citizen of Nigeria. Each Ministry, agency, regulatory body, and entities must tie an individual to a NIN before services can be rendered to the individual.

Direct access to the NIMC Gateway by any third party shall only be after obtaining proper credentials from NIMC. The NIMC Core Database, also referred to as the NIM Super Structure is the only authoritative database recognized by the Federal Government to provide Personal Identification Verification (PIV) services in Nigeria (NIMC, 2011). All access to the system as shown in figure 3, shall be through the Gateway and all access to data in NIMC Core must be predetermined and approved otherwise shall be prohibited.

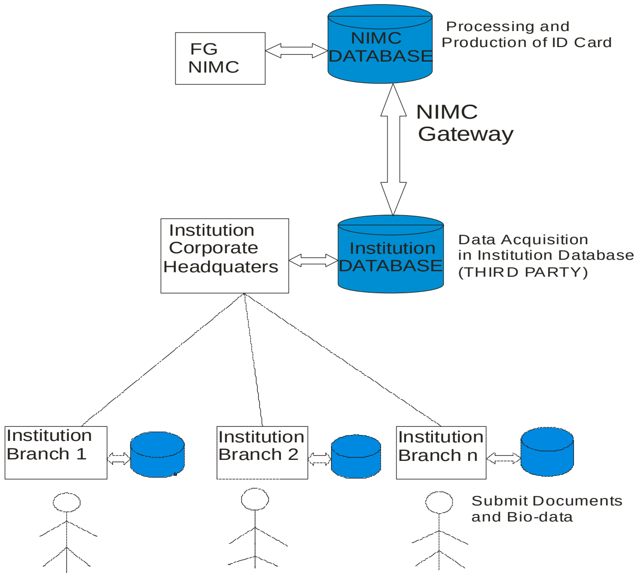

FG NIMC
NIMC DATABASE
Processing and Production of ID Card
NIMC Gateway
Institution Corporate Headquaters
Institution DATABASE
Data Acquisition in Institution Database (THIRD PARTY)
Institution Branch 1
Institution Branch 2
Institution Branch n
Submit Documents and Bio-data

*Figure 3: Hierarchical Structure of Database Server*

### 3.1 Proposed Implementation Plan

For implementing a National ID card system it is necessary to a have a database containing the personal information of all those bearing the ID cards. When such a lot of private information is kept in one database it leads to a lot of questions from privacy advocates about the security of the database, the departments that have access to it and the cost of implementing such a system (George, 2005). The infrastructure used to make identification system simple and secure should have centralized and integrated population database with government trusted identity verification services to prevent identity theft and protect the privacy of citizens. A digital nervous system (DNS) that has a spontaneous response to changes in environment is considered in this design for quick response to changes in citizens' information. The system has the following characteristics:

1. Multiple access points with interactive devices that allow users to actively participate in a technological process instead of just reacting to it.
2. Communication networks with offline capabilities to ensure that system continues to function in case of connection problems.
3. Broadband communication technology for high speed connection.
4. Internet services.

DNS is similar to a biological nervous system in that they both have multi-sensory inputs, intelligent filtering, ability to correlate information in real time and response to various inputs (Jespersen, 2010). It involves a simple idea of getting the right information to the right people at the right time though it depends on the power of latest information technologies to make data flow faster and more cost-effectively than ever before. Data needs to be accessible no matter where a person is, and DNS will enable such like the movement, collection, storage and retrieval of all that information, no matter where one is located whether in a rural or urban areas. The whole concept is to let the people participate in the process of national identification management, no matter the technology available to them.

## 4. RESULTS AND DISCUSSION

Figure 4 shows the network architecture based on the framework given in Figure 1. The architecture makes use of existing resources and infrastructures such as telecommunication links of financial institutions, electricity supply and buildings for servers and other equipments.

At layer 1, the grass root access points, use interactive devices such as smart phones, biometric reader, scanner, digital cameras, etc. to acquire bio-data and other necessary documents. These points could be branch offices of Banks, Insurance companies, Telecommunication, Airports, academic institutions, hospitals, local government etc. Layer 1 connects to layer 2 through different available transmission channels. As moderate to high network traffic is expected here, communication media for connection to upper layer suggested are microwave radio if a line of sight communication could be established, Very Small Aperture Terminal (VSAT), digital subscriber lines (DSL), Optical Fibre Cable. Each of the branches connects to their corporate headquarters via these broadband technologies at layer 2. These headquarters may use microwave radio in a limited distance of line of sight, communication satellite, or fiber-optic cable. Fibre-optic is recommended in this design because of higher data rates, non susceptibility to electromagnetic interference, lower error rates, and more secured against wiretapping compare to other means of transmission. Firewall mechanism is needed to facilitate authentication during data sharing. At the last layer, edge delivery architecture is used to distribute information and services to end users. In edge delivery, the content of NIMC database is available from multiple servers located at the edge of the NIMC network. In other words, an organization would be able to find all requested content on a server within its home network.

Co-location is one of the principles on which this network architecture is built. Servers storing national identification data and records can be located in other institutions using a memorandum of understanding (MOU) to ensure security, accessibility by authorized personnel and availability of electricity.

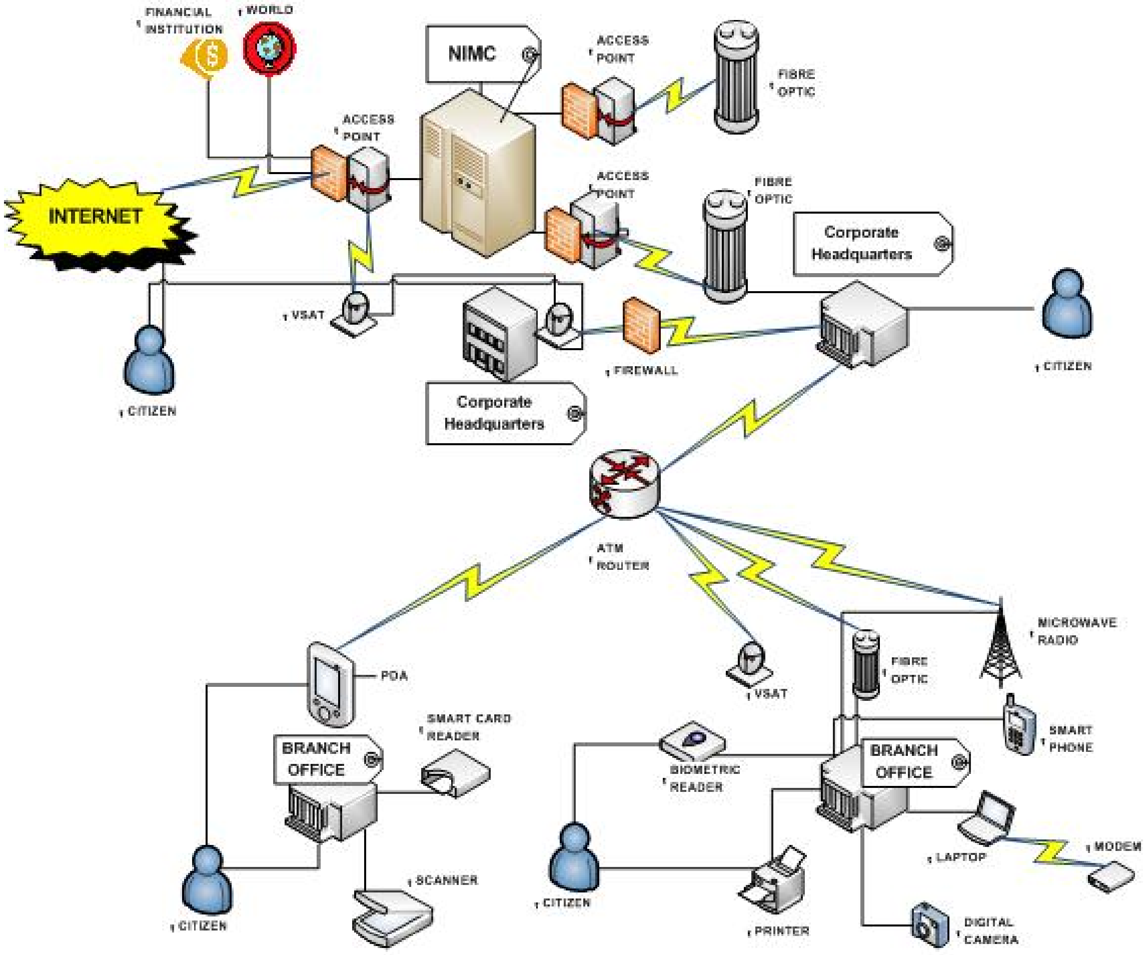


*Figure 4: Network architecture for national identification programme*

The involvement of financial providers in the network architecture is to provide credible data acquisition points that citizens are most likely to use on a daily, weekly or monthly basis. The previous program implementation made use of ad-hoc staff spread across the country using temporary shelters for the data acquisition. The merit of that idea was to reach as many people as possible. With a stable and semi-permanent location for the national identification registration more people will be covered and the need for ad-hoc staff will be reduced. Other locations such as hospitals, university, airport and government ICT units could be used as contact points for potential national identification providers.

The network architecture provides data sharing and redundancy at each level of data storage. This means that two or more centralized database servers in a state are configured to respond to Identification requests. The implementation may allow the database servers to contain the same information or allow each server to be updated by a server higher up in the hierarchy.

Citizens are more likely to feel better about releasing personal information to data acquisition points such as the bank because the financial institutions already have this information. Financial institutions can use the data acquisition process to market their products to citizens of the country. The buy-in for financial institutions and other participating units would be the acceptance of the produced national identification card. If the process or management of the data and records is not secured enough for financial institutions to rely on it for identification then the success of the national program is at stake.

The repository of all citizens in the country should be stored in a data warehouse owned and managed by the government or its representative i.e. NIMC. The warehouse is the apex of the hierarchy where all verified and acquired data are kept.

The multiplicity of data communication media available should be incorporated into the architecture to ensure that it is always available. In Nigeria, there are fibre optic cable in some paths of the country, most financial institutions own VSATs for satellite communication, and telecommunication operators provide frequencies for data transfer. All these media are incorporated into the network architecture to ensure accessibility and availability of the identification databases.

The point of acquisition is also the point of collection. Data verification would be carried out before authorization is given for the production of the card.

## 5. CONCLUSION

The national identification program in Nigeria will have astounding success if the deployment map proposed in this paper is adopted. The architecture takes care of data acquisition, data updating and distribution of identification cards to citizens of the country. The network architecture is the basic infrastructure needed for the success of the national identification program. The deployment map developed is sustainable and applicable to the Nigerian environment.

## REFERENCES

Akinlabi, A. 2006. Nigeria National Identification Card -Its Costs and Benefits. Accessed on May 10, 2011 at www.gamji.com/article6000/NEWS6202.htm

Aginam, E. 2008. Mobile Fraud - NCC to Collaborate with National ID Commission on SIM Card Registration. Vanguard Newspaper. Accessed on May 10, 2011 at allafrica.com/stories/200808181274.html

George C. Paul, 2005. Concerns about National ID Cards. Accessed on May 10, 2011 at http://www.frost.com/prod/servlet/market-insight-top.pag?docid=38947972

Hans Jespersen, 2010. Evolving the Digital Nervous System. http://solacesystems.com/blog/company/news-release/evolving-the-digital-nervous-system/

Komolafe Babajide 2011. Customers to provide National Identity Number at banks – CBN. June 1, Vanguard Newspaper.

MacDonald, L. 2011. Leapfrogging Technology, the Case for Biometrics: Alan Gelb Accessed on May 10, 2011 at http://blogs.cgdev.org/global_prosperity_wonkcast/2011/01/11/leapfrogging-technology-the-case-for-biometrics-alan-gelb/.

National Bureau of Statistics, Facts and Figures about Nigeria, 2008. Accessed on May 10, 2011 at http://www.nigerianstat.gov.ng/ext/latest_release/Fact08.zip

National Identity Management Commission, 2011. National Identity Management System Handbook on Business Processes, Standards and Specifications 6th January, 2011. Accessed on May 10, 2011 at www.nimc.gov.ng/hic/Handbook_on_Business_Processes.pdf

National Identity Management Commission, 2011. Public Notice on the Proposed Adoption of Biometrics and Demographics Data Standards and Verification Procedure for the National Identity Management System (NIMS). Accessed on May 10, 2011 at http://www.nimc.gov.ng/downloads/adverts/Public_Notice_on_Proposed_Biometrics.pdf

Obi, E. U. 2006. National Identification Policy for Nigeria: An Action Agenda. Accessed on May 10, 2011 at www.dawodu.com/obi6.htm

Oketola, Dayo 2012. Nigerians to get national identity numbers in May: March 26, Punch Newspaper.

Omoniyi Tosin, 2012. National Identity Number: A rainbow of views. Monday, 02 April. Daily Trust online

Onyemenam, C. E. Identity Management Systems in Africa: Nigeria's Experience Available online at www.nimc.gov.ng.

Wang, T.V. 2003. The Debate Over a National Identification Card. The Century Foundation Homeland Security Project, Issue in Brief. Accessed on May 10, 2011 at http://tcf.org/publications/pdfs/pb284/National_ID_Card.pdf

Full Paper

# A CONCEPTUAL INTEGRATED MODEL FOR THE ADOPTION AND CONTINUED USE OF E-GOVERNMENT SERVICES

**Gabriel M. M. Obi**
International Business Systems Ltd.,
12 Moleye St. Alagomeji, Yaba Lagos
*gmm.obi@consultant.com*

**ABSTRACT**

Studies in the adoption and use of e-government services have developed along two streams in parallel: determinants of adoption and measurement of success, and even these have focused mainly on individuals or at best, private organizations. Until three years ago, there had been no consideration for the continuity of use after the adoption, and the best effort at this was based on an integration of the technology acceptance and the diffusion of innovation models. This work seeks to address the conceptual gap between the beliefs and attitudes about e-government services and those about using the services, which arises from the aforementioned parallel streams. It presents a conceptual model for the adoption, use and continuance of use of the e-government services, applicable to individuals, groups of individuals, and organizations (public, private and third party), obtained by integrating the updated Technology Acceptance Model (TAM 3), the Diffusion of Innovation Model, the user motivation Model (UMM), and a Benefits Evaluation Framework (BEF) based on the updated Delone and McLean Success Model.

**Keywords:** *Technology acceptance, Information systems success, Benefits evaluation framework, User motivation framework, object-based attitudes and beliefs, behavioral attitudes and beliefs*

## 1. INTRODUCTION

The ideas of behavioral beliefs and attitudes towards the adoption of technology were shaped into the technology adoption model (TAM), presented in (Davis, 1989). Since its introduction the model has been the subject of empirical tests, comparisons, variations and extensions, with the latest variant being the TAM3, (Venkatesh & Bala, 2008) (see APPENDIX 1).

A stream of works on e-government is based on TAM or its variants, which provide sound prediction of usage of the e-government services by linking behaviors to attitudes and beliefs (ease of use and usefulness) that are consistent in time, target and context with the behavior of interest (service usage). Another stream of works is, in parallel, based on the Information System Success model, introduced by DeLone and McLean, (DeLone & McLean, 1992) (see APPENDIX 2), whose related literature explicitly enumerates systems and information design attributes (e.g. information accuracy (information quality), system reliability (system quality)), making it a potentially useful diagnostic for system design.

These approaches, parallel as they are, introduce a conceptual gap between the beliefs and attitudes about e-government services and those about using the services, (Wixom & Todd, 2005). A call has been made to bridge this gap: that although these two research streams have evolved largely as parallel, they can and should be integrated (Goodhue, 1988; Hartwick and Barki, 1994; Melone, 1990; Seddon, 1997). It is argued that such integration can

- help build a conceptual bridge from design and implementation decisions to system characteristics to the prediction of usage,
- ultimately improve the predictive value of user satisfaction and augment the practical utility of technology acceptance, and
- answer the call to provide a way for perception-based IT research to more fully examine the role of the IT artifact (Benbasat and Zmud, 2003; Orlikowski and Iacono, 2001).

This work seeks to address the situation – bridge the conceptual gap between the e-government services object-based and behavioral-based beliefs and attitudes.

The rest of the paper is organized as follows: Section 2 considers related works and the contributions of this work. This is followed in Section 3 by the presentation of the proposed model, and by Section 4, where the future direction and the conclusion are presented.

## 2. RELATED WORKS AND CONTRIBUTIONS OF THIS WORK

In this work the following definition and perspective of e-government are adopted:

E-government is about government, employing technology to improve the efficiency, effectiveness and accessibility of government – (these ends include better accountability and, according to the World Bank, (World Bank, 2011), better delivery of government services to citizens, improved interactions with business and industry, citizen empowerment through access to information, or more efficient government management, culminating in less corruption, increased transparency, greater convenience, revenue growth, and/or cost reductions)

Now, although the aforementioned two streams along which studies in e-government services have been conducted are actually complementary rather than competing (Wixom & Todd, 2005), and despite the need for integration thereof (Özkan & Bilgen, 2003; Wixom & Todd, 2005), the aforementioned gap persists, as the only two attempts made at the integration have not yielded the desired model. The first attempt at integrating the TAM and IS Success approaches, was presented in (Wixom & Todd, 2005). Based on the TAM, (Davis, 1989), and the Updated Delone and McLean model, (DeLone & McLean, 2003), it dealt with adoption and use by the individual (see APPENDIX 3).

It was not until six years later, that another attempt was made, in 2011, this time by a different set of authors, resulting in a hybrid model that integrates TAM1 with the Diffusion of Innovation (DOI) model and a trust factor, (Nour-Mohammad et al., 2011) (see APPENDIX 4), with which to predict and explain an individual's continuous use of e-government services.

The first integrated model did not address organizational and continuance of use while the second did not address the aforementioned conceptual gap as the integration did not include the user satisfaction (DeLone & Mclean) model.

### 2.1. Contributions Of This Work

This work presents a conceptual integrated model for the adoption, use and continuance of use of e-government services, applicable to individuals, groups of individuals, and organizations (public, private and third party e.g Not for Profit and Non-Government organizations). The Model is obtained by integrating the updated Technology Acceptance Model (TAM 3), the User Motivation Model, and a Benefits Evaluation Framework (BEF) based on the updated Delone and McLean Success model, and relying on concepts from the broader attitude literature (e.g., (Ajzen, 2001; Ajzen and Fishbein, 2005); Eagly and Chaiken, 1993; Fazio and Olson, 2003; and Haddock and Zanna, 1999). The model explicitly distinguishes the object-based beliefs and attitudes of the user satisfaction stream from behavioral beliefs and attitudes in the technology acceptance stream and

- enumerates a set of system and information characteristics that influence system and information quality,
- describes how they in turn influence object-based beliefs and attitudes with the system and the information it produces, and
- then describes how these object-based attitudes toward the system can shape the behavioral beliefs of usefulness, ease of use, and, ultimately, system usage and continued usage.
- thus provides a solution to the long standing problem of bridging the aforementioned conceptual gap.

## 3. THE PROPOSED MODEL

### 3.1. Theoretical Issues

Two concepts come into play prominently in discussions about the adoption and use of e-government services: attitude and behavior. The influence of attitude on behavior is the subject of a study, (Ajzen and Fishbein, 2005), building upon the Expectancy-Value Theory, (Ajzen and Fishbein, 1980). According to the aforementioned theory, beliefs about the outcomes associated with performing a behavior are influenced by external variables, which beliefs in turn shape attitudes toward performing a behavior. In the same vein, the intention to perform a behavior and ultimately the behavior itself are in turn, influenced by attitude. These ideas have taken shape in the form of the TAM model, a model that has been widely applied to understand the attitude one holds about the use of technology, and has and is being used to predict the adoption and use of information technology.

With TAM or its variants, expectations about the net benefits of the use of e-government services shape the attitude toward the use of the services, which attitudes in turn, influence the behavioral intention to adopt the services. Thus the attitude construct in TAM represents attitude toward the behavior of using technology.

Now, in a given situation the feelings of fulfillment or gratification of a desire or need, or the attitudes of a person toward a variety of factors affecting that situation constitute the satisfaction of the person in that situation. In the user satisfaction literature, information and services characteristics are the core considerations, (DeLone and McLean, 1992). Within this literature, user satisfaction is typically viewed as the attitude that a user has toward the technology itself; therefore, it represents an object-based attitude, contradistinctive to the TAM where the attitude construct represents attitude towards the behavior toward technology use.

These relationships, by the theory of reasoned action (TRA), will be predictive of behavior when the attitude and belief factors are specified in a manner consistent with the behavior to be explained in terms of time, target, and context (Ajzen and Fishbein 2005; Fazio and Olson, 2003).

Despite its predictive ability, TAM provides only limited guidance about how to influence usage through design and implementation (Taylor and Todd, 1995; Venkatesh et al., 2003). Such guidance was a core objective in the development of TAM, but one that has received limited attention (Davis et al., 1989). On a related note, a fundamental problem with user satisfaction research has been its limited ability to predict system usage (Davis et al., 1989; DeLone and McLean, 1992; Goodhue, 1988; Hartwick and Barki, 1994; Melone, 1990; Seddon, 1997; and Scialdone and Ping, 2010). Satisfaction with the system and its information output is unlikely to be directly predictive of the use of that system. Instead, user satisfaction needs to be recognized as an object-based attitude (Ajzen and Fishbein, 1980) whereby it serves as an external variable with influences on intention and behavior that are fully mediated by behavioral beliefs and attitudes (Ajzen and Fishbein, 1980; Eagly and Chaiken, 1993).

Empirical evidence shows that the object-based attitude is generally a weak predictor of behavior (Ajzen and Fishbein, 2005; Scialdone and Ping, 2010). Thus, better understanding the theoretical relationships within the user satisfaction literature can help bridge such equivocal findings while offering system designers a way to influence usage through design based on system and information characteristics.

### 3.2. The Model

Based on the foregoing, the proposed model is as shown in APPENDIX 5c., with its components in APPENDIX 5a, and APPENDIX 5b.

It is to be noted that the arrows in the diagrams are not indicative of processes. The model is causal in that an arrow from A to B postulates that A causes B, i.e. increasing A increases or decreases B, unlike in a process model where such an arrow would postulate that B follows A.

This study is based on five existing well-founded models relating to technology acceptance and information systems success. These are: the most current version of the Technology Acceptance Model (TAM3) (Venkatesh and Bala, 2008), the Diffusion of Innovation (DOI), (Rogers, 1995), the User Motivation, (Davis et al., 1992), The Benefits Evaluation Framework and the Updated Information Systems Success Model (also known as the Delone & Maclean Model) (Delone and Maclean, 2003).

The theoretical model of this research draws on these models, but combines selected elements of each, along with some additional factors, to present an integrative and holistic picture of behavioral intentions to adopt, the adoption and continued use of e-government services by individuals, groups, organizations (internal and external), and the society at large. It draws on the Theory of Reasoned Action (TRA), (Fishbein and Ajzen, 1975), as well as the Theory of Planned Behaviour (TPB), (Ajzen, (1985, 1991)).

The focus is on e-government services although the model should apply mutatis mutandis to other services, technologies or innovations. This focus is informed by the fact that it has been shown Adams et al., 1992; Im et al., 2008), that in TAM and its variants the type of technology under consideration for adoption impacts on the antecedents of adoption. For example (Adams et al, 1992) compared five technologies, and demonstrated that TAM variables worked differently depending on whether email, voice mail, word processor, spreadsheets or graphics software was in question, concluding that the impact of perceived ease of use decreases as experience with a technology increases. A similar study, (Karahanna and Limayem, 2000), compared email and voicemail, and concluded that there are important differences between antecedents of e-mail and v-mail usage, in both the determinants of system use and in the determinants of Perceived Usefulness and Perceived Ease of Use. Relatively recently, Styliano and Jackson, (Styliano and Jackson, 2007) compared the Internet and e-commerce, and found that different factors informed decisions to adopt each. Curran and Meuter, (Curran and Meuter, 2005) compared consumer attitudes towards and adoption of three different self service technologies in banking, considering perceptions of use, usefulness, risk, and need for interaction, and noted. that the impact of the antecedent beliefs varied according to the technology.

### *3.2.1. Model Constituents And Conceptual Views*

The model comprises of the integration of the TAM3 model which is itself composed of the User Motivation and the DOI, with the BEF. It provides three conceptual views of the key dimensions involved in the adoption and continued use of the e-government services: the micro, meso and macro views.

The micro view addresses the quality of the information, system and services associated with e-government, the use of the services, the user satisfaction, and the net benefits in terms of the positive impact on the user, of the patronage of the aforementioned services.

The meso view addresses the dimensions involving the individual, groups, the organization (internal and/or external), the government and the society at large (volitional e-government services use) that have a direct effect on the micro-level.

The macro view addresses the standards and guidelines, infrastructure, funding and incentives, legislation/policy and governance, societal/political/economic trends, hedonic/utilitarian disposition, and the security/privacy intrusiveness and/or interventions as contextual factors that have direct influence on the extent to which the meso dimensions can affect e-government services adoption, use and continued use. At each level, there is a feedback loop where the adoption efforts and results can reshape the higher-level views.

The premise here is that success in e-government services adoption and continued use requires explicit recognition, strategies and actions to address the respective micro-, meso- and macro-dimensions in the model.

The variables involved: MICRO-, MESO-, and MACRO-, are now described briefly hereunder.

(a) MICRO VIEW VARIABLES

Six variables that have been identified as coming into play in the micro-view are the following

1. Perceived Usefulness, Perceived Ease Of Use, Attitude Toward Use, And Behavioral Intention To Use: The variables of perceived usefulness (PU), perceived ease of use (PEOU), attitude toward use (ATU), and behavioural intention to use (BIU) are employed in the model because not only do they feature prominently in the existing models being integrated they have also proven to be of irrefutable value in research work relating to the models.
2. Compatibility: The DOI construct of compatibility is included as it has proven particularly relevant to this field. The DOI concepts of relative advantage and complexity relate strongly to TAM's PU and PEOU and have therefore not been included separately.
3. Trust, Perceived Risk, Concern For Security: The additional variables that have been introduced are trust, perceived risk and concern for security, whose importance has been widely argued (Pavlou, 2003; Chen and Tan, 2004; Gefen and Straub, 2003), as well as concern for security (data privacy) and innovativeness. The additions are influenced by findings that consider them necessary. It has even been suggested in some works that they may have a greater effect on individual behaviour than the original TAM variables of PU and PEOU (van der Heijden and Verhagen, 2004; Ha and Stoel, 2009).
4. System Quality, Information Quality And Service Quality: The variables system quality, information quality, and service quality, are employed. They are common to the TAM3 and the IS Success models, as well as the user satisfaction and net benefits. They refer to the accuracy, completeness and availability of the e-government information content; features, performance and security of the system; and responsiveness of the support services, and are critical in determining whether or not the expectations have been met.

5. Usage And User Satisfaction: These refer to e-government services usage intention/pattern and user satisfaction in terms of usefulness, ease of use and competency.
6. Net Benefit: This refers to the positive impact as a result of the e-government services adoption by various classes of consumers: individuals, groups, organizations (internal and/or external), the government and the society. (the constructs of group and organization (Internal) and organization (External) in place of just organization, as well as Groups were introduced in (Kurian et al, 2000) the latter distinguishing between internal organizational impact and impact on parties external to the organization that interact with the organization and its agents). E-government quality includes safety, security, privacy, appropriateness/effectiveness/efficiency and outcomes. Benefits include access – service provider/merchant/consumer participation and availability/access to services, as well as productivity, which covers e-government services coordination, efficiency and net cost.

(b) THE MESO-VIEW VARIABLES

The meso view addresses the dimension involving the following:

1. The Individual/Group: The individuals/groups involved, their personal characteristics and expectations and their roles and responsibilities with the e-government services
2. Organization (Internal): The organization involved in decisions relating to the adoption and continued use of the e-government services, how the services fit with the internal organizational strategy, culture, structure/processes, info-/infrastructure and return on value.
3. Organization (External): This is same as the above but relates to parties external to the organization which interact with the organization and/or its agents
4. The Government: The government as a provider and user of e-government services
5. The Society: The society as users, for example, the volitional use of e-government services.

(c) THE MACRO - VIEW

Seven variables that have direct influence on the adoption, use and usage success of e-government services are considered. These are:

1. Security And Privacy Intrusiveness And Interventions: This is the degree to which the e-government services could potentially trespass on or abuse the sensitive data, bodily integrity, self-determination or private life of the user, as well as possible interventions. The significance of the perceived intrusiveness of a technology has been particularly discussed, for instance in relation to electronic identification, in LAM (Xu et al., 2011), biometrics (Andronikou et al., 2005; Shaikh and Rabaiotti, 2010) and RFID (Muller et al., 2009; Ohkubo et al., 2005).
2. Standards: Standards here refer to the types of e-government services, organizational performance, practice standards and guidelines in place. These impact on decisions for adoption and continued use of the services, and are also shaped by the feed back from observations, experiences, and reports regarding the use of the services.
3. Funding And Incentives: These are to the added values, remunerations and incentive programs, and the provisions to engender the adequacy of the infrastructure.
4. Legislation/Policy And Governance: These are legislative acts, regulations /policies, and governance bodies such as professional associations/colleges and advocacy groups and their attitudes toward e-government services. It has been indicated, (Benbasat et al., 2008), that these variables can indeed moderate the feelings of mistrust and hence be promoting influences to adoption.
5. Societal, Political And Economic Trends: Included here are public expectations and the overall socio-political and economic climates with regards to technologies and e-government services.
6. Hedonism/Utilitarianism : The consideration here is whether the e-government technology and/or the related service it brings are hedonic or utilitarian The distinction between hedonic and utilitarian systems (first established in Babin et al., 1994) is used here to define those engagements with the technology or service, which are motivated principally by enjoyment as hedonic, and those undertaken in a directly instrumental spirit as utilitarian. Although this dichotomy is a simplified representation of real-world experiences which often combine elements of the two, the spectrum of completely hedonic to completely utilitarian uses of the e-government technology and/or its related services is highly relevant to the processes through which they are adopted or rejected by consumers. Therefore, hedonism and utilitarianism are included in the variables list, as done in (Childers et al., 2001), Im et al., 2008), (van der Heijden and Verhagen, 2004) noting that in evaluating their influence the methodology encompasses a range of possible positions along the aforementioned spectrum.
7. Familiarity With The E-Government Sercices: The familiarity of the general public with the e-government technology itself or with the services enabled by it i.e. whether or not the e-government technology or the service it enables is already well-established. In this work, the concept of familiarity refers to the level of previous experience and knowledge present in the general public regarding the technology used or the services. A number of studies has demonstrated that this is a relevant factor in technology adoption (e.g. (Hackbarth et al., 2003; Lippert and Forman, 2005).

## 4. CONCLUSION AND FUTURE WORK

Individuals, groups, organizations, the government and indeed the society at large are all leveraging on the advances and offerings of information technology for competitiveness. Exemplary practices in e-government and the quality of the services it offers are revolutionizing not just technology itself but the whole process through which e-government services are provided, and thereby stimulating appetites for the adoption, use and continued use of those services. This work presents a conceptual model to facilitate decisions on adoption and continued use of the services. It bridges the conceptual gap between the beliefs and attitudes about e-government services and those about using the services. This engenders realizing the benefits indicated in the arguments for the integration, helps to better understand e-government and identifies various competence factors like infrastructure, managerial, political, user and security and privacy intrusiveness and intervention, which influence e-government adoption and continued use. This conceptual model can be empirically tested as it provides researchers a framework with which to do an empirical examination on the identified factors of e-government with its performance. It would also help individuals, groups, organizations, the government and the society in deciding to what extent they should invest in e-government by matching the e-government attributes to their own characteristics.

As to the future direction, the model will be subjected to empirical tests using various scenarios, and will also be refined as appropriate for other initiatives such e-payment that is now topical in this environment.

## REFERENCES

Adams, D. A., Nelson R. R, and Todd, P. A. (1992). Perceived Usefulness, Ease of Use, and Usage of Information Technology: A Replication, MIS Quarterly 16 (2) (June), 227.

Ajzen, I., Fishbein, M. (1980), Understanding Attitudes and Predicting Social Behavior. Prentice-Hall, Englewood Cliffs, NJ

Ajzen, I. (1985). From intentions to actions: A theory of planned behavior. In J. Kuhl & J. Beckmann (Eds.), Action-control: From cognition to behavior (pp. 1 l-39). Heidelberg: Springer.

Ajzen, I., (1991), The Theory of Planned Behavior Organizational Behavior And Human Decision Processes 50, 179-211.

Ajzen I, Fishbein, M (2005), Influence of Attitudes on Behavior, The Handbook Of Attitudes, 2005 - Psychology Press, pp 173-221

Andronikou, V., Demetis, D. S., & Varvarigou, T., (2005), Biometric implementations and the implications for security and privacy. Journal of the Future of Identity in the Information Society, 1(1), 20-35.

Babin, Barry J., William R. Darden, and Mitch Griffin, (1994), Work and/or Fun: Measuring Hedonic and Utilitarian Shopping Value." The Journal of Consumer Research 20 (4) (March 1), 644-656.

Benbasat, I., R. Zmud. 2003. The identity crisis within the IS discipline: Defining and communicating the discipline's Coir properties. MIS Quart. 27(2) 183–194.

Benbasat, Izak, David Gefen, and Paul A. Pavlou, (2008), Special Issue: Trust in Online Environments. Journal of Management Information Systems 24 (4) (April), 5-11.

Chen, Lei-Da, and Justin Tan. 2004, Technology Adaptation in E-commerce: Key Determinants of Virtual Stores Acceptance, European Management Journal 22 (1) (February), 74-86

Childers, T. L., Carr, C. L., Peck, J., and Carson, S., (2001), Hedonic and utilitarian motivations for online retail shopping behavior. Journal of Retailing 77, 4, 511-535.

Curran, J M., and Meuter, M. L. (2005),. Self-service technology adoption: comparing three technologies. Journal of Services Marketing 19, 2, 103-113.

Davis, F. D., Bagozzi, R. P., and Warshaw, P. R. 1989. "User Acceptance of Computer Technology: A Comparison of Two Theoretical Models," Management Science, 35, 982-1003.

Davis, F. D., Bagozzi, R. P. and Warshaw, P. R., (1992), "Extrinsic and Intrinsic Motivation to Use Computers in the Workplace," Journal of Applied Social Psychology, vol. 22, no. 14, pp. 1111 - 1132, 1992.

DeLone, W. H., McLean, E. R. (1992) Information systems success: The quest for the dependent variable. Information Systems Research, 3(1), 60-95.

DeLone, W. H., McLean, E. R. (2003) The DeLone and McLean Model of Information systems success: A Ten-Year Update Journal of Information Systems, Spring, Vol.19, pp.9-30

Eagly, A. H., S. Chaiken. (1993). The Psychology of Attitudes. Thomson Wadsworth, Belmont, CA.

Fazio, R. H., M. A. Olson. (2003). Attitudes: Foundation, function and consequences. M. A. Hogg, J. Cooper, eds. The Sage Handbook of Social Psychology. Sage, London, UK.

Fishbein & Ajzen, (1975). Belief, attitude, intention, and behavior: An introduction to theory and research. Addison-Wesley Pub. Co. (Reading, Mass.)

Gefen, D, Straub, D.W., (2004) Consumer trust in B2C e-Commerce and the importance of social presence: experiments in e-Products and e-Services, Omega, 32 (6), 407–424.

Goodhue, D. L. (1988). IS attitudes: Toward theoretical and definitional clarity. Database Adv.Inform.Systems 19(3/4) 6–15

Ha, S, and Stoel, L., (2009), Consumer e-shopping acceptance: Antecedents in a technology acceptance model, Journal of Business Research 62 (5) (May), 565-571

Hackbarth, G., Grover, V., and Yi, M. Y., (2003), Computer playfulness and anxiety: positive and negative mediators of the system experience effect on perceived ease of use, Information & Management 40 (3), 221–232

Haddock, G., M. P. Zanna. (1999). Cognition, affect, and the prediction of social attitudes. W. Stroebe, M. Hewstone, eds. Eur.Rev . Soc.Attitudes 10 75–99..

Hartwick, J., H. Barki. (1994). Explaining the role of user participation in information system use. Management Sci. 40(4) 440–465

Im, I., Kim, Y., and Han, H., (2008), The effects of perceived risk and technology type on users' acceptance of technologies, Information & Management 45, no. 1 (January), 1-9.

Karahanna, E, and Limayem, M..(2000). E-Mail and V-Mail Usage: Generalizing Across Technologies,. Journal of Organizational Computing and Electronic Commerce 10, 1, 49.

Kurian, D., Gallupe, R. B., Diaz , J., (2000), Taking Stock: Measuring Information Systems Success, Proceedings ASAC-IFSAM 2000 Conference Montreal, Quebec2000 pp 1-14

Lippert, S. K, and Forman, H., (2005), Utilization of information technology: examining cognitive and experiential factors of post-adoption behavior, IEEE Transactions on Engineering Management 52 (3) (August), 363- 38

Melone, N. 1990. A theoretical assessment of the user-satisfaction construct in information systems research. Management Sci. 36(1) 76–91.

Müller-Seitz, Gordon, Kirsti Dautzenberg, Utho Creusen, and Christine Stromereder. 2009. Customer acceptance of RFID technology: Evidence from the German electronic retail sector, Journal of Retailing and Consumer Services 16 (1) (January), 31-39.

Nour-Mohammad Y, Sedighe H. B. B and Roghaye Z, (2011), A Survey on Factors Effecting Continuity the Use of Government' E-Services, Australian Journal of Basic and Applied Sciences, 5(8): 209-220, 2011.

Ohkubo, Miyako, Koutarou Suzuki, and Shingo Kinoshita. (2005). RFID privacy issues and technical challenges, Communication of the. ACM, 48 (9) (September), 66–71.

Orlikowski, W. J., C. S. Iacono. 2001. Research commentary: Desperately seeking the "IT" in IT research - A call to theorizing the IT artifact. Inform.Systems Res. 2(12) 121–134.

Özkan Sevgi, Bilgen Semih (2003), Notes Towards Information Systems (IS) Success: A Literature Review And Comparison Of Two IS Success Models Within The Context Of The Internet, Proc International Conference WWW/Internet 2003 pp 1215-1218

Pavlou, P. A., (2003), Consumer Acceptance of Electronic Commerce: Integrating Trust and Risk with the Technology Acceptance Model, International Journal of Electronic Commerce 7 (3), 101-134

Rogers, E. M. (1995). Diffusion of innovations. Simon and Schuster.

Scialdone, Michael J., and Ping Zhang. (2010), "Deconstructing Motivations of ICT Adoption and Use: A Theoretical Model and its Application to Social ICT.", iConference 2010 Papers, Ideals.

Seddon, P. (1997). A respecification and extension of the DeLone and McLean model of IS success. Inform.Systems Res. 8(3) 240–253.

Shaikh, S. A, and Rabaiotti, J. R,.(2010). Characteristic trade-offs in designing large-scale biometric-based identity management systems. Journal of Network and ComputerApplications. vol. 33, no. 3, 2010, Pages: 342-351

Styliano A. and Jackson P. 2007. A comparative examination of individual differences and beliefs on technology usage: Gauging the role of IT, Journal of Computer Information Systems. 47.4 pp 11-18.

Taylor, S., Todd, P. (1995). Decomposition and crossover effects in the theory of planned behavior: a study of consumer adoption intentions', International Journal of Research in Marketing, 12: 137-155.

Van der Heijden, H, and Verhagen Tibert, (2004), Online store image: conceptual foundations and empirical measurement, Information & Management 41 (5) (May), 609-617.

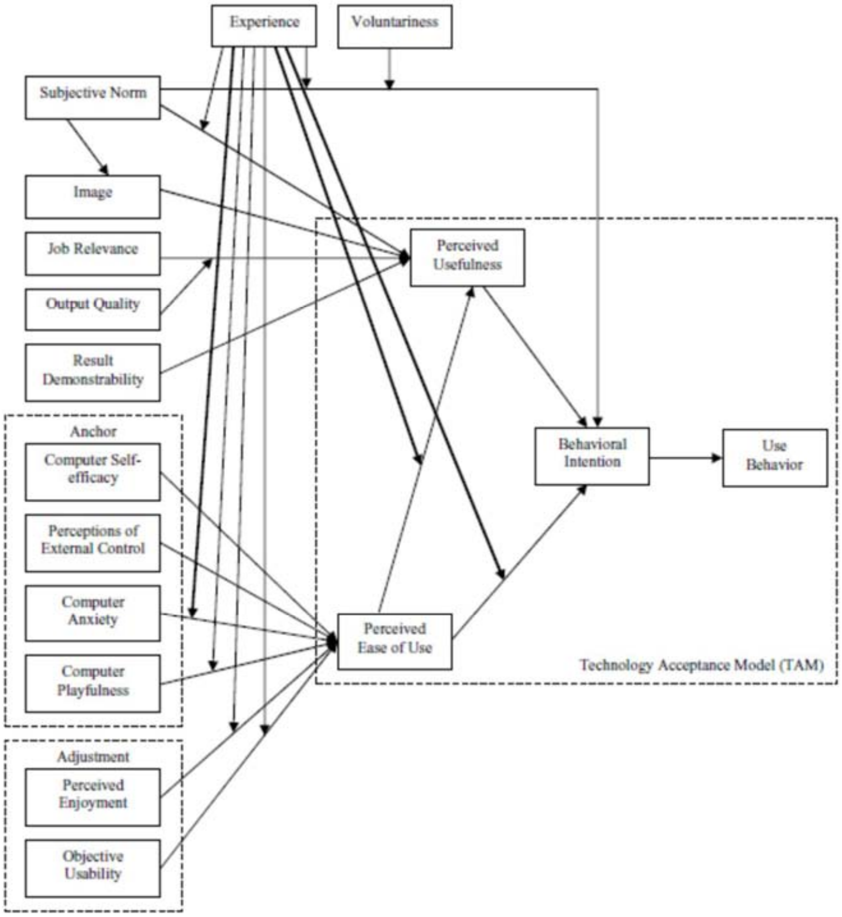
Venkatesh, V and Bala, H, (2008), Technology Adoption Model 3 and a Research Agenda on Interventions, Decision Sciences Vol 39 No. 2 2008 pp 273-315.

Wixom, Barbara H., Todd, Peter A. (2005), A Theoretical Integration of User Satisfaction and Technology Acceptance, Information Systems Research Vol. 16, No. 1, March 2005, pp. 85–102.

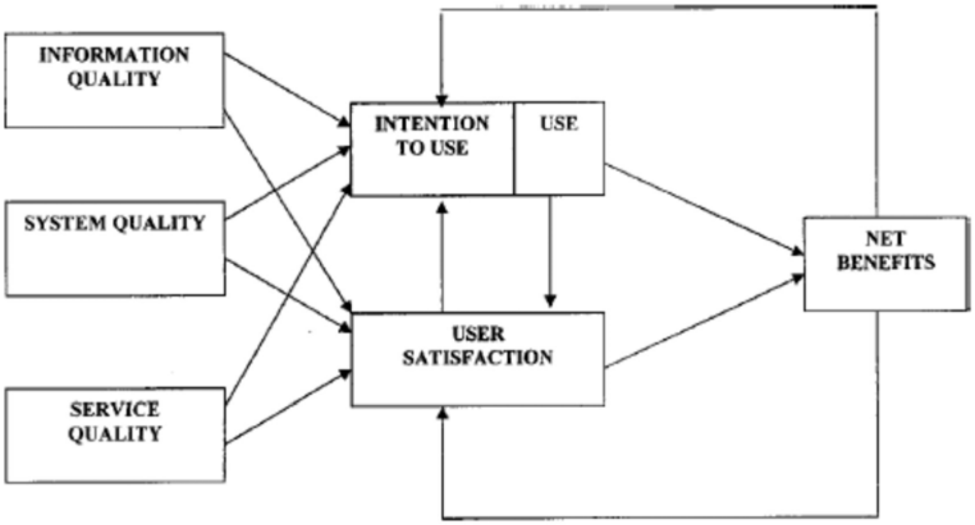
World Bank (2011), Definition of E-Government, available at: http://go.worldbank.org/M1JHE0Z280 (accessed 10 September 2011).

Xu, H, Luo, X. R, Caroll, J. M., and Rosson, M. B., (2011). The personalization privacy paradox: An exploratory study of decision making process for location-aware marketing Decision Support Systems 51 (1) (April), 42-52.

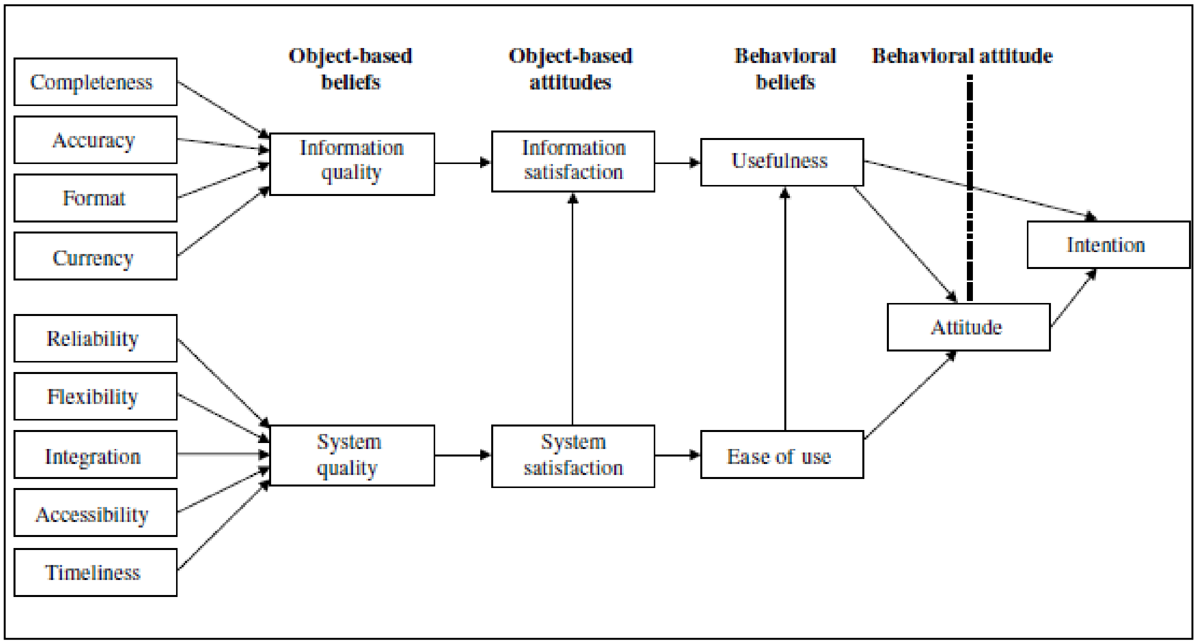
## APPENDICES



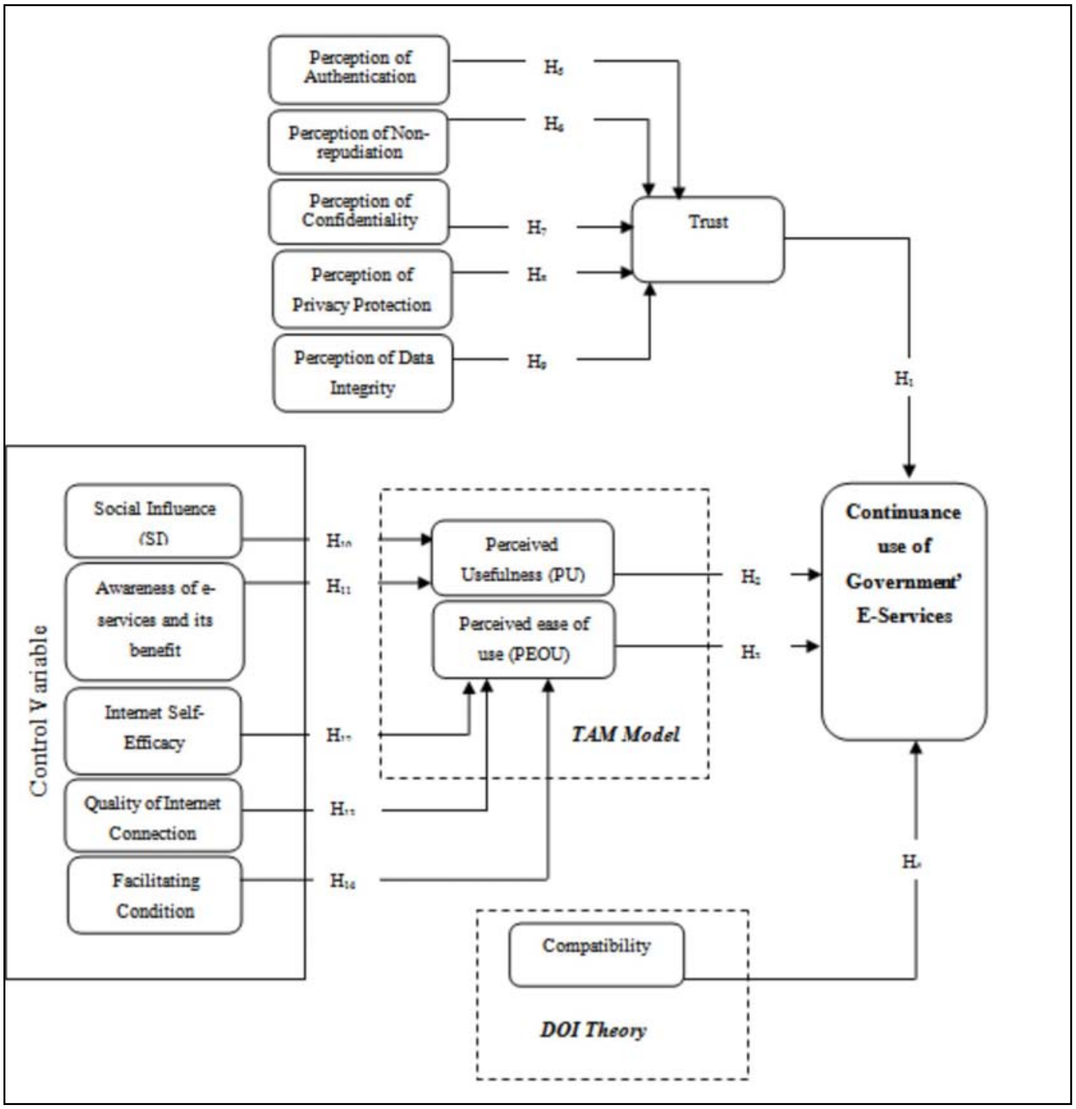
*APPENDIX 1: The Technology Acceptance Model (TAM 3)*
*(Source: (Venkatesh and Bala, 2008)),*



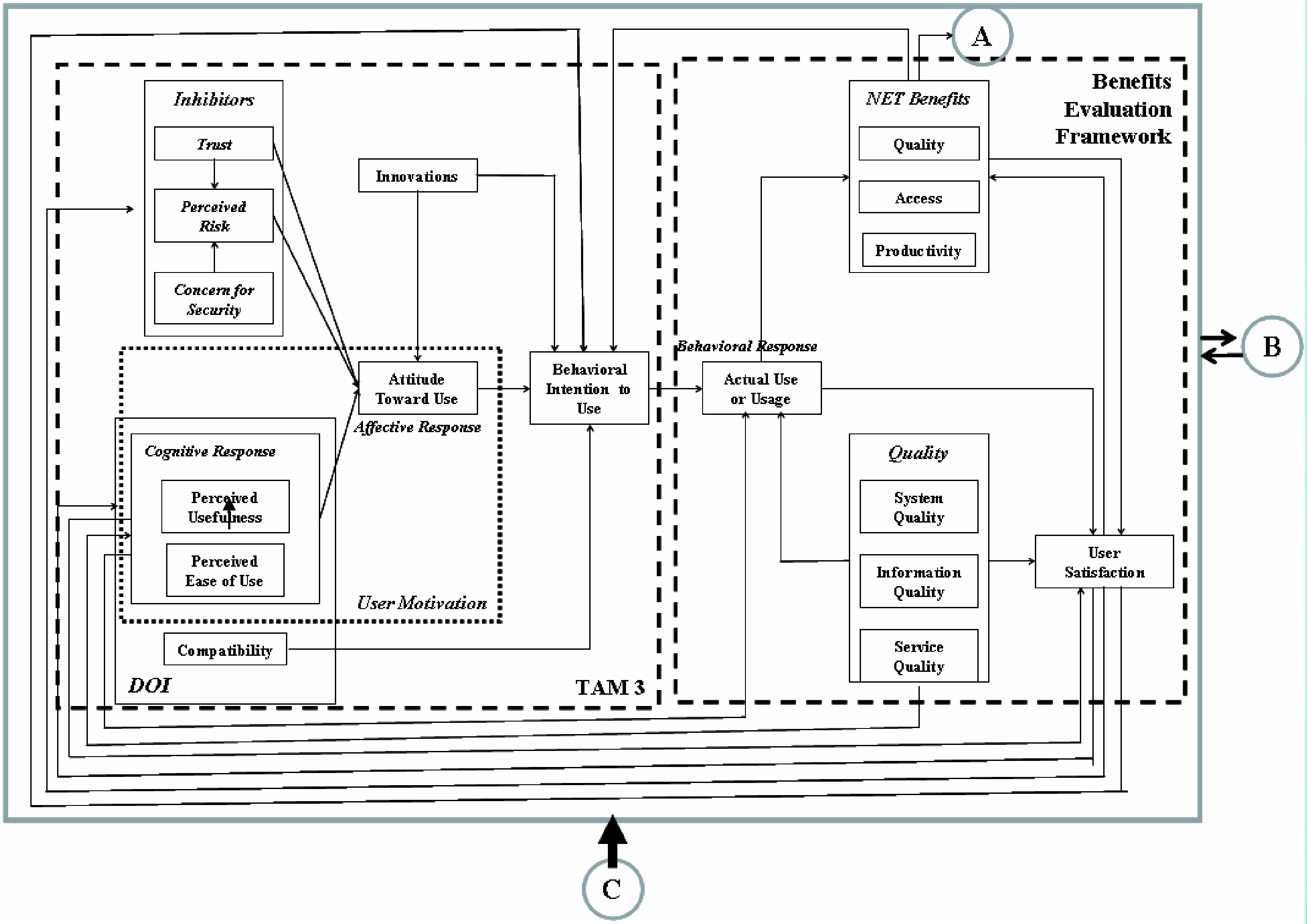
APPENDIX 2: The Updated Delone and McLean Model
(Source: (Delone and McLean, 2003))



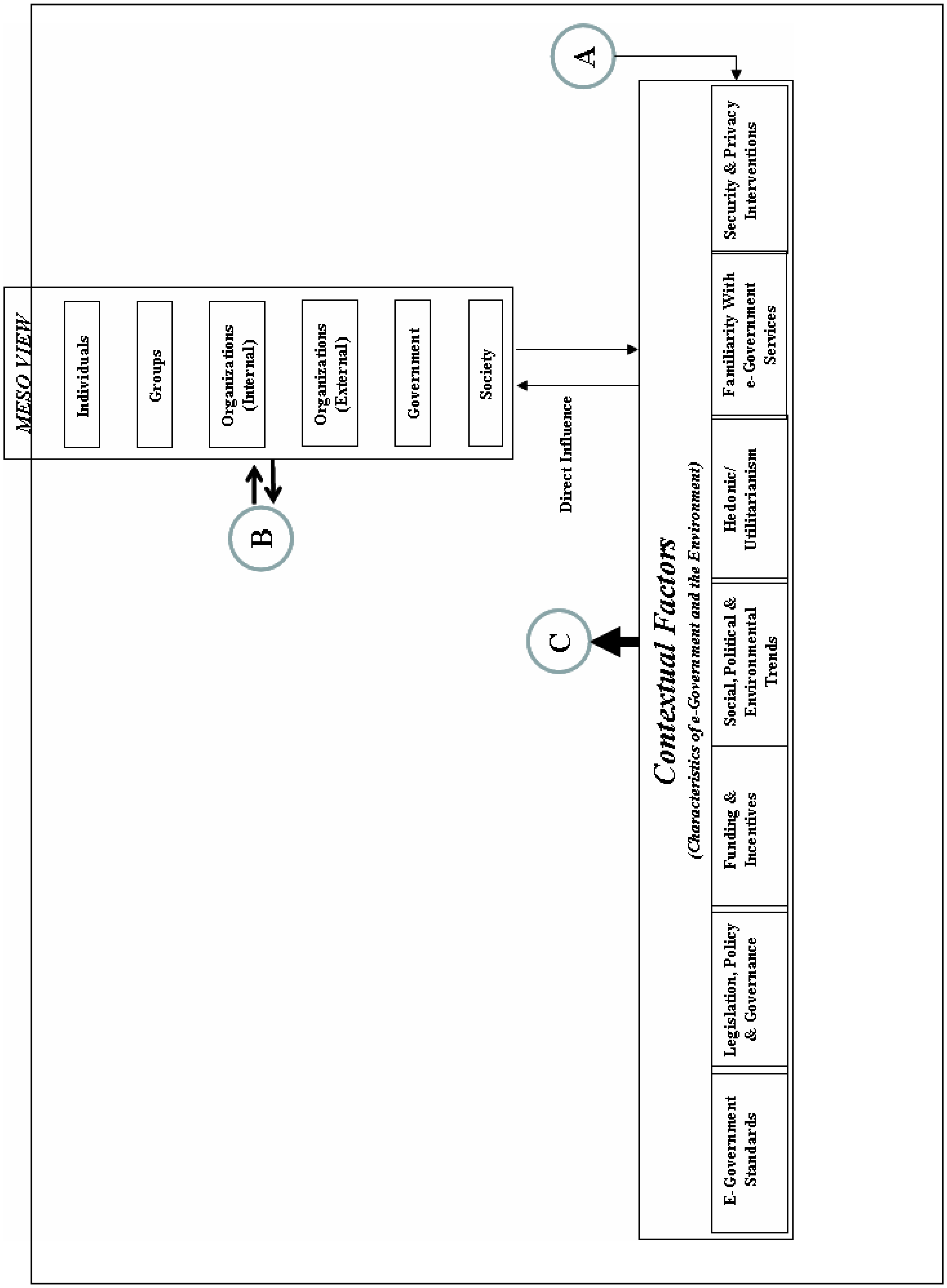
APPENDIX 3: The Wixom and Todd ‘s Model
(Source: (Wixon and Todd, 2005))


Perception of Authentication
$H_5$
Perception of Non-repudiation
$H_6$
Perception of Confidentiality
$H_7$
Perception of Privacy Protection
$H_8$
Perception of Data Integrity
$H_9$
Trust
$H_1$
Control Variable
Social Influence (SI)
Awareness of e-services and its benefit
Internet Self-Efficacy
Quality of Internet Connection
Facilitating Condition
$H_{10}$
$H_{11}$
$H_{12}$
$H_{13}$
$H_{14}$
Perceived Usefulness (PU)
Perceived ease of use (PEOU)
TAM Model
$H_2$
$H_3$
Continuance use of Government' E-Services
$H_4$
Compatibility
DOI Theory

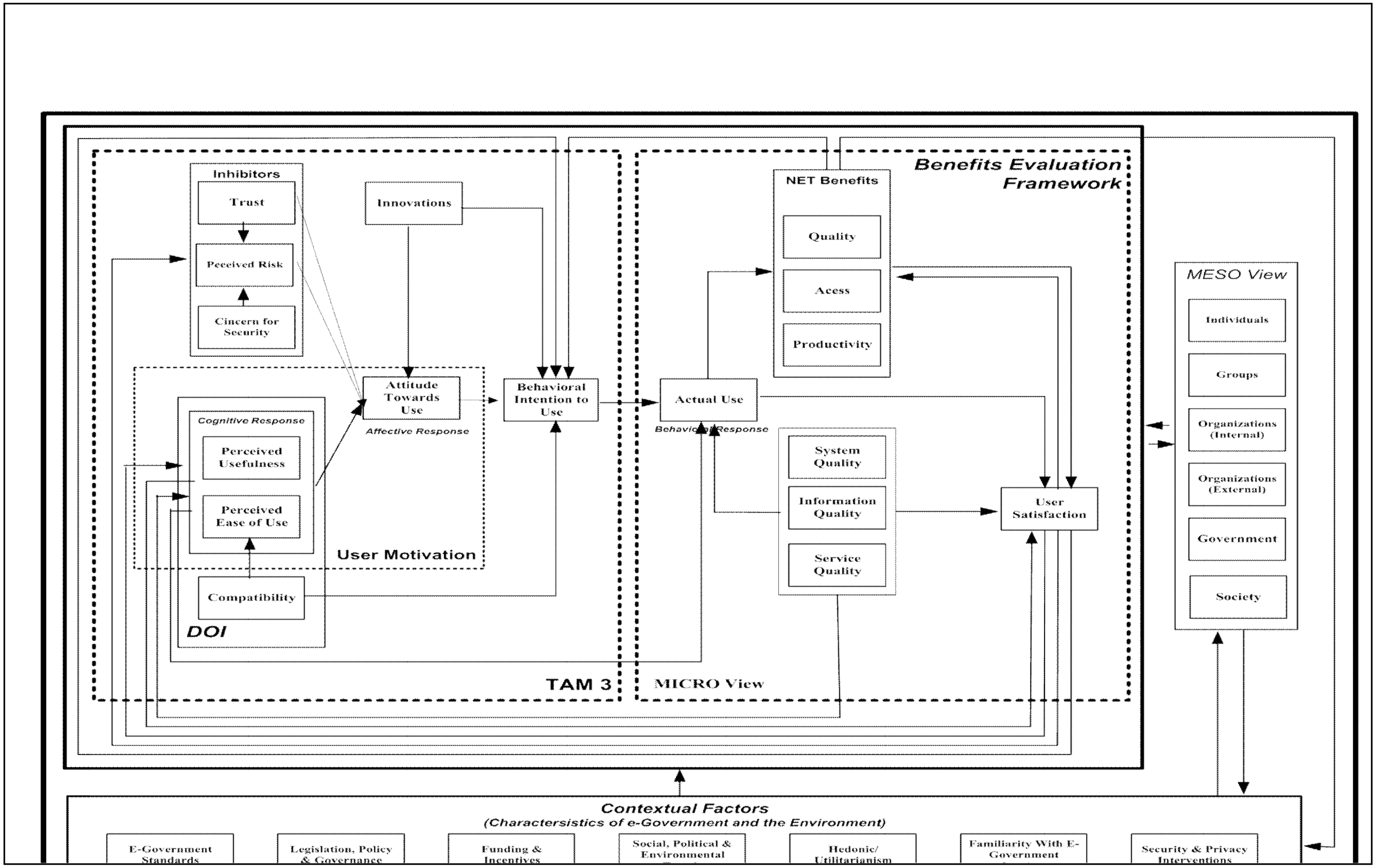
*APPENDIX 4: The Nour-Mohammad et al Model*
*(Source: (Nour-Mohammad et al, 2011))*


A
B
C
Inhibitors
Trust
Perceived Risk
Concern for Security
Innovations
Attitude Toward Use
Affective Response
Behavioral Intention to Use
Cognitive Response
Perceived Usefulness
Perceived Ease of Use
User Motivation
Compatibility
DOI
TAM 3
Behavioral Response
Actual Use or Usage
Benefits Evaluation Framework
NET Benefits
Quality
Access
Productivity
Quality
System Quality
Information Quality
Service Quality
User Satisfaction

*APPENDIX 5a: The MICRO View of the Proposed Model*


A
MESO VIEW
Individuals
Groups
Organizations (Internal)
Organizations (External)
Government
Society
B
Direct Influence
C
Contextual Factors
(Characteristics of e-Government and the Environment)
Security & Privacy Interventions
Familiarity With e-Government Services
Hedonic/ Utilitarianism
Social, Political & Environmental Trends
Funding & Incentives
Legislation, Policy & Governance
E-Government Standards

*APPENDIX 5b: The MESO and MACRO Views of the Proposed Model*


Inhibitors
Trust
Peceived Risk
Cincern for Security
Innovations
Attitude Towards Use
Affective Response
Behavioral Intention to Use
Cognitive Response
Perceived Usefulness
Perceived Ease of Use
User Motivation
Compatibility
DOI
TAM 3
Benefits Evaluation Framework
NET Benefits
Quality
Acess
Productivity
Actual Use
Behavioral Response
System Quality
Information Quality
Service Quality
User Satisfaction
MICRO View
MESO View
Individuals
Groups
Organizations (Internal)
Organizations (External)
Government
Society
Contextual Factors
(Charactersistics of e-Government and the Environment)
E-Government Standards
Legislation, Policy & Governance
Funding & Incentives
Social, Political & Environmental
Hedonic/ Utilitarianism
Familiarity With E-Government
Security & Privacy Interventions

*APPENDIX 5c: The Proposed Model with All the Components*

Full Paper

# A FUZZIFIED DECEPTION DETECTION SYSTEM

**O.Iyare***
Federal University of Technology, Akure
*oiyare@futa.edu.ng*

**B. K. Alese**
Federal University of Technology, Akure
*kaalfad@yahoo.com*

**O.S. Adewale**
Federal University of Technology, Akure
*adewale@futa.edu.ng*

**S. O. Falaki**
Federal University of Technology, Akure
*swolefalaki@yahoo.com*

**ABSTRACT**

The development of a fuzzy approach in law enforcement agencies has a wide range of application to intelligence analysis during interrogation and evidence gathering in the face of investigation. The ability of these methods to mitigate attempted deception by an informant or suspect is affected by many factors including the choice of analytical method, the type of hybridization used, and the ability to address issues of source reliability and information credibility. This work at the end will presents a hybrid system of verbal and non-verbal deception indicators using fuzzy system to aid in the detection of deception during interrogation.

**Keywords**: *Interrogation, Investigation, Deception, Suspect, Witness.*

## 1. INTRODUCTION

An aspect of deception (apart from being an intentional act) is that it is defined solely from the perspective of the deceiver and not from the factuality of the statement. The importance of deception and its detection during interrogation in law enforcement is beyond any doubt. This is acknowledged by authors who have worked on the subject and who understand that false testimonies may corrupt the proper functioning of the law enforcement system (Simon et al, 2006). Hence, human ability to detect deception simply by observing the sender's behaviour is far from perfect.

Deception in its entirety includes several types of communications or omissions that serve to distort or omit the complete truth. In itself, Deception is intentionally managing verbal and/or nonverbal messages so that the message receiver will believe in a way what the message sender knows is false (Jaume et al, 2004).

There are many reasons according to (Vrij, 2008) why lies remain undetected, and they can be clustered into: Poor motivation, Difficulties associated with lie detection and Common error made by lie detector. Another reason is that people do not often attempt to detect them because they do not want to learn the truth; this phenomenon was labelled the ostrich effect in (Vrij, 2008). Also, people sometimes do not investigate whether they have been lied to because they fear the consequences the truth may hold and lastly, people are afraid to detect lies because they would not know what to do if they know the truth. In law enforcement and security outfits, knowing the truth is paramount to the success of its operation.

Evidence can be an object or information used as a proof of guilt or a statement of witnesses to ascertain or establish the truthfulness of a fact while evidence gathering is the collection of these proof or statement of witnesses to resolve the issues surrounding a case. The information needed to further an investigation must be obtained from people who have some significant knowledge concerning the crime. Witnesses or victims are interviewed, and suspects are interrogated. In criminal cases, eyewitnesses to a crime are often asked to identify the perpetrator and different people who have witnessed the same event may recall the event somewhat differently from each other, and sometimes their statements may even be contradicting. It could thus be that none of the witnesses are lying but that at least one of them misremembers the event.

Interrogation is used when the information sought is not readily forthcoming, perhaps because of hostility or guilt. Often some key to the solution of a crime, such as the location of the weapon in a murder case, is known only to the perpetrator. Without the right information provided by the suspect, a crime may go unsolved and in another case innocent citizens can be apprehended, prolong investigations and concealment of the actual offender (Badiru et al, 2005).

Information gathered during interrogation of suspect or eyewitness testimony is of uttermost importance to any investigation therefore the certainty that the information gotten is not deceptive is of paramount benefit. The system proposed will be such that generate rules that will be used to classify the verbal information and non-verbal responses of the suspect into deceptive or truthful statement/evidence. To detect the applicability of the information gathered, the techniques of the system will be applied to discover, identify patterns and make predictions so as to make the law enforcement more efficient.

In current law-enforcement computer systems, police officers run exact-match queries to locate any historical data about a suspect. Vrij (2000) summarized three ways of detecting lies in law enforcement. The first method is to observe liars' non-verbal behaviour, such as their body movements (e.g., scratching the head), their emotional expressions, their facial expression (e.g., blinking of the eyes), and vocal characteristics (e.g., pitch of voice). Non-verbal cues to deception are more likely to occur if the lie is difficult to fabricate (Vrij, 2000). The emotional fluctuation caused by the action of lying will influence one's behaviour, which could expose deception. The second method is to analyze verbal characteristics of what a subject said. Vrij (2000) defined several types of verbal characteristics including negative statements, plausible answers, irrelevant information, over-generalized statement, self-references, and response length. Verbal cues can help to discriminate between deceptive and truthful statements in the sense that some verbal criteria are more likely to occur in false rather than in truthful statements. The third way is to examine physiological responses such as blood pressure, heart rate, palm sweating and respiration.

Forming a hybrid of verbal and non-verbal cues can go a long way in helping law enforcement officers to effectively detect deception during interrogation. The hybrid system will rely on the principles of fuzzy system in formulating the rules that will classify information as deceptive or truthful statement.

## 2. FUZZY SYSTEM

Fuzzy logic, a superset of the conventional Boolean logic, is used for handling the concept of partial truth (truth value between truth and deception), a situation where the deceiver use an event that has happened previously to deceive. It provides a simple way to draw definite conclusions from vague, ambiguous or imprecise information (Akinyokun, 2002). In the real world, the universe of discourse does not have sharply defined boundaries for example, many, tall, much larger than and young are true or false only to some degree unlike in conventional classical set theory where it is either true or false and yes or no. The concept of a fuzzy set has been employed to extend classical sets, which are characterised by crisp boundaries (Masuoka et al, 1990). This addition permits a degree of flexibility for each object belonging to a particular set. This quality is realised by the definition of membership functions that give fuzzy sets the capacity of modelling linguistic, vague expression (Zadeh, 1965). Fuzzy reasoning realises a form of approximate reasoning that, using particular mathematical inferences, derives conclusions based on a set of fuzzy IF-THEN rules, where linguistic variables could be involved. Classical systems cannot cope with inexact or incomplete information, because they do not provide any means of representing imprecise propositions and do not possess any mechanism that can make an inference from such propositions.

Fuzzy logic systems commonly contain expert IF-THEN rules and can be characterised in terms of their fundamental constituents: fuzzification, rule base, inference, defuzzification (Castellano et al, 2001).

Fuzzification is a mapping from a crisp input space to fuzzy sets in a defined universe:

$U: x_l \in R$ Ÿ $X \in U \subset R^q$

Here x represents a crisp value and q is the number of fuzzy classes. The fuzzy sets are characterised by membership functions which portray the degree of belonging of $x_i$ to the values in U, μF (x): U Ÿ [0, 1]. The rule base is constituted by an ensemble of fuzzy rules and the knowledge is expressed in the following form: IF x> a AND x> b AND x>c THEN truth.

The fuzzy inference process can be described by starting with the definition of the membership functions μ (·) related to the $k^{th}$ fuzzy rule and evaluated for each input component of a sample vector x = ($x_{ik}$). The most commonly employed membership functions are the triangular and the Gaussian functions (Castellano et al, 2001).

Finally, the defuzzification process is used to reconvert the fuzzy output values, deriving from the inference mechanism, into crisp values (Castellano et al, 2001). The various components are shown in the figure 1.

## 3. MODEL

The proposed system is based on a combination of expert rules and fuzzy logic perception. It is based on the human deception mechanism: Verbal and Nonverbal. The verbal classes of cues and respective indicators are:

1. Speech Disturbances (number of words, number of verbs, number of sentences)
2. Longer Pauses (average sentence length, average word length, pausality)
3. High Pitched Voice (passive, active)

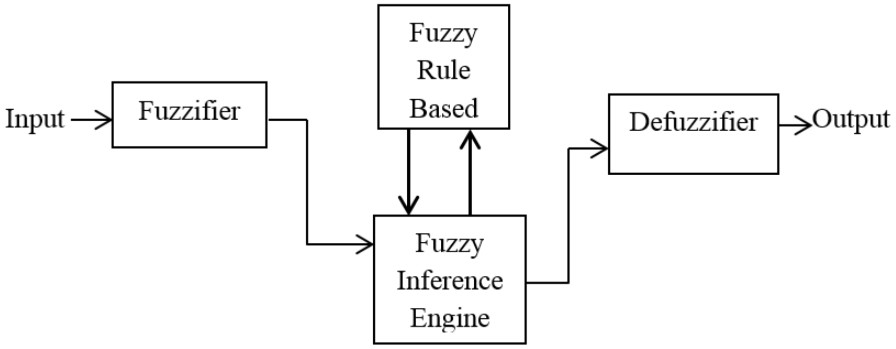


*Fig.1: The basic components of a fuzzy system (Source: Castellano et al, 2001).*

While the nonverbal classes of cues and their respective indicators are:

1. Eye Blinking (interval between the blink)
2. Facial movement (frequency of occurrence)
3. Leg Movement (rate of speed)

The set patterns of the verbal and nonverbal classes of cues are given below:

[illegible] ∈ [illegible] (1)

Where SD is Speech Disturbances, HPV is High Pitched Voice and LP is Longer Pauses.

[illegible] ∈ [illegible] (2)

Where EB is Eye Blinking, HS is Hand Shaking and LM is Leg Movement.

The verbal and nonverbal set will be used to form linguistic rules which will serve as membership functions of the fuzzy set.

The indicators are used to form the following membership functions:

$$\mathrm{Var}(x) = \begin{cases} \text{Truth} & \text{if } x \notin \{\text{ver } \Lambda \text{ nver}\} \\ \text{P.Truth} & \text{if } x \notin \{\text{ver } \vee \text{ nver}\} \\ \text{P.Deceptive} & \text{if } x \in \{\text{ver } \vee \text{ nver}\} \\ \text{Deceptive} & \text{if } x \in \{\text{ver } \Lambda \text{ nver}\} \end{cases}$$

Where P.Truth is partial truth, P.Deceptive is partial deceptive, ver is verbal and never is nonverbal.

The variable x takes on the values in the set {Truth, P.Truth, P.Deceptive and Deceptive} if x satisfy the stated conditions.

Give x as the baseline, (a, b, c) is as defined below: [illegible] ∈ [illegible],

[illegible] ∈ [illegible], [illegible] ∈ [illegible]

Let x = 0.5

$$\left\{ \begin{array}{ll} 0 & \text{if } x > a, b, c \\ {[0, 0.5]} & \text{if } x \geq a, b, c \\ {[0.6, 1]} & \text{if } x \leq a, b, c \\ 1 & \text{if } x < a, b, c \end{array} \right\}$$

From the above, it is deduced that there is deception if the value of x is 1 and the reverse is the case if the value of x is 0 which implies truth. If the value of x is close to 0 then there is partial truth and there is partial deception if the value of x is close to 1.

## 4. CONCLUSION

In conclusion, forming a hybrid of verbal and non-verbal cues of deception can go a long way in helping law enforcement officers to effectively detect deception during interrogation. This in turn will help in arresting the occurrence of innocent citizens going to jail and also hasten the process of investigation. Fuzzy rules was used in tackling the issue of partial truth and partial deception. For future, the model will be combined with the use of Neural Network to extend its functionalities.

## REFERENCES

Simon P, Audun J, and David M (2006). Formal Methods of Countering Deception and Misperception in Intelligence Analysis, Proceedings of the 11th International Command and Control Research Technology Symposium (ICCRTS'06), Cambridge, UK, 2006, pp 1-27.

Jaume M, Eugenio G, and Carmen H (2004). Defining Deception. Journal of anales de psicologia, vol 20 no. 1, pp 147-171.

Vrij A. (2008). Detecting lies and deceit, pitfalls and opportunity. Second edition. Wiley publisher, United Kingdom, 2008.

Badiru Adedeji B., Asaolu O. Sunday, Omitaomu Olufemi A. (2005) Eyewitness Information Management System Using Neuro-fuzzy Classification Schemes, Journal of Information Science and Technology, vol 2, number 3, USA.

Vrij, A. (2000). Detecting lies and deceit: The psychology of lying and the implications for professional practice. Chichester, Wiley publisher, United Kingdom, 2000.

Akinyokun O.C (2002). Neuro-Fuzzy Expert System for Evaluation of Human Resource Performance, a First Bank Endowment Fund Lecture delivered at the Federal University of Technology, Akure, pp 1-65.

Masuoka R., Watanabe N., Kawamura A., Owada Y., and Asakawa K. (1990). Neurofuzzy System- Fuzzy Inference using a Structured Neural Network. Proceedings of International Conference on Fuzzy Logic and Neural Networks, Japan. July 20-24, pp 173-177.

Zadeh LA (1965) Fuzzy Sets. Information and Control 8:338–353.

Castellano G., Castiello C., Fanelli A.M., and Jain L..(2001). Evolutionary neuro-fuzzy systems and applications, Computer Science Department, University of Bari, Italy.

Full Paper

# A SECURE DATA MINING FRAMEWORK FOR E-COMMERCE TRANSACTION

**O.O Bamgboye**
Department of Computer Science,
Moshood Abiola Polytechnic, Abeokuta, Ogun State
seunbamgboye2000@yahoo.com

**A.A Orunsolu**
Department of Computer Science,
Moshood Abiola Polytechnic, Abeokuta, Ogun State
orunsoluabiodun@yahoo.com

**M.A Alaran**
Department of Computer Science,
Moshood Abiola Polytechnic, Abeokuta, Ogun State
wmisturah@yahoo.com

**A.A Adebayo**
Department of Computer Science,
Moshood Abiola Polytechnic, Abeokuta, Ogun State
debamos04@yahoo.com

**A. Akinwunmi**
Department of Computer Science,
Federal University of Agriculture, Abeokuta, Ogun State.
5akintundeakinwunmi@yahoo.com

## ABSTRACT

ATM (Automated Teller Machine) is a recent trend in banking system in Nigeria, where customers interact with a machine to withdraw money or perform some other transactions (like fund transfer, phone recharge etc.). This is done to reduce the stress of queue in the bank and most importantly to provide conveniences in the withdrawal of money at any time and location by the customer. However, the opportunity has been misused by some people who commit fraud with this means. This has led to loss of confidence in this technology. In this paper, a data mining techniques was adopted to address this problem. This was achieved through the use of decision tree approach of data mining to formulate a pattern of transaction of any card user whenever a transaction is initiated. The decision tree models the location of transactions, time of transactions and amount involved in the transaction. The design was implemented using a Java programming language due to its portability, interoperability and scalability. The deployment of this financial institutions will increase customers' confidence in the e-services products.

**Keywords:** *ATM, Data Mining, Decision Tree, Fraud Detection* and Pattern Check

## 1. INTRODUCTION

The advent of electronic banking has marked a significant change in the way banks now approach the implementation of their transactions (withdrawal, loan, fund transfer etc). The use of Automated Teller Machine is one of the key ingredients of sound e-banking systems. The advantages of ATM are evident in the conveniences afforded customers to withdraw cash anytime and at any location. This makes shopping and financial services more accessible and more comfortable. To the banking institutions, the use of ATM reduces the cost overheads in terms of numbers of cashier needed to provide timely service.

However, electronic banking growth has been accompanied by an increase in sharp practices especially among fraudulent customers and bank workers who use such e-services. Such sharp practices have engulfed the domain of ATM transactions. The prevalence of ATM fraud especially in Nigeria has led to low confidence and acceptability of this novel technology among teeming banking customers. Most fraud committed with ATM Card is due to stolen card by close friends or relations who knows the Personal Identification Number (PIN) of the ATM card or when the card is used for any online transaction where the Card Number and Pin Number is required on an unsecured website. The card may then be simulated and used by another person since he or she now knows the PIN to the card.

Although many varied methods to fraud prevention are undertaken by organizations (Baker, 1999), the lack of any coordinated and uniform approach to the solution of these fraudulent activities has meant that the various deficiencies that exist across networked systems can be systematically exploited. The use of systems which are able to build customer transaction profiles and then use this knowledge to extract patterns of fraud, will be better able to adapt as patterns of attack inevitably evolve. Practical application of the technologies of data mining and detection algorithms, allow banks and switching company to identify and understand patterns of fraudulent practices, and then take effective action to combat these incidences (Lach, 1999). Data mining is a new technology that finds insights which are statistically reliable, unknown previously, and actionable from data (Elkan, 2001). This data must be available, relevant, adequate, and clean. In addition, the data mining problem must be well-defined, cannot be solved by query and reporting tools, and guided by a data mining process model (Lavrac et al, 2004).

Using the concept of data mining in predicting ATM Card fraud was achieved by formulating a transaction pattern of any ATM card User whenever a transaction is initiated by the user. The data mining application to predict the fraud is designed to check the new initiated transaction against the pattern formulated by the application. This application will raise an alarm whenever the new initiated transaction has deviated from the formulated pattern by the application up to 40% thereby asked a security question to verify the card user. The initiated transaction is allowed to continue if the card user answers the question correctly else the card will be detained for formal authentication and verification of the card.

The data mining application that predicts the fraud was achieved by using the decision tree algorithm of the data mining to formulate a pattern of transactions, taking into consideration three criteria time, location and amount of the transaction.

All the above three mentioned criteria are paired to formulate a tree of all possible transactions, on this tree a pattern of any customer transaction is derived, any imitated transaction is check against the pattern for any deviation or not.

## 2. RELATED WORKS

The purpose of fraud detection is to mitigate the cost of criminal transactions involving e-services. The notion of security of transaction is a key determinant for the continuous uptake of e-financial products and services (Orunsolu et al. 2012). The idea is to mine transaction system audit data for consistent and useful patterns of user transactional behaviour, and then keep these normal behaviours in profiles. Bose (2006) described a complete fraud detection process as consisting of data cleaning, feature selection and extraction, modelling and fraud action monitoring and prediction.

Francisca N. (2012) implemented a data mining technique in credit card fraud detection. The author designed a neural network (NN) architecture for the credit card detection system that was based on unsupervised method, which was applied to the transactions data to generate four clusters of low, high, risky and high-risk clusters. The self-organizing map neural network (SOMNN) technique was used for solving the problem of carrying out optimal classification of each transaction into its associated group, since a prior output is unknown. The receiver-operating curve (ROC) for credit card fraud (CCF) detection watch detected over 95% of fraud cases without causing false alarms unlike other statistical models and the two-stage clusters.

Priyadharshini et al., (2012) presented a data mining technique through a multilayered approach for providing the security for the credit card frauds. The first layer is communal detection and second is Spike detection layers that highly provides security for detection of frauds like probe resistant and mark the illegal user through their input details and mark it in a list. Then it removes attacks like defense in depths on cards and by removing the data redundancy of the attributes. The paper presented by Khyati et al., (2011) investigated the factors and various techniques involved in credit card fraud detection during/after transaction. In the study, various methods were used to build fraud detecting models. The use of Clustering was introduced as a data mining technique. The Fuzzy Darwinian fraud detection systems was introduced to improve the system accuracy, while neural network improve the method time to detect particular fraud termed as suspicious activity.

In the area of financial accounting fraud detection, Sharma and Panigrahi (2012) presented a comprehensive review of the literature on the application of data mining techniques for the detection of financial accounting fraud using logistics models, neural networks, Bayesian belief network and decision tree.

Orunsolu et al. (2012) investigated factors affecting the adoption of electronic banking in Nigeria. In a survey conducted by the authors, over 95% of the respondents perceived security of transaction as a key indicator in electronic service adoption. Over 60% of the respondents confirmed having negative experience with electronic transaction due to fraud. The implication is that there is a need for a secure framework that will forestall or mitigate the customers' negative experience.

## 3. DATA MINING FRAMEWORK FOR ATM FRAUD DETECTION

An ATM card transaction can be tracked basically with three criteria which are time of transaction, location of transaction and the amount involve in the transaction.

Three locations were chosen for the simulation of this research which is RegionA, RegionB, and RegionC using Nigeria as a case study, RegionA to be the northern part of the county, RegionB the south-west part and RegionC the south-east part of the country.

Three ranges of amount that can be withdrawn by any customer or ATM card user were used in the course of this research as variables to be considered in the course of initiating a transaction on the ATM, which could fall in any of the following range; 500-10,000 (A1), 10,001-30,000 (A2), 30,001-50,000 (A3) since no ATM will dispense above 50,000 per transaction.

The ranges of time used in this research were from 11.01pm-6am, from 6.01-9.00am, from 9.01am-8.00pm, and from 8.01am-11.00am.

Paring the above criteria, we will have the following structures of trees for decision making;

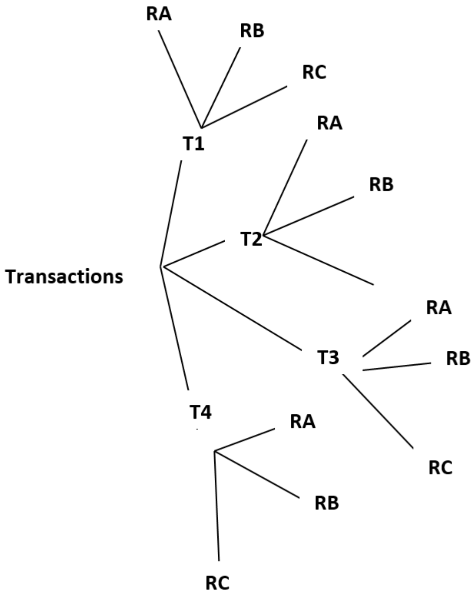


*Figure 1: Paring Time and Location*

From Figure 1, the following samples of patterns of transactions with respect to time and location apply:

Transaction1 (T1,RA)
Transaction2 (T1,RB)
Transaction3 (T1,RC)
Transaction4 (T2,RA)
Transaction5 (T2,RB)
Transaction6 (T2,RC)
Transaction7 (T3,RA)
Transaction8 (T3,RB)
Transaction9 (T3,RC)
Transaction10 (T4,RA)
Transaction11 (T4,RB)
Transaction12 (T4,RC)

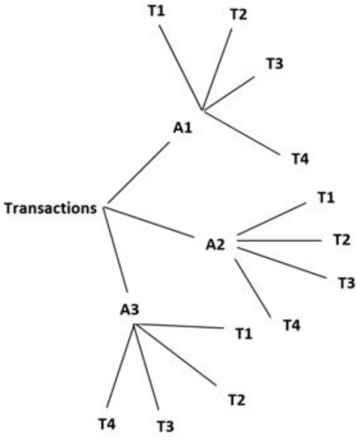


*Figure 2: Paring amount and time*

From Figure 2, the following samples of patterns of transactions with respect to time and amount apply:

Transaction1 (A1,T1)
Transaction2 (A1,T2)
Transaction3 (A1,T3)
Transaction4 (A1,T4)
Transaction5 (A2,T1)
Transaction6 (A2,T2)
Transaction7 (A2,T3)
Transaction8 (A2,T4)
Transaction9 (A3,T1)
Transaction10 (A3,T2)
Transaction11 (A3,T3)
Transaction12 (A4,T4)

From Figure 3, the following samples of patterns of transactions with respect to location and amount apply:

Transaction1 (RA,A1)
Transaction2 (RA,A2)
Transaction3 (RA,A3)
Transaction4 (RB,A1)
Transaction5 (RB,A2)
Transaction6 (RB,A3)
Transaction7 (RC,A1)
Transaction8 (RC,A2)
Transaction9 (RC,A3)

From the Figure 4, 36 transaction patterns are deduced with respect to location, time and amount involved in the transaction and the following samples of the transaction patterns apply:

Transaction1 [(T,T1)&(L,RA)&(A,A1)]
Transaction2 [(T,T1)&(L,RA)&(A,A2)]
Transaction3 [(T,T1)&(L,RA)&(A,A3)]
Transaction4 [(T,T1)&(L,RB)&(A,A1)]
Transaction5 [(T,T1)&(L,RB)&(A,A2)]
Transaction10 [(T,T1)&(L,RA)&(A,A1)]
Transaction20 [(T,T3)&(L,RA)&(A,A2)]
Transaction21 [(T,T3)&(L,RA)&(A,A3)]
Transaction22 [(T,T3)&(L,RB)&(A,A1)]
Transaction23 [(T,T3)&(L,RB)&(A,A2)]
Transaction24 [(T,T3)&(L,RB)&(A,A3)]
Transaction25 [(T,T3)&(L,RC)&(A,A1)]
Transaction26 [(T,T3)&(L,RC)&(A,A2)]
Transaction27 [(T,T3)&(L,RC)&(A,A3)]
Transaction30 [(T,T4)&(L,RA)&(A,A3)]
Transaction35 [(T,T4)&(L,RC)&(A,A2)]
Transaction36 [(T,T4)&(L,RC)&(A,A3)]

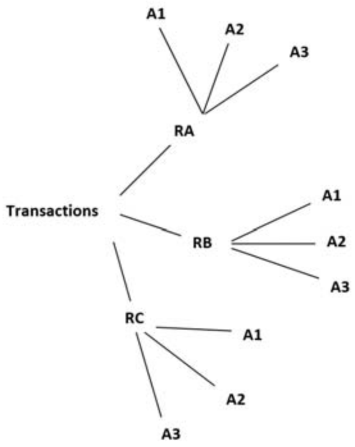


*Figure 3: Paring location and amount*

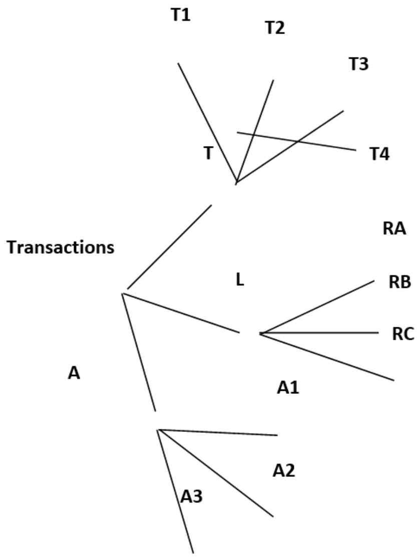
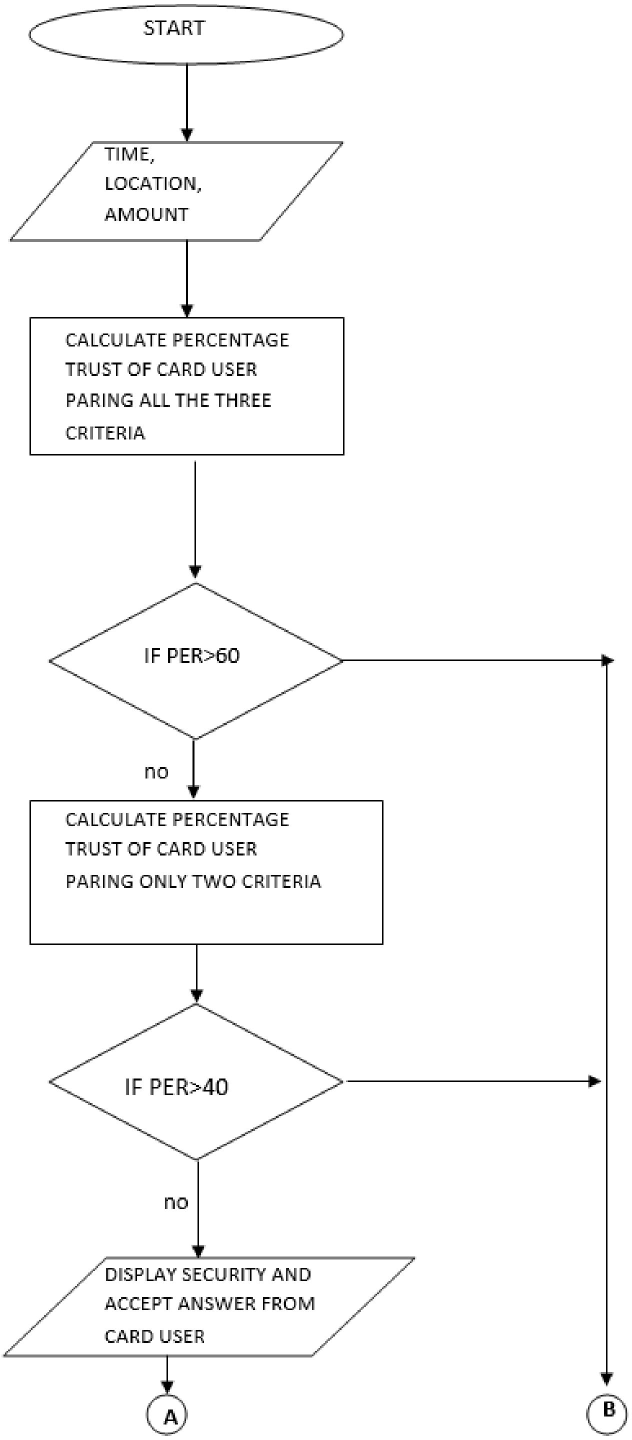


*Figure 4: Paring all the three criteria*

All the pattern of transactions derived from the tree structures from Figure 4 are the possible pattern of transaction considering the time, amount and location of the transaction.

### 3.1. Data Mining Algorithm for ATM Fraud Detection (DMAAFD)

Figure 5 presents DMAAFD, an algorithm that searches through the database that consists of the past record of transaction of any ATM card user to formulate the pattern of the user transaction. The algorithm accepts the user request (that is, the amount, time and location of the transaction) and compares the criteria with the ATM card user transaction pattern. If the user deviates from his/her regular transaction pattern, the ATM machine


START
TIME,
LOCATION,
AMOUNT
CALCULATE PERCENTAGE
TRUST OF CARD USER
PARING ALL THE THREE
CRITERIA
IF PER>60
no
CALCULATE PERCENTAGE
TRUST OF CARD USER
PARING ONLY TWO CRITERIA
IF PER>40
no
DISPLAY SECURITY AND
ACCEPT ANSWER FROM
CARD USER
A
B

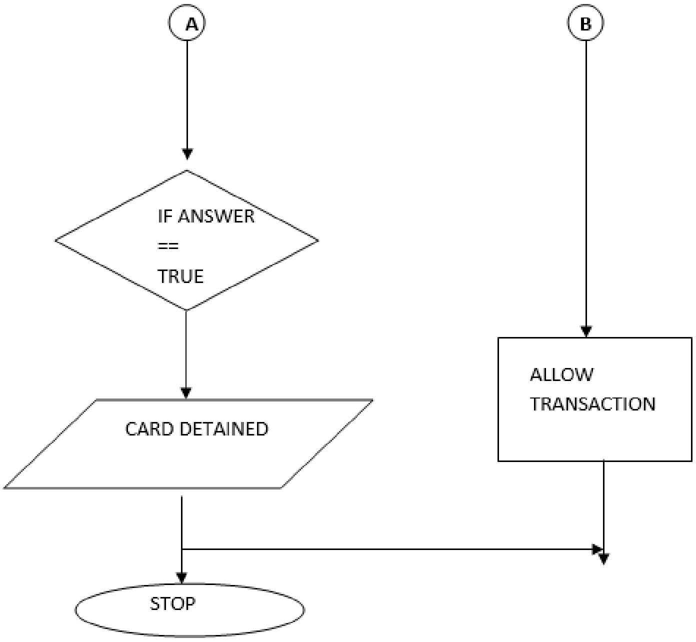


*Figure 5: Data Mining Algorithms for ATM Fraud Detection (DMAAFD)*

will disallow the ATM card user to continue the transaction; else the ATM card user is allowed to complete the transaction.

The algorithm enforces a security technique if the ATM card user has deviated from his/her regular pattern of transaction. The algorithm takes it consideration all the above patterns of transaction.

```
Begin
Output: percentage trust of the ATM card user
Input: Time, amount and location of transaction.
μ = The total transaction the ATM card user has performed
CL = The total transaction the ATM card user has performed in the location
CT = The total transaction the ATM card user has performed in the Time
CA = The total transaction the ATM card user has  performed with the amount

IF(CL[(n[CL])]!=   CL[(n[CL]+1)]   &   (CT[(n[CT])]-(CT[(n[CT]+1])<1hr) THEN
 per= 0
return per
   ELSE
 Per = ((n[CL]/n[μ])+(n[CT]/n[μ]+(n[CA]/n[μ]))/3
     IF per >60 THEN
  Allow Transaction
        ELSE
CTL= The total transaction the ATM card user has performed when Time intercepts Location
CTA= The total transaction the ATM card user has performed when Time intercepts Amount
CLA= The total transaction the ATM card user has performed when Location intercepts Amount
a = (n[CL]/n[μ])*100
b = (n[CT]/n[μ])*100
c = (n[CA]/n[μ])*100
IF(a<50 and b<50 and c>50) THEN
Per=(((n[CLA]/(n[CL])*100)+ ((n[CTL]/(n[CL])*100)))/2
     return per
ELSE IF(a>50 and b<50 and c>50) THEN
 per=(((n[CTL]/(n[CT])*100)+ ((n[CTA]/(n[CT])*100)))/2
     return per
ELSE IF(a>50 and b>50 and c<50) THEN
  per=(((n[CTA]/(n[CA])*100)+ ((n[CLA]/(n[CA])*100)))/2
        return per
ELS       ELSEIF((a<50 and b<50 and c>50) or (a<50 and     b>50 and c<50) or(a>50 and b<50 and c<50)            THEN
           Per =0
       return per
IF per<40 THEN
    return security question
     IF security question == true THEN
          All transaction
                ELSE
            Denied transaction
              ELSE
             Allow transaction
                  END IF
                END IF
             END IF
          END IF
       END IF
End
```

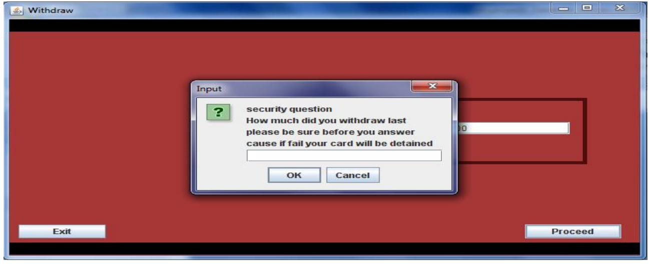
The data mining application is a middle layer application between the front end application (The ATM Application) and back end data storage (The database). The application is design to verify card user by calculating his/her percentage trust based on his/her past record of transaction. The data mining application consist of several user defined functions, which are

- WithDatamin
- WithDatamin2
- securityQues etc.

WithDatamin: This function awaits and accepts time, amount and location of transaction form the ATM application, calculate the percentage trust of the card user by combining all the accepted criteria from the card user. After calculate the percentage trust the function return it to the ATM application to take decision.

WithDatamin2: This function is called upon by the ATM application if decision on the result from the WithDatamin is false. This function also accepts amount and location of transaction form the ATM application, calculate the percentage trust of the card by pairing the criteria from the card user. After calculate the percentage trust the function return it to the ATM application to take decision.

SecurityQuest: If the decision on the result from the WithDatamin2 is also false, the ATM application will call on securityQues function to ask the card user a security question. The securityQues function will accept the answer provided by the card user, compare it with the correct answer and return a decision value to the ATM application. If the decision value is true the ATM application will allow the user to continue, else the card will be detained from the card user for verification. Figure 6 shows a dialogue box pops up if the ATM card user has deviated from his/her pattern of transaction.



security question
How much did you withdraw last
please be sure before you answer
cause if fail your card will be detained

*Figure 6: Pop up Security Question*

## 4. CONCLUSIONS

This paper explored the use of decision tree in detecting ATM fraud in Nigeria. The decision tree pairs the location of transactions, time of transactions and amount involved in the transaction. The location of transaction only examines the three zones out of six-geo political zones in Nigeria. It is hope that future works will capture all the six zones and some major economic hubs in the country such as Lagos, Abuja and Port-Harcourt. The implementation of this research by financial institutions will increase customers' confidence in the e-services rendered by banks.

## REFERENCES

Baker, C. R. 1999. An Analysis of fraud on the Internet. Internet Research-Electronic Networking Applications & Policy, 9(5), 348-359.

Barse, E., Kvarnstrom, H. and Jonsson, E. 2003. Synthesizing Test Data for Fraud Detection Systems. Proc. of the 19th Annual Computer Security Applications Conference, 384-395.

Elkan, C. 2001. Magical Thinking in Data Mining. Proc. of SIGKDD01, 426-431.

Francisca Nonyelum .2012. Data Mining Application In Credit Card Fraud Detection System. Journal of Engineering Science and Technology. Vol. 6, No. 3, pp 311 - 322

Khyati Chaudhary, Bhawna Mallick .2011. Exploration of Data mining techniques in Fraud Detection: Credit Card. International Journal of Electronics and Computer Science Engineering, ISSN 2277-1956/V1N3-1765-1771

Lach, J. 1999. Data Mining Digs In American Demographics. pp38-40, 42-45.

Lavrac, N., Motoda, H., Fawcett, T., Holte, R., Langley, P. And Adriaans, P. 2004. Introduction: Lessons Learned from Data Mining Applications and Collaborative Problem Solving. Machine Learning 57(1-2): 13-34.

Orunsolu A.A, Bamgboye O.O, Alaran M.A and Aina-David O.A,O. 2012. Strategies for Effective Adoption of Electronic Banking In Nigeria. Computing, Information System and Development Informatics Journal

Phua, C., Alahakoon, D. and Lee, V. 2004. Minority Report in Fraud Detection: Classification of Skewed Data, SIGKDD Explorations 6(1): 50-59.

Priyadharshini V., Adiline Macriga G. 2012. An Efficient Data Mining for Credit Card Fraud Detection using Finger Print Recognition. International Journal of Advanced Computer Research. Volume-2 Number-4 Issue-7

Rosset, S., Murad, U., Neumann, E., Idan, Y. and Pinkas, G. 1999. Discovery of Fraud Rules for Telecommunications - Challenges and Solutions. Proc. of SIGKDD99, 409-413.

Sharma A and Panigrahi P.K. 2012. A Review of Financial Accounting Fraud Detection based on Data Mining Techniques. IJCA. Vol. 39 No 1

Full Paper

# AN ASSESSMENT OF FEEDBACK MECHANISM OF SOME SELECTED WEBSITES TOWARDS IMPROVED END-USERS' PASSWORD

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

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

**ABSTRACT**

Many popular websites implement feedback mechanism when assessing the strength of the passwords provided by their users during password creation or alteration. There is, therefore the need to investigate the effects of this feedback mechanism on the quality of password created by their users. An empirical investigation of this was carried out using selected five popular websites. Two thousand five hundred (2,500) randomly selected students from the Federal College of Education, Abeokuta were used for this study. The passwords created by these students using these five websites were subjected to four types of offline attacks. The result shows that feedback mechanism has positive significant effect on the strength of password chosen by the end-users during password creation or alteration. The paper concludes that if end-users are helped in creating stronger passwords through this method, then cracking will become more difficult and the activities of cyber-criminals towards this direction will be reduced.

**Keywords:** *Cyber-economic crime, Feedback, Offline Attacks,*

## 1. INTRODUCTION

The evolution of networked computing and especially the Internet, with the many user centric/data sensitive capabilities readily available, has made user authentication a top priority in systems deployed today. The main authentication mechanism employed in millions of computer installations and websites is passwords. Password have maintained their predominance as a form of authentication even in the face of new developments e.g. biometric authentication devices and this seems to remain the case for the foreseeable future (Andreas, 2012). St. Clair et al (2006) examined the question of whether passwords are facing exhaustion. Their findings reveal that password has come to stay and that it will be difficult to replace or abandon the use of passwords completely. Herley et al (2009) examined the state of passwords and why better progress has not been made towards other stronger authentication methods and concluded that password has come to stay. In an effort to secure their systems, administrators create mandatory password policies that users are required to follow when creating or altering their passwords.

A popular scheme that helps users choose strong passwords is to proactively check passwords. This mechanism is currently employed by many websites serving millions of users. Most of the times, by using a number of criteria set by the developers, these proactive password checkers provide users with feedback labeling their password as too short, weak, fair, strong or very strong.

As systems continue to rely more and more on passwords for authentication, password security and password creation policies become more important to investigate. Some researchers such as Shiva (2011) and Sodiya & Agholor (2012) investigated on how users select passwords and found that most of the users do not pay sufficient attention to protect their passwords or choose strong passwords for their accounts. Therefore, password creation policies try to enforce security by mandating users to add complexity to their passwords such as including numbers or special characters. There have been few studies regarding password creation policies, but none of them showed how effective these policies could be against real attacks. In other words, none of these studies focused specifically on password strength, which should be provided by the password creation policies.

Therefore, the important research questions that have not yet been answered are:

Is Password Creation Policy uniform across websites? Which Password Creation Policy can be more effective when defending end-user against real attacks? Do the existing feedback mechanisms help end-users in creating strong passwords? These questions will be addressed in this paper.

The rest of this paper is organized as follows: Section 2 presents a brief overview of Related Work. In Section 3, Research Methodology is discussed in detail. Analysis, discussion of results and implications for cyber-economic crime are presented in Section 4. Finally, recommendations, conclusion and future work are discussed in Section 5.

## 2. RELATED WORK

Passwords have been the prominent means for authentication almost since the need for user authentication and authorization emerged in multi-user environments. Along with passwords came the concerns about their security and usability. In the first UNIX systems different options for password creation and security were proposed and evaluated. It was early understood that because of users' weak passwords practices and choices such as using the username as their password, security risks came into being. The realization, in these early years, of the weakness a single ill-chosen password posed to the whole system led to large volumes of research in the creation of secure passwords and password policies and it has been proposed by many researchers that a good policy will help increase the security of user accounts in a given system (Komaduri et al, 2011, Shay & Bertino, 2009, Shay et al, 2007 and Summers & Bosworth, 2004).

Florencio et al (2007) argued that when there is only an online brute-force attack, adequate lockout policies make brute-forcing infeasible. In one of the most closely related works, Mannan and Van'Oorschot (2007) examined usability in online banking. They studied policies beyond passwords, and found that compliance in some cases is difficult for end-users. Efforts should therefore, be made towards a friendly policy that could help end-users create very strong password. Herley (2009) suggested that users behave rationally in ignoring recommendation to choose stronger passwords and other security advice especially when the recommendations place considerable burden on them, and deliver little reduction in risk, hence the need for password creation policy that is user friendly.

Much research has been conducted on mechanisms and policies that will enable users to choose strong and memorable passwords. Various avenues for password creation have been explored. Among them, are systems that employ graphical passwords (Suo et al, 2005), which utilize images instead of the traditional textual passwords to limit adversary's abilities to attempt brute-force attacks like the ones commonly used against systems with textual passwords as well as enhance memorability of the passwords. Graphical passwords have, however, their own drawbacks, for example, it is susceptible to shoulder surface attacks - when an adversary can acquire a password by observing the owner while using it and much research is still directed towards tackling them. Forget et al (2008) presented a system that aims at improving password strength by placing randomly-chosen characters at random positions into the password. This system was successful in increasing password security but at the same time users came up with strategies that would limit the mechanism's effectiveness when many random characters were placed into a password. In order to accommodate better password creation strategies Yan et al (2004) suggested that mnemonic phrase-based passwords and memorable phrases condensed into passwords, could be employed and provide equal protection to those of random passwords. It was demonstrated by Kuo et al (2006) that these passwords could be broken, especially as human mnemonic phrase dictionaries would become more available to attackers. However, Sodiya and Agholor (2012) found out that mnemonic phrase-based passwords when constructed using Nigerian Languages can prove to be very strong passwords.

Furthermore, a common mechanism to help users in creating strong password has been Reactive and Proactive password checking. This is further explained below.

### 2.1. Reactive Password Checker

It has being suggested that educating users, letting them understand the need for security and the rationale behind good password choices will lead to better overall security of a system as well as better attitude towards password policies on their part (Sodiya & Agholor, 2012). However there are cases that education and guidance are ineffective or the users might not be willing or savvy enough to read and understand the policies in place, let alone the reasoning behind them. In such cases, alternative and automatic mechanisms should be employed. Such a mechanism is the reactive password checker. The administrator periodically checks the system to find guessable passwords with password cracker programs. Accounts that are cracked are suspended until the passwords have been changed. The disadvantage of this mechanism is that these checks consume resources and there is the possibility that between checks a vulnerable account is exploited. Another disadvantage which is very costly is the exposure of users' passwords to this administrator. A disgruntled administrator can use this privilege negatively.

### 2.2. Proactive Password Checker

As a response to the limitations of reactive password checker, proactive password checking has been put in place. A proactive password checker is a mechanism that interacts with the user while they are creating or changing their account's password and informs them whether their password is one that could be easily guessed or not. Proactive password checkers operate as a form of user education at the time of creation of the password and can also be used to explain why the password chosen is inappropriate for the task e.g., too short, or very weak or weak. Over the years, proactive password checking has been extensively studied in various cases. A few systems that check passwords proactively based on different rule-sets and try to discourage or disable users from using weak passwords can be found in (Schechter et al, 2010). In most cases, the password meter relies on designer choices about the rule-set employed, that is, the policies that passwords must follow to be deemed fit for acceptance or otherwise.

## 3. METHODOLOGY

This section describes the methodology used in carrying out this study.

### 3.1 Website Selection

For this study, five popular websites were selected. They are:

1. Gmail
2. You Tube;
3. Facebook;
4. Microsoft (MS) Live
5. Yahoo.

### 3.2. Conduct of Experiment

This was done in three stages as described below.

#### *3.2.1 Stage 1: Survey Tests*

Several tests were conducted on the five selected websites by the researchers. This is to give us first hand information about the feedback given by the various websites as well as understand their minimum character requirement for a password and other relevant information.

*3.2.2 Stage 2: Experimental Study*

The participants for this study were students from the Federal College of Education, Abeokuta, Nigeria. Five hundred students per School were randomly selected as participants and were assigned to the website written against their School as shown in table 1. The experimental study commenced on November 1, 2012.

*Table 1: Assignment of Participants into Groups and Websites*

| Group | School | Website | Number of Students |
|---|---|---|---|
| 1 | Arts and Social Sciences | Gmail | 500 |
| 2 | Education | YouTube | 500 |
| 3 | Languages | Facebook | 500 |
| 4 | Science | MS Live | 500 |
| 5 | Vocational | Yahoo | 500 |
| Total Number of Participants | | | 2,500 |

The participants were asked to open an actual account using the website assigned to them as well as complete the questionnaire given to them. The questionnaire was used to capture their demographic information and experience in the use of passwords in accessing online accounts. It was also used to capture the password strength indicator and obtain information on whether a participant changes his or her password during creation as a result of feedback he or she received. To complete the experiment, the participants were asked to use the password emanating from the website assigned to them to open account at the ICT Centre and complete the registration process. All the participants completed the experimental process.

*3.2.3 Stage 3: Offline Attacks*

One month after the usage of the passwords by the participants at the College ICT Centre, four types of offline attacks were conducted on the passwords as shown below:

1. Basic Dictionary Attack: John the Ripper Password Cracker (2012) was invoked using the “wordlist” command line option. This option checks the password against each word in the dictionary. We also check the password against each password in the Mnemonic Dictionary Wordlist (2012).
2. Dictionary Attack with Permutation: We invoked John the Ripper with the “rules” command line option on each dictionary. This performed “word mangling” through character replacement e.g. permute with 0, 1, 2 and 3 digit(s) to construct possible password candidates, replacing “a” with “@”, capitalization, the addition of prefixes and suffices. Also make common number substitutions, such a 1 for I, 5 for S, 3 for E, and other permutations, etc.
3. User Information Attack: We use user information collected from password files, e.g, userid, user full name, initial substring of name and concatenation of names to crack the passwords.
4. Brute Force Attack: John the Ripper Password Cracker (2012) was invoked without command line options, forcing it to try all combinations of characters for all passwords.

## 4. ANALYSIS AND DISCUSSION OF RESULTS

### 4.1. Participants’ Demographics

Table 2 shows that 53% of the participants are male while 47% are female.

*Table 2: Demographic Analysis of the total Participants*

| Sex | Number of Participants | % of Participants |
|---|---|---|
| Male | 1,325 | 53.0% |
| Female | 1,175 | 47.0% |
| Total | 2,500 | 100.0% |

The participants reported having between three and ten accounts that require passwords. Their usage of these accounts span over between two and six years. This implies that participants have good background on the use of passwords before the conduct of the experimental study.

### 4.2. Password Creation Policy, Strength Feedback and Minimum Password Length

Results showing the password creation policies and the strength of passwords are shown in table 3.

The result from table 3 shows that there are huge differences on how password strength feedback is implemented and what strength assessments the users are presented with among the websites surveyed.

From the results in table 3, we believe that the computation of the password strength by the websites under study is somewhat faulty. This gives rise to erroneous feedback. For example, Yahoo displaying P@ssword and Pa$$word as “very strong” passwords will misguide the users because attackers can easily guess such passwords. Results of the tests showing various verbal characterizations of passwords for the five websites are presented in Table 4. From table 4, it is clear that the password strength feedback in the selected five websites is somewhat different.

Another important aspect we tested was the minimum password requirements for the websites. The result of this test presented in table 5 shows that the minimum password requirement is not uniform. For example, a password can receive a rating as “strong” with only 6 digits on Facebook but not on Gmail where it must have at least 8 digits.

The results from tables 3, 4, and 5 show that Password Creation Policy is not uniform across websites. These findings confirm the finding of Furnell (2007) who found that users’ guidance in password selection varies from website to website.

### 4.3 Effectiveness of the Password Creation Policies

The result showing the summary of passwords cracked is presented in table 6. From table 6, the percentage of cracked passwords is highest (40.6%) for Facebook group followed by Yahoo group (38.6%). These websites have the least character length of a password, that is, 6 characters. On the other hand, MS Live which accepts 8 characters as minimum password length has the lowest percentage (20.0%) of cracked password. Therefore, MS Live Password Creation Policy is more effective when defending end-user against real attacks.

*Table 3: Password Policies and resultant Passwords*

| Website | Policy | Remark/Resultant Password |
|---|---|---|
| Gmail | Use at least 8 chars. Do not use password from another site or something too obvious like your pet's name.<br>Note: Policy displayed before creation of password | Treats 8-digit number, userid or email and concatenation of firstname and lastname(if more than 8 chars) as strong password. Accepts firstname, lastname and birthday but strength differs depending on character length. Treats P@ssword and Pa$$word as weak passwords. |
| YouTube | Use at least 8 chars. Do not use password from another site or something too obvious like your pet's name.<br>Note: Policy displayed before creation of password | Treats 8-digit number, userid or email and concatenation of firstname and lastname(if more than 8 chars) as strong password. Accepts firstname, lastname and birthday but strength differs depending on character length. Treats P@ssword and Pa$$word as weak passwords. |
| Facebook | Please choose a secure password. It should be longer than 6 characters, unique to you and difficult to guess.<br>Note: Policy displayed only on rejection of a password | Accepts 6-digit number, userid or email, P@sssword, Pa$$word and concatenation of firstname and lastname as passwords but no strength feedback. Rejects Firstname and lastname. |
| MSLive | Must be at least 8 chars and contain at least two of the following: uppercase, lowercase, numbers and symbols.<br>Note: Full policy displayed only upon rejection of a password while "8-chacracter minimum; case sensitive" displayed before creation of password. | Accepts P@ssword with the following feedback: "choose a password that's harder for people to guess". Accepts Pa$$word with no feedback. Rejects firstname, lastname, userid, digit- password and concatenation of firstname and lastname. |
| Yahoo | For a more secure password:<br>-Use both letters and numbers.<br>-Add special chars such as @, ?, % etc.<br>-Mix capital and lowercase chars.<br>-At least 6 characters<br>Note: Policy displayed before creation of password | Accepts P@ssword and Pa$$word as very strong password. Rejects firstname, lastname, userid and concatenation of firstname and lastname. |

*Table 4: Password Strength Feedback Levels*

| Name | Password Strength Feedback |
|---|---|
| Gmail | Too Short, Weak, Fair, Good, Strong |
| You Tube | Too Short, Weak, Fair, Good, Strong |
| Facebook | No strength feedback |
| MS Live | No strength feedback |
| Yahoo | Too Short, Weak, Strong, Very Strong |

*Table 5: Minimum Password Length across tested Websites*

| Name | Minimum Password Length |
|---|---|
| Gmail | 8 characters minimum length |
| You Tube | 8 characters minimum length |
| Facebook | 6 characters minimum length |
| MS Live | 8 characters minimum length |
| Yahoo | 6 characters minimum length |

*Table 6: Summary of number of cracked Passwords*

| Website | Number of Passwords attacked | Number of Passwords cracked | % of Passwords cracked |
|---|---|---|---|
| Gmail | 500 | 112 | 22.4% |
| YouTube | 500 | 109 | 21.8% |
| Facebook | 500 | 203 | 40.6% |
| MS Live | 500 | 100 | 20.0% |
| Yahoo | 500 | 193 | 38.6% |
| Total | 2,500 | 717 | 28.7% |

### 4.4 Effects of the feedback Mechanism on Quality of Passwords

The result in table 7 shows the summary of the number of passwords cracked with the corresponding number of passwords changed during creation while table 8 shows the participants that changed their password during creation.

*Table 7: Summary of number of passwords cracked/changed.*

| Website | Number of Password attacked | Number of Passwords cracked | Number of Password changed |
|---|---|---|---|
| Gmail | 500 | 112 | 19 |
| YouTube | 500 | 109 | 22 |
| Facebook | 500 | 203 | 03 |
| MS Live | 500 | 100 | 17 |
| Yahoo | 500 | 193 | 09 |
| Total | 2,500 | 717 | 70 |

*Table 8: Summary of Participants that change their password during creation*

| Website | No. of students | Remark on Strength & Policy Feedback | No. of Password changed | % of Password changed |
|---|---|---|---|---|
| Gmail | 500 | Strength & Policy Feedback implemented | 19 | 3.8% |
| YouTube | 500 | Strength & Policy Feedback implemented | 22 | 4.4% |
| Facebook | 500 | No Strength & No Policy Feedback | 03 | 0.6% |
| MS Live | 500 | No Strength Feedback but Policy Feedback implemented | 17 | 3.4% |
| Yahoo | 500 | Strength & Policy Feedback implemented | 09 | 1.8% |
| Total | 2,500 | | 70 | 2.8% |

While Facebook accepts 6-digit number, userid, P@ssword, etc as passwords with no strength and policy feedback, Yahoo on the other hand accepts P@ssword and Pa$$word as passwords with strength feedback indicating that they are "very strong" passwords. Results from tables 6, 7 and 8 show that feedback mechanism has positive effect on the choice of password by the end-users. Thus the number of password changed by the end-users for the websites with feedback mechanism is by far higher than that of no feedback mechanism. For example, Facebook, with no feedback mechanism has the least number (0.6%) of participants that changed their passwords during creation. Correspondingly, Facebook group has the highest (40.6%) number of cracked passwords.

Table 9 shows a very strong correlation between the number of passwords cracked and number of passwords changed during creation. The negative sign, not surprising, indicates that as more participants change to stronger passwords during creation as a result of the feedback received that their chosen passwords are weak, cracking success decreases. It is akin to the simple economic theory of demand, that is, the higher the price, the lower the demand and vice versa.

*Table 9: Correlation of number of passwords changed and number of passwords cracked*

| | CRACKED | CHANGED |
|---|---|---|
| CRACKED | | |
| Pearson Correlation | 1.000 | -0.935* |
| Sig. (2-tailed) | . | 0.019 |
| N | 5 | 5 |
| CHANGED | | |
| Pearson Correlation | -0.935* | 1.000 |
| Sig. (2-tailed) | 0.019 | . |
| N | 5 | 5 |

**Correlation coefficient is significant at the 0.5 level (2-tailed).*

Figure 1 shows the graph of the number of passwords cracked when plotted against the number of passwords changed. From the graph (figure 1), the two variables, cracked and changed representing number of passwords cracked and number of passwords changed respectively are strongly correlated. In other words, the higher the passwords changed during creation or alteration, the lower the passwords cracked and vice versa.

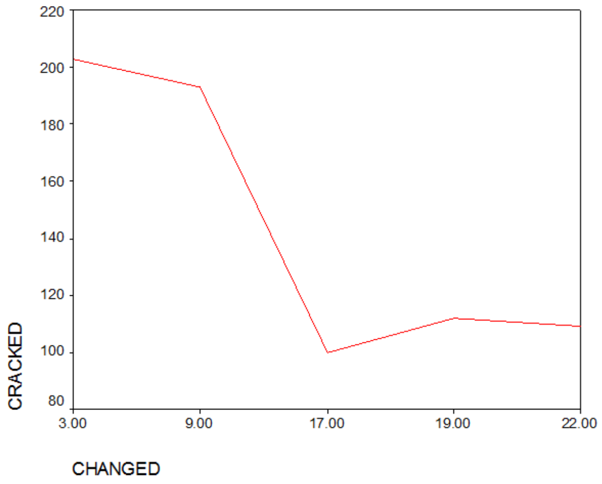


*Figure 1: Graph of number of password changed versus number of password cracked*

### 4.5 Implications for Cyber-Economic Crime

The implication of having very strong password in protecting end-users' accounts against cyber-economic crime and other unauthorized access cannot be over-emphasized.

A strong password is resistant to both online and offline attacks as shown in our findings. Assisting end-users in creating strong passwords through feedback mechanism is therefore a welcome development.

Since strong passwords are difficult to crack, it will help bring cyber-economic crimes to the barest minimum. This finding is in line with Doctor et al (2009) who stated that Strong Passwords are good protection for unauthorized access to computer systems and are effective countermeasures against cyber-criminals.

## 5. RECOMMENDATIONS, CONCLUSION AND FUTURE WORK

### 5.1. Recommendations

The findings of this study highlight the significance of assisting end-users in creating stronger passwords through feedback mechanism. Arising from the findings, the paper recommends the following:

1. A minimum password character length of 10 for non-financial accounts and 14 for financial accounts should be used in creating password.
2. An innovative feedback mechanism should be adopted.
3. Since feedback mechanism is derived from computation of password entropy, a more robust entropy model that will give true password strength to the end-users should be developed.

### 5.2. Conclusion and Future Work

The results of this study revealed significant effect on improving password strength chosen by end-users if adequate feedback mechanism is put in place. One other finding of this work shows that end-users have to deal with a number of different and sometimes conflicting password strength assessments and feedbacks at various sites.

In future work, efforts should be made to deal with conflicting password strength assessments and feedbacks. To tackle this, the paper suggests the development of a mathematical model that can be used in computing minimum password character length. Since the computation of the password strength by the websites under study is somewhat faulty, future work should be concerned on how to come up with a more robust model for computation of password strength.

## ACKNOWLEDGEMENTS

We appreciate the partial support from Tertiary Education Trust Fund (tetFund), Abuja, Nigeria. The contents are solely the responsibility of the authors and do not necessarily represent the official views of Tertiary Education Trust Fund, Abuja, Nigeria.

## REFERENCES

Andreas, S (2012) Influencing User Password Choice Through Peer Pressure. Unpublished Thesis submitted to the Department of Electrical and Computer Engineering, The University of British Columbia

Doctor, Q., Emmet D. and Toby, S., 2009. CompTIA A+. Indianapolis, Indiana: Wiley Publishing Inc,. pp. 560–563.

Florencio, D., Herley, C. and Coskun, B., 2007. Do Strong Web Passwords Accomplish Anything? In Proceedings of USENIX Hot Topics in Security, USA, pp. 97-107.

Forget, A., Chiasson, S. van Oorschot, P. C. and Biddle, R., 2008. Improving Text Passwords through Persuasion. In Proceedings of the 4th SOUPS, New York, NY, USA, pp. 1–12.

Furnell, S., 2007. An Assessment of website Password Practices. In Computers and Security, Vol. 26, No. 7, pp. 445 – 451.

Herley, C (2009) So long, and no thanks for the externalities: the rational rejection of security advice by users. In Proceedings of the 2009 Workshop on New Security Paradigms Workshop, NSPW '09, New York, NY, USA, pp. 133–144

Herley, C., van Oorschot, P. C. and Patrick, A. S., 2009. Passwords: If We Are So Smart Why Are We Still Using Them? In Proceedings of Financial Cryptology

John the Ripper Password Cracker., 2012. From www.openwall.com/john Date visited 23/03/12

Komanduri, S., Shay, R., Kelley, P. G., Mazurek, M. L., Bauer, L., Christin, B. N., Cranor, L. F. and Egelman, S., 2011. Of Passwords and People: Measuring the effect of password composition policies. In Proceedings of the 2011 Annual Conference on Human Factors in Computing Systems, New York, NY, USA, pp.2595–2604.

Kuo, C., Romanosky, S. and Cranor, L. F. 2006. Human Selection of Mnemonic Phrase-based Passwords. In Proceedings of SOUPS, New York, NY, USA, pp. 67-78.

Mannan, M. and Van'Oorschot, P. C., 2007. Security and Usability: The Gap in Real-World Online Banking. In Proceedings of the Workshop on New Security Paradigms Workshop, (NSPW)

Mnemonic Dictionary Wordlist., 2012. From www.mnemonicdictionary.com Date visited 08/11/12

Schechter, S., Herley, C. and Mitzenmacher, M., 2010. Popularity is everything: A new approach to protecting passwords from statistical-guessing attacks. In Proceedings of the 5th USENIX conference on Hot Topics in security, HotSec'10, Berkeley, CA, USA, pp. 1–8.

Shay, R. and Bertino, E., 2009. A Comprehensive Simulation Tool for the Analysis of Password Policies. In International Journal of Information Security, Vol. 8, pp. 275–289.

Shay, R., Bhargav-Spantzel, A. and Bertino, E., 2007. Password Policy Simulation and Analysis. In Proceedings of the ACM workshop on Digital Identity Management, DIM '07, New York, NY, USA, pp. 1–10.

Shiva, H. Y., 2011. Analyzing Password Strength & Efficient Password Cracking. Unpublished Thesis submitted to Department of Computer Science, The Florida State University.

Sodiya, A. S and Agholor, S., 2012. Evaluation of Memorability and Security of Randonmly- and Mnemonic-Generated Passwords. In International Journal of Scientific Innovations

Sodiya, A. S and Agholor, S., 2012. Users's Password Selection and Management Methods: Implications for Nigeria's Cashless Society. In Proceedings of the 24th National Conference of the Nigeria Computer Society, Uyo, Nigeria, Vol. 23, pp. 39 – 47.

St. Clair, L., Johansen, L., Enck, W., Pirretti, M., Traynor, P., McDaniel, P. and Jaeger, T., 2006. Password Exhaustion: Predicting the End of Password Usefulness. In Proceedings of 2nd International Conference on Information Systems Security (ICISS)

Summers, W. E. and Bosworth, E., 2004. Password Policy: The Good, The Bad, and The Ugly. In Proceedings of the Winter International Symposium on Information and Communication Technologies, (WISICT), Trinity College Dublin, pp. 1–6.

Suo, X., Zhu, Y. and Owen, G. S., 2005. Graphical Passwords: A Survey. In Annual Computer Security Applications Conference. From www.doi.ieeecomputersociety.org/10.1109/ CSAC.2005.27 Date visited 14/11/2012

Yan, J. J., Blackwell, A., Anderson, R. and 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

Full Paper

# ANALYSIS OF e-PAYMENT ADOPTION IN A DEVELOPING ECONOMY CONTEXT

**B.A. Akinnuwesi**
Department of Information Technology,
Bells University of Technology, Ota, Ogun State Nigeria
boluakinnuwesi@bellsuniversity.edu.ng

**F.M.E. Uzoka**
Department of Computer Science & Information Systems,
Mount Royal University Calgary, Canada

**E.O. Chukwueloke**
Department of Information Technology,
Bells University of Technology, Ota, Ogun State Nigeria
uzokafm@yahoo.com

**ABSTRACT**

There is a global paradigm shift form cash-based economy to cashless/cash light economy where all business transactions are completed electronically. It seems that a number of developing economies (especially in Africa) are still cash based economies. This study analyses the adoption of electronic payment systems in Nigeria from the point of view of the users. We utilized random sampling technique to survey users from various professions. Regression analysis was carried out on completed questionnaire to test the hypotheses derived from the modified UTAUT model. The study reveals that though electronic payment systems are utilized in the country, poor attitude and lack of facilitating conditions still militate against high level of adoption of e-payment systems. A number of other factors, which have been identified in literature, were not statistically significant in our study.

**Keywords:** *Electronic payment, technology adoption, developing country, UTAUT, cashless society*

## 1. INTRODUCTION

Electronic Payment (e-Payment) is a form of direct payment or banking through electronic means, interactive communication channels and other technology infrastructure. e-Payment can be described as the method of effecting payments from one entity to another through electronic means. In Nigeria, the modernization of the payment process started with the introduction of payment cards in 1993 by the Central Bank of Nigeria (CBN). In 2004, CBN introduced a broad guideline on e-banking, which included the introduction of ATM, and e-money products such as credit and debit cards. Currently, there is a real-time gross settlement (RTGS) system that eliminates the risks involved in large-value payment. The new Internet money, that is the form of money using Internet as the main transaction mode, builds on payment instruments such as credit/debit cards, direct debit/credit and electronic versions of cash and cheques. It differs from earlier forms of money in that it is both impersonal and virtual.

The relatively slow development of efficient e-Payment systems in Nigeria have been attributed to attitudinal and social problems as manifested in the huge amount of money that resides outside the banking sector. Nigeria is largely a cash-based economy with over 90% of funds residing outside the banking sector. This is in contrast with developed countries such as UK (4%) and USA (9%) (Ojo 2004; Ovia, 2002). The cash-based economy is characterized by the psychology to physically hold and touch cash: a culture informed by ignorance, illiteracy, lack of security consciousness, and low appreciation of the merits of digital payment (Ayo 2006). The cash based nature of the Nigerian economy has to a great extent, hindered the participation of her citizens in e-commerce. An efficient payment system is necessary for e-Commerce to be successful. The use of formal payment systems also enhances the ability to execute and manage monetary policies, which is essential for a country's financial sector (Ayo, 2006).

In order to ensure transparency and accountability, the Nigerian government unveiled e-Payment system which took effect from January 1, 2009. Consequently, all financial transactions in the public sector were to be conducted electronically. That is, all government agencies were to stop cash-based and cheque-based transactions and commence cashless transactions using electronic payment medium (e.g. Point of Sale [POS] machines, Automatic Teller machine [ATM], secured payment portal on Internet, electronic bank transfer, etc) (Asaolu et. al., 2011; Dankwambo, 2009a; Dankwambo, 2009b). The Central Bank of Nigeria (CBN) in collaboration with the Bankers' committee placed the cash lodgement and withdrawal limits of individual to N500,000 (Five hundred thousand naira). The processing fee for withdrawal is 3% while 2% is charged for processing fee for lodgement. Also cash lodgement and withdrawal limit for corporate organizations is N3,000,000 (Three million naira). The processing fee for withdrawal is 5% while processing fee for lodgement is 3%. Presently, exemptions have been granted to Ministries, Departments and Agencies of federal and state government on lodgements for revenue collection account only. The placement of limit to cash lodgement and withdrawal helps to enforce the cashless policy and thus enhance the efficacy of Nigerian monetary policy. The CBN in conjunction with banks was to commence the implementation of the cashless policy in phases. The pilot scheme started with Lagos and was tagged "Cashless Lagos" (Abdullahi, 2011).

In (Asaolu et. al., 2011), some of the constraints confronting implementation of electronic payment system in Nigeria were identified and some recommendations were suggested for effective implementation. Similarly in (Ovia, 2009), the following were identified as constraints to effective implementation of the cashless policy in Nigeria: 1) inadequate ICT infrastructure; 2) high cost of IT deployment; 3) slow internet connection; 4) unexpected system failure; 5) system insecurity; 6) behavioural constraints; 7) inadequate funding. Our study analyses the performance of e-payment systems in Nigeria from the users' perspectives. It investigates the factors that affect users' intention to adopt e-payment in Nigeria. In Section 2, we review some existing literature on e-Payment. Section 3 presents the research framework, the methodology of the study, while the data analysis and discussion of results are presented in Section 4. Section 5 concludes the paper.

## 2. REVIEW OF RELATED WORKS

The Internet has served as a catalyst to online business transactions particularly in some of the developed countries like US, UK, France, Germany etc. Electronic commerce (e-Commerce) is becoming the medium for business transactions and payment is done electronically using electronic payment (e-Payment) system (Anik and Pathan, 2002). Moreover, with the rapid growth of Information and Communication Technology (ICT), electronic commerce is now acting as a means of carrying out business transactions through electronic means (Asaolu et. al., 2011).

The stakeholders of e-Payment system can be classified as internal and external. The internal stakeholders are the personnel (staff and management) of the enterprise that owns the e-Payment system while the external stakeholders are the clients/customers that are expected to transact business via the e-Payment platform provided. The stakeholders are principal entities that an e-Payment system must satisfy their requirements for it to be accepted, adopted and implemented.

A number of research works have been carried out on electronic transaction (e-Transaction) systems in Europe, US, Asia and Africa on the adoption and implementation of electronic payment system for business transactions. In (Uzoka and Seleka, 2006), the development level of e-Commerce in Botswana was investigated. The result (in 2006) showed that only 44% of the total organizations surveyed in Botswana performed well on the e-Commerce indicators and that the adoption level of e-Commerce in most of the organizations was low. This implies that e-Payment system adoption in Botswana as at 2006 was low. Also it was established in (Uzoka et. al., 2006) that infrastructural, organizational and behavioural factors influence the adoption of e-Commerce in developing countries. In (Al-adawi et. al., 2005), the perspective of end users of e-Government was studied with the view to understanding the views of the citizens on using e-Government system as a primary channel for citizen-to-government and government-to-citizen interaction. A conceptual model was proposed for citizen adoption of e-Government system. The major function of the model is to aid government to increase the level of citizen adoption of online services that are provided and also ensure that trust and risk issues are taken care of.

Papaefstathiou and Manifavas (2004) highlighted the forbiddingly high cost attributed to some technical components of micropayment system, which increases the cost of developing and also using the electronic payment instrument. The authors established that the implication of high technical cost is one of the main reasons for low usage of e-Payment systems by stakeholders. It was recommended in the paper that e-Payment mechanisms should contain only the important features that provide the relevant services and that the system designers should consider and minimize each of the development cost factors. In addition, a study was carried out on the factors influencing users' acceptance of mobile payment (m-Payment) system in (Agnieszka et. al, 2004). The focus was on understanding the users' motivation and attitudes towards m-Payment procedure with the view to proposing a mobile payment user acceptance model.

In (Qile et. al., 2006), the adoption of online e-Payment by Chinese business organizations was examined using Rogers' relational model of perceived innovation attributes and rate of adoption. It was established that perceived compatibility has significant impact on the adoption of online e-Payment system of Chinese companies. In (Yao-Hua and Walter, 2000; Dimitrakos, 2002), a trust model was developed for electronic commerce system in order to take care of trust issues that may influence customers' intention to use electronic mechanisms for business transaction and payment. The quest to address security issue of e-Payment system adoption led to the development of a security model using Elliptic Curve Cryptosystem in (Vincent et. al., 2010). Various trust models were presented in (Myoung-Soo and Jae-Hyeon, 2005; Yun et. al., 2005; Xianfeng and Qin, 2005; Guoling and Liping, 2005) in order to have secured electronic transactions.

Several factors have been identified in literatures as determinants that influence publics' adoption, acceptance and utilization of a technology or system. Some of the factors are presented in Table 1. In addition some studies have been carried out on publics' adoption of some electronic trading systems (e.g. e-Commerce, e-Taxing system, online auctioning system, grid computing) in some places like Taiwan, Singapore, Botswana among others. Some of the research works are presented in Table 2.

## 3. RESEARCH FRAMEWORK

One of the earliest models of adoption and innovation is the Diffusion of Innovation [DOI] model (Rogers, 1983). The DOI model indicates that the rate of adoption is impacted by five factors: relative advantage, compatibility, triability, observability and complexity. A number of other theorists have studied technology adoption from different perspectives (technological, organizational, individual, contextual, environmental, and managerial). However, Venkatesh et al. (2003) produced the Unified Theory of Acceptance and Use of Technology (UTAUT), which attempts to improve on the predictive ability of other individual models by identifying communalities and capitalising on the best aspects of each model. Venkatesh et al (2003) argue that the UTAUT model can explain as much as 70 percent of the variance in intention, on individual acceptance and usage decisions in organizations. Some authors (e.g. Chau and Hu 2002, Al-Qeisi, 2009, Schaper and Pervan 2007, and Aggelidis and Chatzoglou 2009) have modified the UTAUT to increase its ability to explain adoption behaviour intention. The framework used in the study adapts the modified UTAUT from these

*Table 1: Determinants of Technology Adoption*

| Literature | Determining Factors of Adoption |
|---|---|
| Chang et. al. (2005); Wu and Lederer (2009) | Perceived usefulness, perceived ease of use, information system quality, information quality, perceived credibility |
| Mallat et. al. (2008); Mallat et. al. (2009); Hsiao (2003); Quaddus and Achjari (2005) | Compatibility of the technology with consumers' behaviour, Mobility and contextual factors, monetary cost of use, availability of other alternative technologies, time of service delivery, prior experience on the services delivered by the technology, social influence, attitude towards technology, perceived trust, perceived risk of use, income level of users, access to the service provided by the technology, ability of users to solve different contextual problems associated with the technology. |
| Tan and Teo (2000); Schepers and Wetzels (2007); Chun-Der et. al. (2007). | Attitudinal factors (e.g relative advantage, compatibility with respondent's values, experience and needs, trial ability and risk); subjective norms and perceived behavioural control, awareness of technology to users, fears of privacy and security risks, confidence in using services provided, perception of government support for the technology. |
| Crespo and Bosque (2010) | Product perception, shopping experience, level of risk perceived, attitudes toward the technology, subjective norm. |
| Shin-Yuan et.al. (2006); Pin-Yu et. al. (2004); Otto et. al. (2005); Shin (2009); Shin-Yuan et.al. (2009) | Perceived usefulness, ease of use, perceived risk, trust, compatibility, external influences, interpersonal influence, self-efficacy, and facilitating condition |
| Lee and Kim (2007); Lee and Kim (2009). | Technical support, Web experience, task equivocality, task interdependence, compatibility, Information System (IS) infrastructure and Expertise in IS. |
| Yang (2005) | Consumer perceived usefulness, consumer innovativeness, past adoption behaviour, technology cluster adoption, age, gender, government policies, telecommunications infrastructure, marketing strategies of service providers, harmonization of technical standards, and the abilities to protect consumer privacy and transaction security. |
| Kim et. al. (2010) | User-centric factors (e.g. users' innovativeness and knowledge about the technology), system-centric factors (e.g. mobility, reachability, compatibility, and convenience of the technology). |
| Mallat (2007) | Complex solutions, premium pricing, low adoption rates, perceived risks and perceived incompatibility. |
| Loo et. al. (2009) | Lack of understanding of the benefits of the technology, lack of facilitating conditions, anxiety of damaging devices needed for the use of the technology, lack of social support (e.g. influence from peer group) and credibility of using the technology applications. |

*Table 2: Studies on Technology Adoption*

| Literature | Description of Research | Location |
|---|---|---|
| Pin-Yu et. al. (2004) | Exploring Success Factors for Taiwan's Government Electronic Tendering System: Behavioural Perspectives from End Users | Taiwan |
| Shin-Yuan et. al. (2006) | Determinants of User Acceptance of the e-Government Services: The case of online tax filing and payment system | Taiwan |
| Chun-Der et. al. (2007) | Predicting electronic toll collection service adoption: An integration of the technology acceptance model and the theory of planned behaviour | Taiwan |
| Gatautis and Neverauskas (2005 | E-commerce Adoption in Transition Economies: SMEs Perspectives in Lithuania | Lithuania |
| Lin and Li (2005) | The Online Auction Market in China - A Comparative Study between Taobao and eBay | China |
| Martinsons (2002) | Electronic commerce in China: emerging success stories | China |
| Famin and Lilin (2005) | Electronic Market and Operating Intermediary | China |
| Qingfei et. al. (2008) | Mobile Commerce User Acceptance Study in China: A Revised UTAUT Model | China |
| Yang (2005) | Exploring factors affecting the adoption of mobile commerce in Singapore | Singapore |
| Kendall et. al. (2001) | Receptivity of Singapore's SME to Electronic Commerce Adoption | Singapore |
| Asaolu et. al. (2011) | Electronic Payment System in Nigeria: Implementation, Constraints and Solutions | Nigeria |
| Lee and Kim (2007) | Factors Affecting the Implementation Success of Internet-based Information Systems | North Korea |
| Kim and Lee (2008) | Factors Affecting the Implementation of Electronic Data Interchange in Korea. | North Korea |
| Ka-Young et. al. (2009) | The Adoption of e-Trade Innovations by Korean Small and Medium Sized Firms. | South Korea |
| Kshetri (2007) | Barriers to E-Commerce and Competitive Business Models in Developing Countries: A Case Study | Nepal |
| Uzoka and Seleka (2006) | B2C E-Commerce Development in Africa: Case Study of Botswana | Botswana |
| Quaddus and Achjari (2005) | A Model for Electronic Commerce Success | Australia |
| Cheng et. al. (2006) | Adoption of Internet Banking: An empirical study in Hong Kong | Hong Kong |
| Loo et. al. (2009) | User Acceptance of Malaysian Government Multipurpose Smartcard Applications | Malaysia |

authors to explain the behavioural intention to adopt biometric technology. Chau and Hu posited that that technology acceptance should be examined from three different contexts: the individual context, the implementation context and technological context. Our research model (Figure 1) recognizes the technology adoption influencing variables under these three contexts and the following moderating factors: age, gender, and experience. Experience is captured by the following variables: educational background and job experience.

The individual context includes essential individual characteristics, contexts and perceptions that relate to technology use intention. The individual context consists of attitude, self-efficacy, awareness and anxiety. The attitude of an individual towards a technology would influence the individual's decision to adopt the technology (Lau et. al, 2001). Awareness of a system and the risks associated with it, and its inherent problems (if any occurs) go a long way to determining the individual's attitude and behavior towards using and adopting the system (Argarwal and Prasad 1998). Self Efficacy refers to the belief that one can successfully carry out the behavior required to produce the outcome. Prior research (Taylor and Todd, 1995) investigating technology usage behavior has shown self-efficacy to contribute to the use behavior. Anxiety defines the degree at which an individual is nervous while using the given technology. It could negatively affect the individual's intention to adopt the technology (Schaper and Pervan 2007).

The implementation context defines the specific environment where the individual works and the technology under investigation is utilized (Chau and Hu, 2002; Aggelidis and Chatzoglou, 2009). The implementation context includes social influence, facilitating conditions, and security. Social influence defines the extent to which an individual perceives that important others believe he or she should use a technology (Lau et al, 2001). Facilitating conditions deal with organizational and technical infrastructure that are in place to support use of the technology. Previous adoption studies (e.g. Venkatesh et al 2003; Chang et al, 2007) have pointed to a positive relationship between facilitating conditions and technology use intention. Security defines the extent to which the system provides a sense of protection against loss, attack, or harm. Security concerns have been found to have a negative effect on the intention to adopt technology (Kirter, 1997).

The Technological context deals with effort expectancy and performance expectancy. Effort expectancy defines the degree to which an individual perceives that a technology would be easy to use. A number of studies have found effort expectancy to influence decision to use a technology (e.g. Agarwal and Prasad 2000), while some others have not found any significant influence (e.g. Chau and Hu 2002). Performance expectancy is the degree to which an individual believes that e-payment would help him or her attain gains in both job performance and personal endeavours. Previous adoption studies (e.g. Venkatesh et al, 2003, Chang et al 2007) have found performance expectancy to be a strong predictor of use intention.

Based on the research model, the following hypotheses were tested:

H1: An individual's awareness of the existence and utility of e-payment would affect the intention to use e-payment.

H2: Attitude towards the e-payment system has a direct effect on an individual's behavioural intention to use the system.

H3: High performance of e-payment system increases an individual's intention to use the e-payment system.

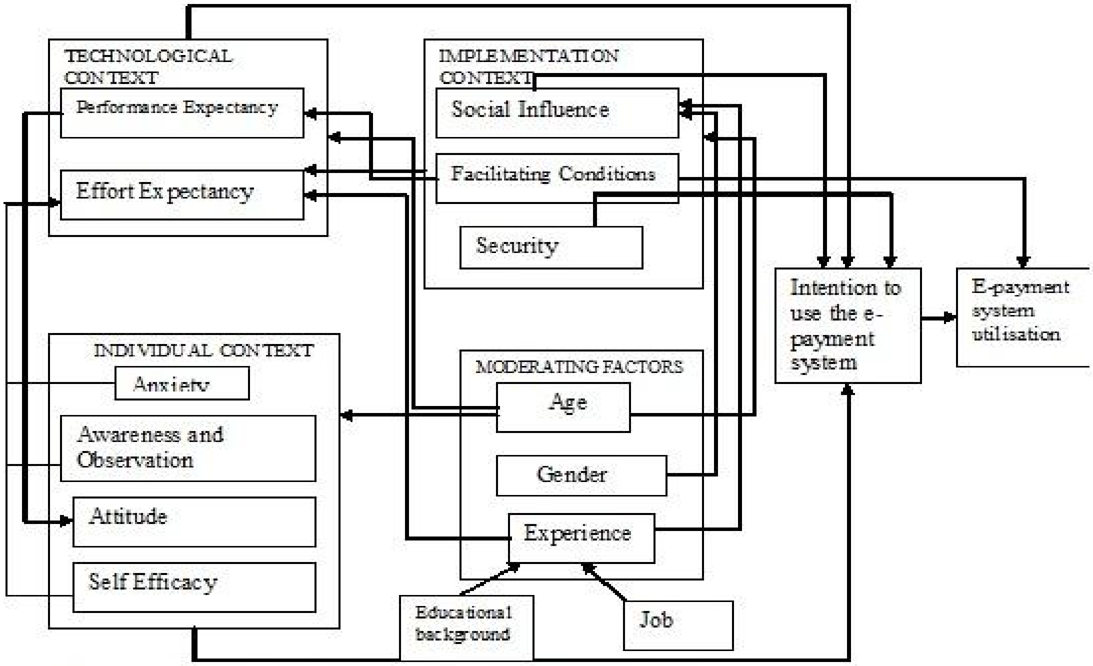


**Figure 1** Research Model based on the Modified UTAUT Framework

*Figure 1: Research model based on the Modified UTAUT Framework*

H4: The level of efforts required for the utilization of e-payment system would inversely affect the individual's intention to use e-payment.

H5: Anxiety has a direct negative effect on an individual's intention to use the e-payment system

H6: Influence of peers and other social groups would have a direct impact on the individual's intention to utilize e-payment system.

H7: Self efficacy has a positive impact on an individual's intention to use and continue using the e-payment system.

H8: Security concerns would negatively affect the intention to adopt e-payment

H9: Availability of facilitating conditions such as electricity, currency denominations dispensed by ATMs, Internet access would have a direct positive impact on the individual's intention to use e-payment.

H10: Observation of e-payment workability in other contexts could affect the individual's intention to use e-payment

H11: According to the research framework, a number of moderating relationships exist as follows:

| Sub-hypothesis | Factor | Moderator |
|---|---|---|
| H11.1 | Anxiety | Age |
| H11.2 | Awareness | Age |
| H11.3 | Attitude | Age |
| H11.4 | Self Efficacy | Age |
| H11.5 | Social Influence | Age |
| H11.6 | Effort expectancy | Educational Background |
| H11.7 | Social influence | Educational Background |
| H11.8 | Effort expectancy | Job |
| H11.9 | Social Influence | Job |
| H11.10 | Social Influence | Gender |
| H11.11 | Effort expectancy | Self Efficacy |
| H11.12 | Effort expectancy | Awareness |
| H11.13 | Attitude | Performance expectancy |
| H11.14 | Effort expectancy | Anxiety |
| H11.15 | Effort expectancy | Facilitating Conditions |
| H11.16 | Performance expectancy | Facilitating Conditions |

### 3.1 Methodology

*3.1.1 Survey Procedure and Sampling Instrument*

The primary source of data for this study was the questionnaire. Using a random sampling technique, the questionnaire was administered to several individuals in different professions, which include banking, law, teaching, students, engineering, carpentry, medicine, catering, fashion designing, information and communications technology and others. Three hundred and ten questionnaires were distributed, while one hundred and fifty (48.38%) copies of the questionnaires were properly filled and returned for purposes of data analysis.

The questionnaire consisted of two sections. Section A contains the demographic information such as sex, age, marital status, profession, and highest educational qualification. Other variables in section A include class of e-payment card used, frequency of use, length of use, number of times an individual has encountered problems using the e-payment card, and a question to capture if the individual has ever been a victim of internet fraud. In Section B, the questions were grouped into factors affecting adoption which include; awareness, attitude towards technology, performance expectancy, effort expectancy, anxiety, social influence, self efficacy, security, hindrances, and observation.

*3.1.2. Data Analysis*

Statistical Package for Social Sciences (SPSS) version 17 was employed in the analysis of data. Descriptive statistics was utilized in describing the demographics of respondents, while regression analysis was conducted to determine the effects of the identified factors (based on UTAUT) on intention to use e-payment. A further correlation analysis was conducted to determine the relationship between each pair of factor.

## 4. RESULTS AND DISCUSSION

### 4.1. Descriptive Statistics of Respondents' Characteristics

Presented in Table 1 is the descriptive statistics of respondents' characteristics. The descriptive statistics of the respondents' characteristics shows that the respondents were mostly people between ages 20 and 50 which accounts for 95.3% of respondents. Both male (52.7%) and female (47.3%) actively participated in the survey with a narrow margin in favour of the male respondents. Majority (70.0%) of the respondents were not married and are mostly (55.4%) holders of Bachelor's degree certificate. They (70.0%) make high use of e-Payment cards. Our statistics showed that 79.4% of the respondents have over a year experience in the usage of e-Payment systems; however, many of the respondents which account to 57.3% have encountered some problems with the e-Payment system while 42.7% of the respondents have never encountered problems with the e-Payment system. People that have been victims of e-Payment frauds in more than one time account to 45.7%, while those that are not, account to 54.3%. Our statistics also revealed that most of the respondents which account to 94.6% are knowledgeable about the e-Payment technology but many of them (67.5%) did not have adequate training on the use of the technology. Therefore based on the results of the descriptive statistics, lack of adequate training of the end users and frequency of problems encountered by some people in the use of the e-Payment system were identified as factors inhibiting the adoption of the technology; however, further test was carried out to establish this.

### 4.2. Hypotheses Testing

In order to test the study hypotheses, a regression analysis was carried out using "intention to use e-payment" as the dependent variable. The independent variables include; awareness, attitude towards technology, performance expectancy, effort expectancy, anxiety, social influence, self efficacy, security, and observation. Table 2 shows the model summary.

$R^2$ indicates the predictive capability of the model. An initial model summary showed an $R^2$ value of 0.747 and adjusted $R^2$ of 0.558 which indicates a good model fit. When the moderating factors were introduced into the analysis, the $R^2$ value improved to 0.802, and adjusted $R^2$ of 0.644. This showed and even stronger model fit. The ANOVA test (Table 3 shows an F value of 10.439 (p<<0.5), which is an indication that the predictors significantly affects the dependent variable (intention to use e-payment) as shown in Table 3.

*Table 1: Respondent's Characteristics*

| Characteristics | Number | Percentage |
|---|---|---|
| *Respondents' Age* | | |
| Over 51 | 2 | 1.4% |
| 31 – 50 | 42 | 28.0% |
| 20 – 30 | 101 | 67.3% |
| Less than 20 | 5 | 3.3% |
| *Respondents' Sex* | | |
| Male | 79 | 52.7% |
| Female | 71 | 47.3% |
| *Marital Status* | | |
| Single | 105 | 70.0% |
| Married | 45 | 30.0% |
| *Respondent's Qualification* | | |
| Senior School Certificate (SSC) | 19 | 12.7% |
| Ordinary National Diploma (OND) | 12 | 8.2% |
| Higher National Diploma (HND) | 12 | 8.2% |
| Bachelor's Degree (B.Sc & B.Tech) | 83 | 55.4% |
| Master's Degree | 18 | 11.7% |
| Doctorate Degree (Ph.D) | 6 | 3.8% |
| *Frequency of e-Payment Card usage* | | |
| Moderately used | 45 | 30.0% |
| Highly used | 86 | 57.3% |
| Very Highly used | 19 | 12.7% |
| *Length of e-Payment Card usage* | | |
| Below 1 year | 31 | 20.6% |
| 1 – 5 years | 109 | 72.7% |
| Above 5 years | 10 | 6.7% |
| *Frequency of Problem with ATM Technology* | | |
| Never encounter problem | 64 | 42.7% |
| 1 – 5 times | 68 | 45.3% |
| Over 5 times | 18 | 12.0% |
| *Victims of Internet Fraud* | | |
| Never | 81 | 54.3% |
| 1 – 5 times | 67 | 44.7% |
| Over 5 times | 2 | 1.0% |
| *Knowledge of ATM Technology* | | |
| Very Knowledgeable | 74 | 49.3% |
| Knowledgeable | 68 | 45.3 |
| Not Sure | 4 | 2.7% |
| Not Knowledgeable | 2 | 1.4% |
| Strong not knowledgeable | 2 | 1.3% |
| *Training Respondents on ATM usage* | | |
| Strongly Trained | 29 | 19.1% |
| Fairly Trained | 46 | 30.9% |
| Poorly Trained | 55 | 36.6% |

*Table 2: Model Summary*

| Model | R | R Square | Adjusted R Square | Std. Error of the Estimate |
|---|---|---|---|---|
| 1 | .802[a] | .644 | .526 | .68837118 |

b. Dependent Variable: e-payment use Intention

*Table 3: ANOVA*

| Model | | Sum of Squares | Degree of Freedom | Mean Square | F value | Sig. |
|---|---|---|---|---|---|---|
| 1 | Regression | 60.859 | 11 | 5.533 | 11.263 | .000[a] |
| | Residual | 48.141 | 98 | .491 | | |
| | Total | 109.000 | 109 | | | |

The statistical coefficients (standardized) presented in Table 4, resulting from the regression analysis show the factors that influence the users' intention to adopt e-payment. It also indicates the extent of influence of each factor on e-payment adoption. The cross terms show the moderating influence of a moderator on a factor. For example, AgeSocialInf represents the cross term between age on social influence. The results show that the following factors significantly affect the intention to adopt e-payment: attitude (t= 3.088, p=0.03), facilitating conditions (t=3.025, p= 0.003). Every other factor does not have a significant influence on the intention of the individual to adopt e-payment. The moderating influences were not statistically significant. However, a number of relationships had near significant influences, such as Age & Social Influence and Performance expectancy & Attitude. Hypotheses H2, H9 are supported while other hypotheses are not supported.

*Table 4: Regression Analysis*

| Model | Beta | t | Sig. (p) |
|---|---|---|---|
| (Constant) | | 1.047 | .298 |
| Awareness | .108 | 1.322 | .190 |
| Attitude | .252 | 3.088 | .003 |
| Performance expectancy | .018 | .200 | .842 |
| Effort expectancy | .063 | .673 | .503 |
| Anxiety | -.101 | -1.186 | .239 |
| Social influence | -.016 | -.190 | .850 |
| Self efficacy | .083 | .970 | .335 |
| Security | -.017 | -.215 | .831 |
| Facilitating Condition | .286 | 3.025 | .003 |
| Observation | -.095 | -1.212 | .229 |
| AgeAnxiety | -.037 | -.473 | .638 |
| AgeAwareness | -.098 | -1.141 | .257 |
| AgeAttitude | -.024 | -.295 | .769 |
| AgeSelfEf | .071 | .867 | .389 |
| AgeSocialInf | .154 | 1.878 | .064 |
| EducbackEffort | .064 | .823 | .413 |
| EducbackSocialInf | .044 | .514 | .609 |
| JobEffort | -.115 | -1.364 | .176 |
| JobSocialInf | -.081 | -1.072 | .287 |
| GenderSocialInf | .065 | .798 | .427 |
| SelfEffort | -.059 | -.676 | .501 |
| AwarenessEffort | -.044 | -.488 | .627 |
| PerfAttitude | -.142 | -1.767 | .081 |
| AnxietyEffort | .057 | .633 | .529 |
| FcondEffort | .005 | .037 | .971 |
| FcondPerf | .030 | .267 | .790 |

The results of the hypothesis tests point to only two factors: attitude and facilitating conditions. The attitude of Nigerians towards e-payment may be affected by awareness, ease of use of the system, educational background, social influence, system performance. For instance, if awareness created about the system performance is low/poor, users' attitude towards the system will be poor. In addition, poor educational background or illiteracy may negatively influence the attitude of people using the system. Facilitating conditions such as electricity, availability and accessibility of the ATM have also been a source of concern to Nigerians. It is worthy to note that despite the availability of credit cards in Nigeria, there is still a problem with acceptance of credit cards from Nigeria by some international organizations. The respondents considered this as one of the facilitating conditions that could enhance adoption of e-payments in the Nigerian economy. Overall, one would say that despite the fact that about 80% of the respondents have used e-payment systems for over one year, only about 13% of the respondents used the e-payment systems very frequently. This still boils down to the two key factors: attitude and facilitating conditions affecting the use of e-payment systems. Poor facilitating conditions could potentially reduce the adoption intensity.

### 4.3. Correlation Analysis for Individual and Group Factors

The correlations (Table 5) of all factors show the level of association between each factor pair Performance and awareness are correlated at 95% level of significance. If the e-payment system has a high performance then people would be aware of the system, its correlation (performance) with attitudes towards the technology is at 99% which means people would have a good attitude towards using the e-payment system if the system has a high performance and vice versa, It also means that people would like to use the system and would be willing to accept the system. More so, an e-payment system's performance includes flexibility. If the system is flexible enough for the user then he/she would not feel nervous using the system. This explains the negative correlation (p< 0.05) between anxiety and performance, that is, a user would only feel intimidated by the system if it is not flexible. Anxiety also has a positive correlation (p< 0.01) with effort expectancy which suggests that if an individual does not feel nervous using the system then it would be easy for him or her to use the system. Also, while anxiety is not statistically significant, it shows a reasonable (t= -1.186) negative impact on adoption. If a person is anxious about a system, it reduces the tendency to adopt the system. The correlation analysis (Table 5) shows that facilitating conditions shows some significant correlation with anxiety.

The correlation between security and social influence is significant at 99% (p< 0.01), which suggests that if the e-payment providers are not trust worthy and users do not feel secured about their privacy while carrying out electronic payment transactions then they would discourage whoever is using the system from using it else they would encourage them or influence them positively towards the use of the system. The correlation between security and self efficacy (p< 0.01) is significant, which suggests that a user would feel confident and would be able to carry out transactions without help if he/she is confident. Facilitating conditions has a negative correlation (p< 0.01) with performance. This indicates that the performance of the e-payment system is affected by poor facilitating conditions. Equally, due to the poor facilitating conditions, users exercise some form of anxiety with the use of e-payment systems. There is also a significant negative correlation (P< 0.01) between facilitating conditions and effort expectancy, which suggests that a person would not put in so much effort towards using the system if he/she is not sure that there would be power supply and some currency in an ATM machine. There is significant positive correlation between: security and awareness; use intention and awareness; and use intention and anxiety. This suggests that (1) adequate publicity is needed on the safety of business transaction via e-payment platforms; (2) Users would be more interested to use the system provided there is enough awareness programme to promote the good functionality of the system, (3) users' intention to use e-payment system will be high provided they exhibit minimal anxiety about the system functionality. In addition, there is significant negative correlation between: users' intention and performance expectancy; users' intention and security; anxiety and performance expectancy. This suggest that: (1) low level of e-payment system performance would raise users' anxiety and thus discourage them from adopting it as channel for payment for business transactions; (2) users' would be discourage to use e-payment system if security of business transaction is not guaranteed using the system.

## 5. CONCLUSION

The advent of e-payment system in Nigeria has brought a lot of benefits and advantages. But even with this, some citizens still don't make use of the e-payment system. The regression result indicates that the infrastructures available for e-payment use determine a person's intention to use the e-payment system. 53% of the respondents identified poor electricity supply as a major hindrance in making internet based transactions. The descriptive statistics also shows that lack of adequate training of the users and frequency of problem encountered while using the system are among the factors affecting e-payment adoption. Only 32.5% of the respondents have been trained on how to use the e-payment system.

*Table 5: Factor Pair Correlations*

| | awareness | Attitude | performance expectancy | Effort expectancy | anxiety | Social influence | Self efficacy | security | Facilitating Conditions | observation |
|---|---|---|---|---|---|---|---|---|---|---|
| Awareness | 1 | | | | | | | | | |
| Attitude | .179 | 1 | | | | | | | | |
| Performance Expectancy | .211* | .318** | 1 | | | | | | | |
| Effort expectancy | .183 | .195* | .517** | 1 | | | | | | |
| Anxiety | -.181 | .126 | -.223* | -.317** | 1 | | | | | |
| Social Influence | .106 | .175 | .164 | .120 | .124 | 1 | | | | |
| Security | .171 | .092 | .083 | .104 | -.030 | .273** | .314** | 1 | | |
| Hindrance | -.125 | -.064 | -.246** | -.279** | .289** | -.160 | -.068 | -.169 | 1 | |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| Observation | .105 | .234* | .082 | .045 | .213* | .173 | .110 | -.001 | .220* | 1 |
| Use Intention | .105 | .211* | -.066 | -.048 | .163 | -.121 | -.035 | -.076 | .635** | .105 |
| Facilitating conditions | .155 | .021 | -.148 | -.200* | .294** | -.140 | -.078 | -.075 | .524** | -.022 |

Our study indicates that people are aware of the benefits of using the e-payment system. About 90% of the respondents said they save time using the ATM machine instead of going to the bank. The respondents indicate a positive attitude towards e-payment systems. However, facilitating conditions are not improved upon; the growth of e-payment systems in Nigeria would likely be stunted. The Nigerian economy still has a chance of becoming cashless if barriers (such as poor infrastructure and international rejection of payments from Nigeria) are removed.

Existing e-payment infrastructure for e-payment in Nigeria include: Automated Teller Machine, Point of Sale Terminals, on-line payment via Internet, Electronic fund transfer using ATM or the fund transfer portal of the banks. Apart from poor electricity supply, these infrastructure are currently saddled with a number of problems, which include: 1)Inability of ATM Machines to dispense cash, while same money has been deducted from the customer's account. When this happens, there is often a reversal within 24-48 hours and in some cases, there is no reversal and customer will have to complain at the bank's customer care centre. The resolution of such complaints could take up to one or two weeks; 2) Incessant network failures which prevents users from completing online transactions without truncation; 3) Seizure of debit cards by the ATMs. This tends to increase the customer's anxiety level regarding; 4) Inability to complete transactions at the point of sale systems (POS) due to either electricity failure or network failure; 5) lack of knowledge on the use of POSs by some sales cashier and customers on the use of POS. Our results corroborate the findings of Ovia (2009) who identified mainly infrastructural and behavioural constraints as impediments to implementation of cashless society in Nigeria.

We recommend the following measures as ways of improving the utilization of e-payment systems in Nigeria: 1)Provision of stable electricity; 2) Improvement in network bandwidth to enable efficient online transactions; 3) Enhancement of the payment or e-commerce/e-business portals of the banks; 4) Proper training for staff on the use of e-business/e-payment/e-commerce platforms or portals; 5) Provision of enough awareness and training programmes for customers on how to use all e-payment/e-business platforms; 6) Reduction in tariffs and other price related mechanisms in order to facilitate individual acquisition of network equipment and computing devices (smart phones, PCs, Tablets etc) needed for e-business / e-payment operations.

## REFERENCES

Abdullahi M.M. (2011). Questions and Answers On The CBN Policy On Cash Withdrawal/Lodgement Limit. CBN Publication. Available @ http://www.cenbank.org/Out/2011/pressrelease/gvd/Revised%20QnA%20on%20CBN%20POLICY%20ON%20CASH%20WITHDRAWAL%20LIMIT.pdf, Date accessed: May 25, 2012

Al-adawi Z., Yousafzai S. and Pallister J. (2005). Conceptual Model of Citizen Adoption of e-Government. In proceedings of the Second International Conference on Innovations in Information Technology (IIT'05),

Al-Qeisi Kholoud Ibrahim (2009). "Analyzing the Use of UTAUT Model in Explaining an Online Behaviour: Internet Banking Adoption", A thesis submitted for the degree of Doctor of Philosophy.

Anik, A.A. and Pathan, A.K. ( 2002) A framework for managing cost effective and easy electronic payment system in the developing countries. Available at www.Commonwealth.com. Accessed Date November 12, 2012.

Agarwal R and Prasad J (1998). The antecedents and consequents of user perceptions in information technology adoption. Decision Support Systems, Vol 22, No 1, pp.15-29.

Agarwal R and Prasad J (2000). A field study of the adoption of software process innovations by information systems professionals. IEEE Transactions on Engineering Management, Vol. 43, No. 3, pp. 295-308.

Aggelidis V.P and Chatzoglou (2009). Using a modified technology acceptance model in hospitals. International Journal of Medical Informatics, Vol. 78, pp. 115-126.

Agnieszka Z., Elaine L. and Robert S (2004). Towards Understanding of Factors Influencing User Acceptance of Mobile Payment Systems. In Proceedings of the IADIS International Conference WWW/Internet 2004, Madrid, Spain, 2 Volumes, pp 270-277.

Asaolu T.O., Ayoola T.J. and Akinloye E.Y. (2011). Electronic Payment System in Nigeria: Implementation, Constraints and Solutions. Journal of Management and Society, Vol. 1, No 2, pp. 16-21.

Ayo C.K (2006) Designing a Reliable E-payment System: Nigeria a Case Study Journal of Internet Banking and Commerce, August 2006, vol. 11, no.2

Available at http://www.arraydev.com/commerce/jibc/, Accessed Date: November 12, 2012

Chang I., Li Y., Hung W., and Hwang H. (2005). An Empirical Study on the Impact of Quality Antecedents on Tax Payers' Acceptance of Internet Tax-Filing Systems. Government Information Quarterly (Elsevier), Vol. 22, pp. 389–410

Chang I., Li Y., Hung W., and Hwang H.(2007). Physicians acceptance of pharmokinetics-based clinical decision support systems. Expert Systems with Applications. Vol. 33, No. 2, pp. 296-303.

Chau P.Y.K and Hu P.J-H (2002). Investigating healthcare professionals ' decisions to accept telemedicine technology: an empirical test of competing theories. Information and Management, Vol. 39, No. 4, pp. 297-311.

Cheng T.C.E., Lam D.Y.C. and Yeung A.C.L. (2006). Adoption of Internet Banking: An empirical study in Hong Kong. Decision Support Systems (Elsevier), Vol. 42, pp. 1558–1572

Chun-Der C., Yi-Wen F. and Cheng-Kiang F. (2007). Predicting electronic toll collection service adoption: An integration of the technology acceptance model and the theory of planned behaviour. Transportation Research Part C (Elsevier), Vol. 15, pp. 300–311.

Crespo A.H. and Bosque I.R. (2010). The influence of the commercial features of the Internet on the Adoption of e-Commerce by Consumers. Electronic Commerce Research and Applications (Elsevier), Vol. 9, pp. 562–575.

Dankwambo I.H. (2009a). Understanding the e-Payment System. Available @ http://www.budgetoffice.gov.ng/workshop%20paper/e-payment%20BoF.pdf, Date accessed: May 25, 2012

Dankwambo I.H. (2009b). E-payment Policy And Economic Development. Cardexpo Africa held at civic center, pp. 1-22.

Dimitrakos T. (2002). System Models, e-Risks and e-Trust: Towards bridging the gap?. In Proceedings of Towards the E-Society , IFIP International Federation for Information Processing, Vol. 74/2002, pp. 45-58

Famin Y. and Lilin D. (2005). Electronic Market and Operating Intermediary. In Proceedings of ICEC'05, August 15–17, 2005, Xi'an, China, pp. 130-135

Gatautis R. and Neverauskas B. (2005). E-commerce Adoption in Transition Economies: SMEs Perspectives in Lithuania. In Proceedings of ICEC'05, August 15–17, 2005, Xi'an, China, pp. 109-113.

Guoling L. and Liping W. (2005). Application of E-commerce Security Management Strategy in Banking. In Proceedings of ICEC'05, August 15–17, Xi'an, China, pp. 627-632.

Hsiao R. (2003). Technology fears: distrust and cultural persistence in electronic marketplace adoption. Journal of Strategic Information Systems (Elsevier), Vol. 12, pp. 169–199.

Ka-Young O., Cruickshank D. and Anderson A.R. (2009). The Adoption of e-Trade Innovations by Korean Small and Medium Sized Firms. Technovation (Elsevier), Vol. 29, pp. 110–121.

Kendall J.D., Tung L.L., Chua K.H., Hong N.D.C. and Tan M.S. (2001). Receptivity of Singapore's SME to Electronic Commerce Adoption. Journal of Strategic Information Systems (Elsevier), Vol. 10, pp. 223-242.

Kim B.G. and Lee S. (2008). Factors Affecting the Implementation of Electronic Data Interchange in Korea. Computers in Human Behaviour (Elsevier), Vol. 24, pp. 263–283.

Kim C., Mirusmonov M. and Lee I. (2010). An Empirical Examination of Factors Influencing the Intention to Use Mobile Payment. Computers in Human Behaviour, Vol. 26, pp. 310–322.

Kirter, O (1997). Security issues delay Internet use in health care. Communications News 34, 5 (May 1997)

Kshetri N. (2007). Barriers to E-Commerce and Competitive Business Models in Developing Countries: A Case Study. Electronic Commerce Research and Applications (Elsevier), Vol. 6, pp. 443-452.

Lau Adela and Jerome Yen, Patrick Y. K. Chau (2001). "Adoption of on-line trading in the hong kong financial market", Journal of Electronic Commerce Research, vol. 2, no. 2.

Lee S. and Kim K. (2007). Factors Affecting the Implementation Success of Internet-based Information Systems. Computers in Human Behaviour (Elsevier), Vol. 23, pp. 1853–1880.

Lee S. and Kim B.G. (2009). Factors affecting the usage of intranet: A confirmatory study. Computers in Human Behaviour (Elsevier), Vol. 25, pp.191–201.

Lin Z. and Li J. (2005). The Online Auction Market in China - A Comparative Study between Taobao and eBay. In Proceedings of ICEC'05, August 15–17, 2005, Xi'an, China, pp. 123-129.

Loo W.H., Yeow P.H.P. and Chong S.C. (2009). User Acceptance of Malaysian Government Multipurpose Smartcard Applications. Government Information Quarterly (Elsevier), Vol. 26, pp. 358–367.

Mallat N. (2007). Exploring Consumer Adoption of Mobile Payments – A Qualitative Study. Journal of Strategic Information Systems (Elsevier), Vol. 16, pp. 413–432.

Mallat N., Rossi M., Tuunainen V.K. and Oorni A. (2008). An empirical investigation of mobile ticketing service adoption in public transportation. Pers Ubiquit Comput (Springer Publications), Vol. 12, pp.57–65

Mallat N., Rossi M., Tuunainen V.K. and Oorni A. (2009). The Impact of Use Context on Mobile Services Acceptance: The case of mobile ticketing. Information & Management (Elsevier), Vol. 46, pp.190–195.

Martinsons M.G. (2002). Electronic commerce in China: emerging success stories. Information & Management (Elsevier), Vol. 39, pp. 571–579.

Ming Q. and Xianjun H. (2005). The Design and Analysis of Three-Dimensional E-Business Model. In Proceedings of ICEC'05, August 15–17, Xi'an, China, pp. 136-138.

Myoung-Soo K. and Jae-Hyeon A. (2005). A Model for Buyer's Trust in the E-marketplace. In Proceedings of ICEC'05, August 15–17, Xi'an, China, pp. 195 – 200.

Ojo A.T. (2004). Enhancing the efficiency of the payment system: Conceptual Framework, A paper presented at the 9th CBN Monetary Policy Forum, Abuja, May 2004.

Otto K., Wouter S., Oliver S., Bart V. and Eric V.H. (2005). Why Are Customers Coming Back To Buy Their Airline Tickets Online? Theoretical Explanations and Empirical Evidence. ICEC'05, August 15–17, 2005, Xi'an, China, 319 – 326

Ovia J. (2002). "Payment System and Financial Innovations", a paper presented at the Annual Policy Conference, Nov. 2002.

Ovia J. (2009). The Use of E-payment Systems –the Nigerian Experience. Available @ http://www.zenithbank.com/presentations/E-payment.pdf, Date accessed: May 25, 2012

Papaefstathiou I. and Manifavas C. (2004). Evaluation of Micropayment Transaction Costs. Journal of Electronic Commerce Research, Vol. 5, No. 2, pp. 99 – 113.

Pin-Yu C., Naiyi H., Fung-Wu L. and Chun-Wei C. (2004). Exploring Success Factors for Taiwan's Government Electronic Tendering System: Behavioural Perspectives from End Users. Government Information Quarterly (Elsevier), Vol. 21, pp. 219–234.

Quaddus M. and Achjari D. (2005). A Model for Electronic Commerce Success. Telecommunications Policy (Elsevier), Vol. 29, pp. 127–152.

Qile H., Yanqing D., Zetian F. and Daoliang L. (2006). An Innovation Adoption Study of Online E-Payment in Chinese Companies. Journal of Electronic Commerce in Organizations (JECO), Vol. 4, Issue 1, pp 48-69

Qingfei M., Shaobo J. and Gang Q. (2008). Mobile Commerce User Acceptance Study in China: A Revised UTAUT Model. Tsinghua Science and Technology, Vol. 13, No. 3, pp. 257-264

Rogers, E. (1983) "Diffusion of Innovations", New York: Free Press.

Schaper L.K and Pervan G.P (2007). ICT and OTs: A model of information and communication technology acceptance and utilisation by occupation therapists. International Journal of Medical Informatics, Vol 76S, pp S212-S221.

Schepers J. and Wetzels M. (2007). A Meta-analysis of the Technology Acceptance Model: Investigating subjective norm and moderation effects. Information & Management (Elsevier), Vol. 44 , pp. 90–103

Shin-Yuan H., Chia-Ming C., Ting-Jing Y. (2006). Determinants of User Acceptance of the e-Government Services: The case of online tax filing and payment system. Government Information Quarterly (Elsevier), Vol. 23, pp. 97–122.

Shin-Yuan H., King-Zoo T., Chia-Ming C. and Ching-De K. (2009). User Acceptance of Intergovernmental Services: An example of electronic document management system. Government Information Quarterly (Elsevier), Vol. 26, pp. 387–397.

Shin D. (2009). Towards an Understanding of the Consumer Acceptance of Mobile Wallet. Computers in Human Behaviour (Elsevier), Vol. 25, pp. 1343–1354.

Tan M. and Teo T.S.H. (2000). Factors Influencing the Adoption of Internet Banking. Journal of the Association for Information Systems, Vol. 1, Article 5, pp. 1-44.

Taylor, S., and Todd, P. (1995). "Decomposition and crossover effects in the theory of planned behaviour: A study of consumer adoption intentions".International Journal of Research in Marketing, vol. 12, Issue 2, pp 137-155.

Uzoka F.M.E. and Seleka G.G. (2006). B2C E-Commerce Development in Africa: Case Study of Botswana. In Proceedings of EC'06, June 11–15, 2006, Ann Arbor, Michigan, USA., pp. 290 – 295.

Uzoka, F.M.E., Seleka G.G, and Shemi A.P. (2006). Infrastructural and Behavioural Influences on the Adoption of eCommerce in Developing Countries. In proceedings of IST-Africa conference, Pretoria South Africa , May 3-5, 2006.

Venkatesh, V., Morris, M., Davis, G., and Davis, F. (2003). “User acceptance of information technology: toward a unified view”, MIS Quarterly, vol. 27 issue 3, pp 425-478.

Vincent O. R., Folorunso O. and Akinde A. D. (2010). Improving e-payment security using Elliptic Curve Cryptosystem. Electronic Commerce Research (Springer Journal), Vol. 10, No. 1, pp. 27-41.

Wu J. and Lederer A. (2009). A Meta-Analysis of the Role Of Environment-based Voluntariness in Information Technology Acceptance. MIS Quarterly, Vol. 33, No. 2, pp. 419-432.

Xianfeng Z. and Qin Z. (2005). Online Trust Forming Mechanism: Approaches and An Integrated Model. In Proceedings of ICEC’05, August 15–17, Xi’an, China, pp. 201-209.

Yang K.C.C. (2005). Exploring factors affecting the adoption of mobile commerce in Singapore. Telematics and Informatics (Elsevier), Vol. 22, pp. 257–277

Yao-Hua T. and Walter T. (2000). An Outline of a Trust Model for Electronic Commerce. Applied Artificial Intelligence: An International Journal , Vol. 14, Issue 8, pp. 849-862

Yun Y., Yong H. and Juhua C. (2005). A Web Trust-I nducing Model for E-commerce and Empirical Research. In Proceedings of ICEC’05, August 15–17, Xi’an, China, pp. 188-194

Full Paper

# DESIGN AND IMPLEMENTATION OF SOCIAL SECURITY SCHEME: THE ROLE OF ICT

**E. Okewu**
Centre for Information Technology and Systems
University of Lagos
*eokewu@unilag.edu.ng*

**ABSTRACT**

There is no gainsaying the fact that Nigeria needs a social security system that would prevent people from acting desperately before it can make progress in all aspects of socio-politico-economic spectrum. This assertion is hinged on the realization that Nigeria is in dire need of a coordinated and holistic social security system that will not only protect its citizenry from economic and social risks but also help in reducing the high rate of poverty in the country. Social security places responsibility on the state to protect and provide for the individual when he is unemployed, or losses his job as a result of occupational injury, accident , when he or she grows old and when a woman is on maternal leave, just to mention a few. The state of vulnerable groups like women, persons with disabilities, and the thousands of unemployed youths in the country underscores the fact that all challenges that have impinged on successful implementation of a holistic social security system in the country for several decades need to be urgently addressed. Interestingly, the integration of ICT in sustained and sustainable social protection schemes cannot be overemphasized owing to its pervasive and persuasive nature. This paper outlines a blue print for the design and implementation of social security scheme using ICT.

**Keywords:** *ICT, poverty, safety net, social security, unemployment*

## 1. INTRODUCTION

Irked by the ubiquity of opportunistic negativists, Alade (2012:15) captures the present state of insecurity in Nigeria with his write-up Operation Capture Boko Haram Leader. And determined to locate the root cause, Edukugho (2012: 7) in his caption Unemployment: Nigeria sitting on keg of gun-powder fingers unemployment as the chief factor responsible for the current insecurity in Nigeria. Security as an essential concept is commonly associated with the alleviation of threats to cherished values, especially the survival of individuals, groups or objects in the near future. Thus, security as the name implies, involves the ability to pursue cherished political and social ambitions (Williams, 2008:6). According to Paime (1992:9), "there is a correlation between security and survival". Whereas survival is an essential condition, security is viewed as safety, confidence, free from danger, fear, doubt, among others. Therefore, security is 'survival-plus' and the word 'plus' could be understood from the standpoint of being able to enjoy some freedom from life- determining threats and some life choices (Booth, 2007: 15).

However, the concept - security, is meaningless without a critical discourse of something pertinent to secure. Indeed, security could best be understood when situated within the context of a referent object. In the long sweep of human history, the central focus of security has been people (Rothschild, 1995:68). Contrarily, some scholars especially those in international politics have argued that when thinking about security, states should be the most important referents. On the other hand, some analysts have challenged this position by arguing that any intellectual discourse on security should accord priority to human beings since without reference to individual humans, security makes no sense (McSweeney, 1999:127).

Nwagboso (2012) examines the security challenges in Nigeria and the extent to which the insurgencies of different militia groups as well as the prevailing internal insurrections across the country have adversely affected the Nigerian economy from 2007-2011. He opines further that our security strategy should not only focus on safeguarding the lives of the citizens, but also to achieve the desired economic growth and development in the state.

The security situation between 2007 and 2012 in Nigeria obviously took different dimensions. This period, however, witnessed a consistent pressure on the government by Movement for the Emancipation of the Niger Delta (MEND), Movement for the Sovereign State of Biafra (MOSSOB), increasing spate of kidnapping in the South - East geo – political zone, incessant bombings in the northern parts of Nigeria by Boko Haran group, Mayhem by the Islamic assailants in Jos crisis, politically motivated killings by unscrupulous groups, among others (Ameh, 2008:9). Perhaps, a critical look at table 1 helps in the concise understanding of security threats in Nigeria from 2007-2012. It encapsulates findings of case studies based on observation and review of relevant literatures. The research survey spanned network news monitoring on local electronic media like NTA (9 pm Network News belt), FRCN (7 am, 4 pm and 10 pm Radio Nigeria Network News belts) and Nigerian Info (Hourly news belts).

Although the achievement of total or absolute security in Nigeria is a difficult but achievable milestone, the contemporary security challenges in the country have not only raised critical questions bordering on formulation and implementation of Nigeria's internal security policies but also the incorporation of social security as a lasting and long term solution to insurgencies. There is no gainsaying the fact that military tactics like show of force, Police's operation fire for fire and outright use of brute force cannot march systemic and systematic wealth redistribution strategy as canvassed by social security scheme in curbing the burning issue of insecurity in the long run.

*Table 1: Select security threats in Nigeria and originating zones*

| SN | Security threat | Period | Geo-political zone |
|---|---|---|---|
| 1. | Niger Delta | 1999-2007 | South-South |
| 2. | Jos crisis | 2001- to date | North-central |
| 3. | Kidnapping, ritual killing and armed robbery | 2007- to date | South- East, South-West |
| 4. | Boko Haram crisis | 2009 – to date | North – east, North-central and North-West |

*Source: Okewu's case studies, 2012 using observation and literature review*

Social security refers to the action programmes of government intended to promote the welfare of the population through assistance measures guaranteeing access to sufficient resources for food and shelter and to promote health and wellbeing for the population at large and potentially vulnerable segments such as children, the elderly, the sick and the unemployed. Services providing social security are often called social services.

## 2. RELATED WORK

Nwagboso (2012) relies on the Democratic Peace Thesis and the Relative Deprivation Theory to explain the security challenges and economy of the Nigerian State. He argues that for Nigeria to address her perennial security challenges, the need to adopt and faithfully implement strategic security policies and viable socio economic programmes capable of strengthening the growth of democracy in Nigeria are the first step to be adopted by government. The increasing spate of security threats in Nigeria which if unchecked could further distort the country's economy is clearly indicative of the abysmal failure of the institutions constitutionally charged with the responsibility of protecting the lives and properties of Nigerian citizens (Dinneya, 2006:47).

By application, this theory assists us to trace the historical antecedence of conflicts, agitations and frequent rise of individuals and groups against the Nigerian government. From the standpoint of the assumptions of Relative Deprivation Theory, scholars argue that the abysmal failure of the Nigerian government to addressing critical challenges of development in many parts of the country may be responsible for the internal insurrection by armed militia groups against the state. Further, they equally argue that security challenges or threats in some parts of Nigeria particularly the northern region, are clear indications that government seems to have failed in her constitutional role of protecting lives and properties of the Nigerian people. This is clearly because, available evidence demonstrates that there is increasing rate of poverty among Nigerians. Also, unemployment looms large, per capita income is low and high rate of inflation has not be addressed. Similarly, Nigerians are still facing challenges of poor health status, poor state of infrastructures, high rate of illiteracy, low technological development, among others (Anosike, 2010:8).

These ugly situations which adversely affect the security of lives and property of Nigerians as well as socioeconomic development of the country are carefully articulated by Akinrefon and Oke (2007:20).

Apparently, as part of efforts to live up to its contractual role in citizens service delivery, governments embark on such programmes to implement social security scheme that will provide health care and financial assistance to the poorest indigenes and residents of their areas of jurisdiction. Health care assistance can be in the form of free health care for pregnant women and children under the age of 5. Financial assistance comes in the form of conditional cash transfers to poor households to support the education of their children and supplementing of their meager incomes to effectively support their families.

## 3. METHODOLOGY

According to the International Labour Organization, social protection has proven to be a powerful anti-crisis measure. It protects and empowers people, and contributes to boosting economic demand and accelerates recovery. It is also a foundation for sustainable and inclusive economic growth. The absence of solid national social security scheme in Nigeria 52 years after independence despite the country being an active player in the International Labour Organisation's (ILO) affairs and playing host to the labour watchdog since 1960 is indeed worrisome. However, some efforts have been made and should be acknowledged.

In October 2011, Ekiti State in south-west Nigeria established a social pension scheme aimed at providing a minimum level of security to older generations. The only qualifying criteria are that recipients must be over the age of 65 and must have been a resident in Ekiti for at least three years.

As of May 2012, 20,000 elderly people were in receipt of this pension, which entitles them to N5000 (five thousand naira) a month. And following the signing of the Social Security Bill in Ekiti State this social pension scheme now has a legal backing which will ensure its sustainability. Table 2 profiles findings of a field survey using observation and literature review of secondary materials. The research survey encompassed network news monitoring on local electronic media like NTA (9 pm Network News belt), FRCN (7 am, 4 pm and 10 pm Radio Nigeria Network News belts) and Nigerian Info (Hourly news belts).

Nine months after the first payments were made in Ekiti State, its neighbour Osun State announced the implementation of a monthly pension of N10,000 (ten thousand naira) to 1,602 older people who have been identified as the most vulnerable. It also includes the provision of some medical treatment for recipients. At nearly 50% of the national average income, Osun's pension scheme is, in relative terms, the second most generous social pension in the world.

Regardless of their shortcomings, the introduction of these pension systems - the first of their kind in Nigeria - marks a major step forward in providing a minimum income to older people. And with calls for social protection increasing, these pensions have garnered interest from local and national organizations and individuals. Already, many states in Nigeria have approached Ekiti State to learn more about, and potentially adopt the scheme.

Table 2: Select social security programmes in Nigeria

| SN | Code Name | Government | Type | Target | Commencement date | Status | Supervising ministry |
|---|---|---|---|---|---|---|---|
| 1. | SURE-P (Subsidy Reinvestment Programme) | Federal Government | Safety-net tagged Community Service Scheme (CSS) | Women, disabled and unemployed | 2012 | Take-off stage – capacity building and empowerment of women, unemployed youths and disabled. Stipends and seed money offered. | Ministry of Labour and Productivity |
| 2. | National Social Insurance Trust Fund | Federal Government | Social insurance | All categories | 1961 | Passive – the common man is yet to feel its impact | Fed. Min. of Labour & Productivity |
| 3. | Social Security | Ekiti State | Social pension | The elderly – 65 years and above | October 2011 | Functional – beneficiaries receive monthly stipend of 5,000 naira | State Ministry Labour, Productivity and Human Capital Development |
| 4. | Project Comfort | Cross River | Safety Net – conditional cash transfer | Poor (vulnerable) households | 2012 | Functional - beneficiaries receive monthly stipend of 5,000 naira | State Ministry of Social Welfare |
| 5. | *Agba Osun* | Osun State | Social pension | The elderly – 65 years and above | November 2012 | Functional - beneficiaries receive monthly stipend of 5,000 naira | Office of the Governor |
| 6. | National Health Insurance Scheme (NHIS) | Federal Government | Social protection | All ages | 1989 | Passive – the common man is yet to feel its impact | Fed. Min. of Health |
| 7. | Project Hope | Cross River | Safety Net – free health care services | Women and children under 5 years | 2012 | Functional – 7 local governments receiving free health care | State Ministry of Social Welfare |

*Source: Okewu's field survey, 2012 using observation and literature review.*

One remarkable advance in Cross River State is Project Hope and Project Comfort, two safety nets designed to achieve transformation of the welfare of the vulnerable and underprivileged in the state. Project Hope is about free health services for women and children under the age of five while Project Comfort involves cash transfer for vulnerable households with 6,000 poor households empowered under the social security safety net called Conditional Cash Transfer (CCT). The households are beneficiaries of the N5,000 monthly stipend from the government.

Out of 18 local governments in the State, seven are receiving free healthcare from the State Government. Bekwara, Abi, Obudu, Obubra and Ikom are currently enjoying these services. With the application of biometric mechanism, the State Government, in collaboration with an Indian Foundation, has recorded the first ever zero infant / maternal deaths in Bekwarra and Obubra local government areas in 2010-2011 and 2011 and 2012 accounting periods, respectively.

Irrespective of the amounts being paid to these elderly people, it is a good starting point towards being responsible to the citizens as far as meeting the provision of the Universal Declaration of Human Rights is concerned.

Yet another social security scheme is the Nigeria Social Insurance Trust Fund (NSITF).It is an organization with the mandate to facilitate the implementation of the social security program of the Federal Government. The scheme is to take a holistic look at best practice in most developed countries and domesticate. The social protection scheme courtesy NSITF, is mandated to deliver social security to the poor - help address poverty and social ills that may result from neglect. The unemployed, the elderly, those physically challenged and people who are socially disadvantaged are to be cared for. The Nigerian Social Insurance Trust Fund is empowered vide Section 71 (2) of the Pension Reform Act 2004 and Section 16 of the NSITF Act 1993 to provide these social security services for Nigerians.

The National Health Insurance Scheme (NHIS) is another social security scheme of the federal government. Through the NHIS, government hopes to achieve more flexible, more innovative, and more competitive response to the health sector in order to ensure that every Nigerian has access to good health care services.

## 4. SIMULATION/IMPLEMENTATION

For this implementation, the social benefit scheme encompasses free medical care and conditional cash transfer.

### 4.1 Design and Implementation

To ensure credibility and nip in bud fraudulent activities in social security initiatives, government needs the services of ICT (Information and Communication Technology). As Ndeh-Che (2008:8) observes, there is need to engage the services of reputable Systems Integrators for the integration of a reliable system for identifying and registering eligible beneficiaries, and to setup systems to support delivery of benefits, accounting for benefits, and monitoring and evaluation of the Social Benefit Scheme.Accordingly, effort is geared towards production of systems, processes and human resource requirements which will serve as an information platform; and as a service delivery medium for all stakeholders.

Systems integrator firms are saddled with the provision of systems integration services as needed by the government. They will assist government in the conceptualization, analysis, design, development, and deployment and maintenance of information systems that will ensure effective and secure management of the benefits scheme including, inter alia, (a) enrolment system for bona-fide beneficiaries, (b) biometric identity management and verification, (c) ID card production, and (d) system for the accounting of benefits.

To achieve this objective, system integrators need to possess a deep understanding of, and the resources for, the analysis, design, development, deployment and maintenance of the systems and processes for the social security programme. Equally important, they have to demonstrate proven track record of outstanding work in the area of biometric enrolment and verification, as well application development, deployment and integration.

For such social security engagement, the scope of work will include:

1. Software and services for development and deployment of biometric enrolment system and training of technical personnel and provision of technical support during verification and enrolment effort – Provision of systems integration expertise to ensure accurate data capture for potential beneficiaries of the Social Benefit Scheme. Personal and biometric data are captured and stored in a relational database system. Human error can be mitigated by using state-of-art forms processing systems, whilst time-tested biometric approach shall eliminate multiple enrolments of the same individual. During the exercise, beneficiaries will also have their supporting documents scanned, converted into e-forms and archived in a document management system. Support team will be on ground throughout, in order to ensure that the enrolment exercise runs smoothly. After the initial phase of the verification and enrolment exercise, continuous verification and enrolment will continue to ensure that new potential beneficiaries are properly verified and registered. Figure 3 and Figure 4 highlight enrolment infrastructure and enrolment process respectively.
2. Systems integration for biometric enrolment database and identity management system –Sufficient systems integration expertise should be deployed to ensure that after field enrolment, the various biometric enrolment databases from enrolment centres, the scanned documents and the e-forms, are consolidated in a central database. To avoid duplicate enrolments across enrolment centres, an Automated Fingerprint Identification System (AFIS) should be deployed.

   An identity management system can be set up, based on the consolidated database, to provide identification services. Figures 5 and 6 respectively model a consolidated view and the consolidation process.

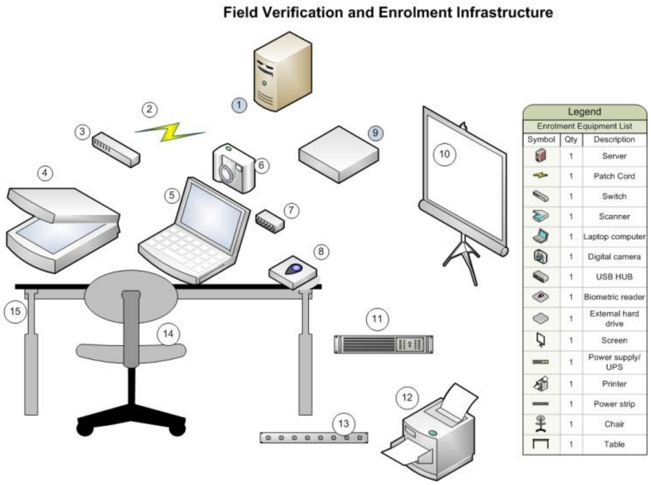


*Figure 3: The enrolment infrastructure for an enrolment centre*

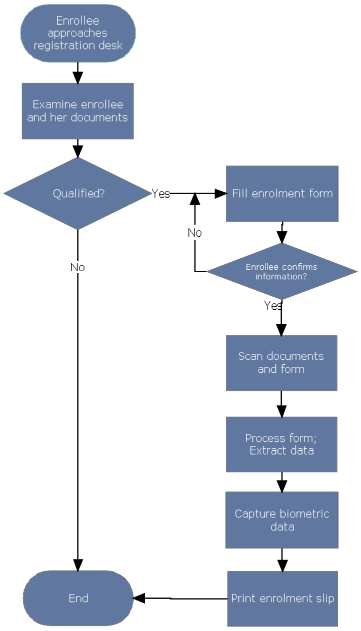

Enrollee approaches registration desk
Examine enrollee and her documents
Qualified?
Yes
No
Fill enrolment form
No
Enrollee confirms information?
Yes
Scan documents and form
Process form; Extract data
Capture biometric data
Print enrolment slip
End

*Figure 4: The enrolment process*

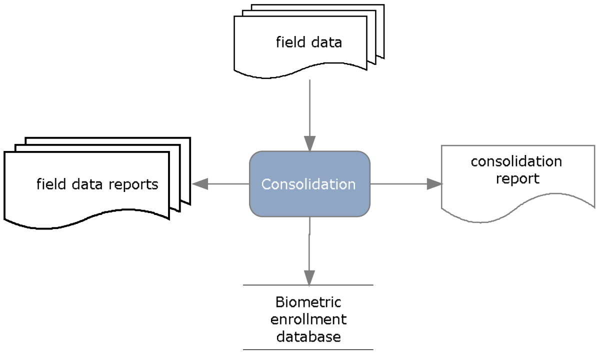


*Figure 5: Consolidated view*

3. Systems integration for ID card production, card acceptance devices and identity verification system – Interestingly, a possible fall-out of the excerise is the production of authentic identity card (ID card).Beneficiaries can be provided with secure smart ID cards as proof of eligibility to receive benefits. Each card contains biometric information to verify the beneficiary on location, as well as other data as may be decided from time to time by the government. It is worthy of note that in the absence of the ID card, verification will still be possible over a remote connection to the central identity system.

A production station should be set up for the design and production of the smart ID cards. The ID cards and ID card verification systems should be deployed at strategic locations (e.g. Benefits Stations) to prevent abuse of the scheme. Figure 7 shows a quintessential card printing infrastructure just as Figure 8 presents an ID card-enabled verification process. In the event a beneficiary has no card, he/she can still be verified remotely using finger print as captured in Figure 9.

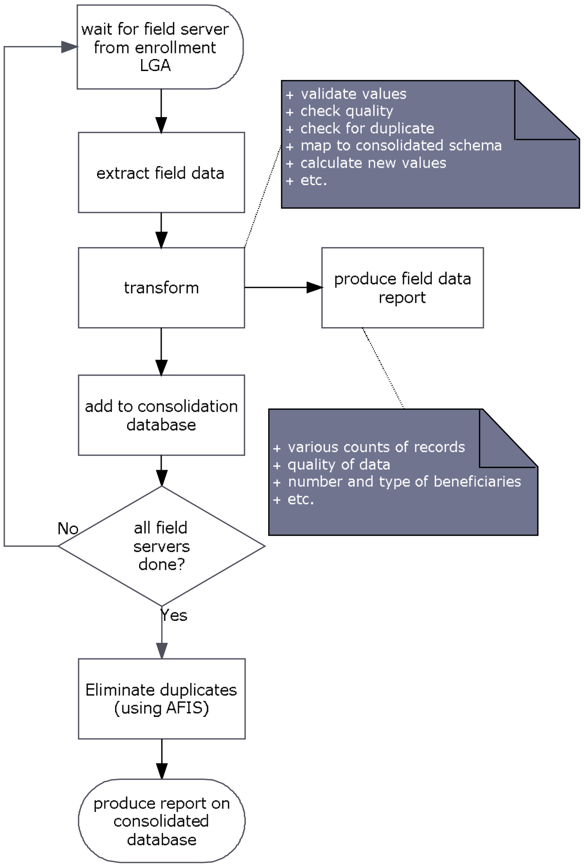

wait for field server from enrollment LGA
extract field data
transform
produce field data report
add to consolidation database
all field servers done?
No
Yes
Eliminate duplicates (using AFIS)
produce report on consolidated database
+ validate values
+ check quality
+ check for duplicate
+ map to consolidated schema
+ calculate new values
+ etc.
+ various counts of records
+ quality of data
+ number and type of beneficiaries
+ etc.

*Figure 6: Consolidation process*

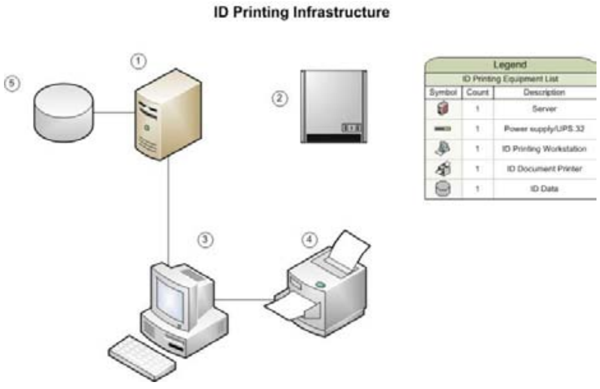


*Figure 7: Card printing infrastructure*

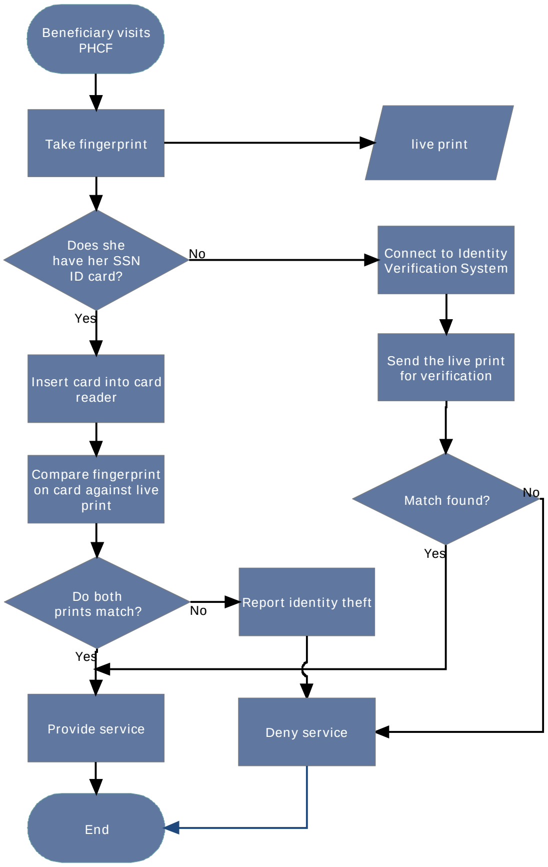

Beneficiary visits PHCF
Take fingerprint
live print
Does she have her SSN ID card?
No
Yes
Connect to Identity Verification System
Send the live print for verification
Insert card into card reader
Compare fingerprint on card against live print
Match found?
No
Yes
Do both prints match?
No
Yes
Report identity theft
Provide service
Deny service
End

*Figure 8: ID Card Verification Process*

Figure 9: Identity verification process

4. Software and services for development and deployment of Benefits Accounting System – In order to ensure proper management of benefits accruing to citizens under any social security scheme, system integrators should partner with the government to develop a benefits administration system. This system will be custom-built to

suit the specific requirements of the respective social safety net programme.

5. Technical and End-User Training – The need for adequate capacity building cannot be overemphasized. System Integration firms should provide comprehensive capacity building services to ensure that all human resources participating in the social protection programme are able to carry out their roles and responsibilities. Training categories could include i) Enrolment Officers, ii) Identity Management System Administrators, iii) Benefits Administration System End Users and iv) Benefits Administration Support Personnel.
6. Ongoing Support and Maintenance – To ensure smooth running of all systems deployed, the system integrator will provide ongoing support and maintenance services to the government.

The firm should deploy a multi-disciplinary team of professionals and support personnel, working over a stated period to complete and roll-out the systems for the scheme. Emphasis should be placed on the engagement of a reputable firm to assist the government in realizing its vision of free health care for, and financial assistance to the under-privileged. References of track record of successfully delivering expected project outcomes in similar engagements for other clients should be taken into cognizance. The firm should understand the challenges, possess the skill sets and emphasize client collaboration. Modalities should be put in place to guarantee fruitful working relationship between the firm and government.

### 4.2 Critical Scheme Success Factors

Ndeh-Che (2008:15) outlines the following measures for success.

- Establishment of a uniform, clearly defined and objective criteria for determining eligibility for the scheme
- Collection of realistic baseline data on poverty for target setting
- Establishment of realistic targets and timeframes
- Establishment of a comprehensive Monitoring & Evaluation (M&E) Framework for all aspects of the scheme
- Sensitization of beneficiaries and stakeholders
- Institutionalizing transparency, accountability and good corporate governance in the scheme from the onset.
- Proper identification and registration of beneficiaries using the latest advances in identity management technologies
- Adoption of a holistic approach to achieving scheme objectives
- Reuse of data and resources from complementary initiatives such as census data and images and Roll Back Malaria initiative

## 5. CONCLUSION

Though the social security scheme is a new concept in Africa and indeed in Nigeria, it has come to stay. Countries like Zambia, South Africa, Libya and Egypt have edged in social security programmes for citizens. As Nigeria joins the league of countries whose governments' execute socially responsible programmes for need-based citizens, it will gather lost confidence from citizens with far-flung expectations. And more importantly, idle minds will be engaged productively hence mitigating the chances of such citizens being indoctrinated and used as foot soldiers for fuelling crisis.

## REFERENCES

Akinrefon, D. and Oke, G., 2007. Why insecurity and democracy don't mix. Vanguard Newspaper, August 20, pp.20.

Akinterinwa, B. A., 2001. US national security strategy and Nigeria. The Nigerian Voice Newspaper, February 24.pp. 2.

Alade, A., 2012. Operation Capture Boko Haram Leader. Saturday Sun Newspaper November 17, pp.15.

Ameh, J., 2008. Nigeria under security threats from Jetties - Reps. The Punch Newspaper, September 4, pp. 9.

Anosike, P., 2010. Ohanaeze tasks FG on security. Daily Sun Newspaper, October 6, pp. 8.

Booth, K., 2007. Theory of world security. London; Cambridge University Press.

Davies, J. C., 1962. Towards a theory of revolution. American Sociological Review, (27), 5 - 19

Dinneya, G., 2006. Political economy of democratization. Lagos: Concept Publications.

Edukugho, E., 2012. Unemployment: Nigeria sitting on keg of gun-powder. Vanguard Newspaper November 17.pp.7

Feierabend, 1. & Feierabend, R., 1966.Aggressive behaviour within polities: A cross-national study (1948 - 1962). Journal of Conflict Resolution. (10: 249 – 272).

McSweeney, B. (1999). Security, identity and interests: Asociology of international relations. London: Cambridge University Press.

Ndeh-Che, F., 2008. Positioning Cross River State Government to Deliver a World Class Social Safety Net Program. A Technical Proposal. Abuja, Nigeria.

Nwagboso, C.,Security Challenges and Economy of the Nigerian State (2007 – 2011). American International Journal of Contemporary Research Vol. 2 No. 6; June 2012

Paime, M. A., (1992). Guardians of the gulf. New York: Free Press.

Rothschild, E. (1995). What is security. New York: Columbia University Press.

William, P. D. (2008). Security studies: An introduction (ed.). New York: Routledge.

Full Paper

# E-GOVERNANCE SMARTNOTICE: A WIRELESS RF PROXEMIC DISPLAY SYSTEM

**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
udezechidiebele@yahoo.com

**M. C. Ndinechi**
Electronics Development Institute, Awka,
National Agency for Science and Engineering Infrastructure,
Federal Ministry of Science and Technology
mike4god@yahoo.com

## ABSTRACT

E-Government Automation Processes (e-GAP) and Smart Governance (SG) through the use of Information Technology (IT) in citizens service delivery is gradually gaining wide acceptance in the 21st century. In this respect, this research work develops and presents an e-Governance SmartNotice Board (e-GSNB) which can be widely used for remote information dissemination (e-Government Dimensions) and used for multitude of applications in the educational sector, traffic control, public advertisements, etc. Essentially, this research carried out an investigation on independent radio transmitter-receiver model using MATLAB Simulink to show a two case scenario where a proposed Signal Processing Block (SPB) could help to address SMS text data quality and channel error correction. Our overall methodology is detailed in the body of the work.

**Keywords:** *e-Government, Information Technology , SPB, Proxemic, Citizens*

## 1. INTRODUCTION

Contemporarily, e-government is at the implementation stage in various countries of the world. E-governance creates digital interactions via ICTs between Government to citizens, employees, business and agencies. The E-Governance platform needs low cost and high speed infrastructure which must provide high quality transmission (data, video and voice traffic) and reliable connectivity with efficient service delivery [Okafor et al].The developing nations needs an optimized integrated architecture framework for e-government that represents the alignment of newest IT infrastructure with business process management in public sector organizations and clearly understand the implementation constraints of the proposed architecture framework. This research contributes to literature in the E-Government models, helping experts to learn how to use and manage the contemporary 4G Long Term Evolution (LTE) information technologies to revitalize business processes, improve decision-making, and gain a competitive advantage from the adoption of e-government. The e-Governance SmartNotice which is Proxemic Cognitive Intelligent Display System depends on GSM Radio Link as presented in this paper, will eradicate complications surrounding e-government infrastructure deployment models (see figure 1). An understanding of the proposed e-government processes and flowchart model, as well as performance analysis of a SPB model in this work will validate e-government display automation processes. Table1 shows the proposed implementation framework for both e-government system modules and dimensions.

What Is E-Government?

The work in [Okafor et al] observes that the term e-government in the context of the developing counties is of recent origin and there exists no standard definition since the conceptual understanding is still evolving. However, the website in [www.en.wikipedia.org/wiki/e-government] defines E-Government as a digital interactions between a government and citizens (G2C), government and businesses/Commerce (G2B), government and employees (G2E), and also between government and governments/agencies (G2G). In the world today, the use of ICTs by government agencies is necessitated by the following reasons [Okafor K.C et al]:

Need for exchange of information with employees, citizens, businesses and other government departments

Need for efficient delivery of public services while reducing systematic rigidities and paperwork

Need to improve internal efficiency and avoid over-centralization

Need for cost savings and increase revenue generation

Need to re-structure the administrative processes, hence reducing bureaucratic routine

Need for accountability and transparency

Need for absolute convenience via mobile based service deliveries, home delivery of processed papers, no need for office

*Table 1: E-Government dimensions*

| E-Government Dimensions | | Modules |
|---|---|---|
| Infrastructure | [ Frame work Readiness ] | -Mobile Infrastructure<br>-Broadband Infrastructure<br>Wimax 802.16e + LTE 4G |
| Policy | | -Laws on E-Government Security<br>-Institutional Models of E-Government |
| Governance | | -ICT backoffice for E-Government<br>-Reengineering Public Processes |
| Outreach Service Models | | - E-Government Services to Citizens [G2C]<br>- E-Government Services to Bussiness [G2B]<br>- Interagency E-Government Services [G2G]<br>- E-Government Services to Employees [G2E]<br>- E-Government Services from Citizens to Governments) [C2G] |

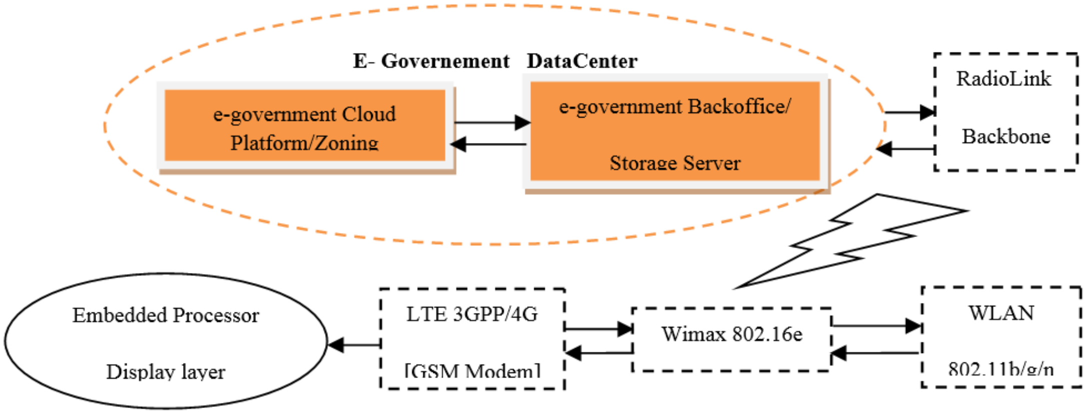

E- Governement DataCenter
e-government Cloud Platform/Zoning
e-government Backoffice/ Storage Server
RadioLink Backbone
Embedded Processor Display layer
LTE 3GPP/4G [GSM Modem]
Wimax 802.16e
WLAN 802.11b/g/n

*Figure 1: e-government Smart Infrastructure Model (SIM)*

visits and follow ups, no need to approach different offices for different work, clarity on requirements.

According to [Zakareya et al, 2004], E-government refers to the delivery of government information and services online through the Internet or other digital means. Accordingly, government leaders and officials are increasingly aware of the potential of e-government to improve the performance of government organizations and provide potential benefits to their citizens and business partners [Zakareya et al, 2005]. The study in [Moon, M.J, 2002] shows that e-government is still at the rudimentary stage and has not obtained many of the expected outcomes in terms of cost savings. Horizontal and vertical interoperability can be regarded as the key to realizing the potential gains in e-government [Hans's. et al, 2012]. For all classes of the e-Government delivery models, the e-GSNB certifies the interoperability functionalities. Essentially, the e-Government delivery models can be briefly summed up as showed in [Jeong, 2007] viz:

G2C (Government to Citizens)
G2B (Government to Businesses)
G2E (Government to Employees)
G2G (Government to Governments)
C2G (Citizens to Governments)

Essentially, this research makes a novel contribution to e-governance strategy by implementing a prototype e-GSNB while carrying out an investigation on independent radio transmitter-receiver model using MATLAB Simulink to show a two case scenario where a proposed Signal Processing Block could help to address SMS text data quality and channel error correction. Upon validations of the SPB, a prototype system implementation was developed and tested considering time-to-market. The display algorithm leveraged on a Audience Funnel framework (AFF) and Proxemic Peddler Frameworks (PPF) which stipulates that public displays should attract, and sustain cognitive attention to the point of internalizing the information displayed. In our design, (future work), by integrating SIM 300(GSM Modulator) with MAX 232 interface to an ASIC embedded processor,(AT8285), Windows 7 OS hyperterminal was connected the GSM HSPDA modem via AT command. Upon authentication, the GSM SMS cloud forwards an SMS text to a wireless GSM receiver interface (MODEM). The AT8285 then displays the remote information on the proxemic display module. This system offers numerous advantages compared with other existing displays systems. In its architecture, we seek to control the proxemic out door display unit using a reliable, but secured wireless communication between a GSM MODEM Modulator-Demodulator) and an embedded processor using GSM (Global System for Mobile Communication) module.

## 2. RELATED WORKS

In this e-governance era, digital signboards (public display systems) have the ability to display anything which a television or computer monitor can, including moving images. This section reviewed various works on public display designs.

[Fahmy. et al, 2010] presented and designed a textual display system, based on a light emitting diode (LED) dot matrix array powered by solar energy as shown in figure 2. The work involved taking the device from an initial concept, through a design phase, to constructing a prototype of the product. The system consists of the display unit, which is powered from a photovoltaic (PV) module and a solar sealed lead acid battery. The authors claimed that the self-contained nature of the design allows the display to be mounted almost anywhere it is needed. The work utilized solar energy and a rechargeable battery to power a universal self-contained characters display unit. This display unit is useful for creating attention-getting messages, location identifiers such as maps and address identification display modules. The implementation of the moving message display can only display a text containing 22 characters (i.e., PHOTOVOLTAIC DEPARTMENT), and is powered by a PV module has been achieved. The control of the panel is based on an Atmega 8515 a Microcontroller which runs on Assembly language, through an AVR studio software and STK500 kit. The photovoltaic module charges the battery during the day and the battery is continuously feeds the display panel. The major advantage of the designed display system is that it is easy to set up, program and handle, it also allows the outlet to simply and clearly present the scrolled text.

[O'Hara. et al. 2001] presented a way of designing a digital noticeboard by programming and reprogramming the board using a PC, though the system does not offer real time dissimination of information and the stress involved in having to reprogram the board every time information is to be passed. [Hara.M.w., 2009] presented a community based digital bulletin boards and mobile phone interaction which is a better improvement to the work by [O'Hara. et al. 2001].

The work is based on the use of bluetooth protocol for interaction between the user and the board. The work offers low cost, less power consumption and less complexity, but it has two drawbacks viz: System Inflexibility and distance limitations.

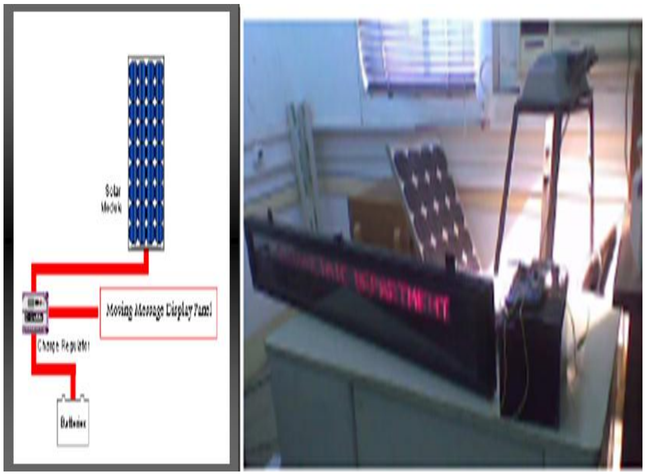


Figure 2: Striped Photovoltaic display testbed
*[Fahmy. et al, 2010]*

A better solution proffered by [Wei et al, 2008] tried to solve this problem of distance limitation. In their work, an authorized user can quickly access the system and update the information to the display through internet using simple web browser without any client-side application software. The update information is passed from user to the web controller using TCP/IP protocol. Then, the web controller generates chains of pulses to the IR module to control the LED panel which displays the message. The complexity of this system makes it hard for easy deployment.

Zigbee based wireless electronics notice board [www.wineyardProjects. Com.], and [Lonn.,et al,2011] used zigbee protocol to design a wireless notice board. Zigbee devices have the ability to form a mesh network between nodes, this technique allows the short range of an individual node to be expanded and multiplied covering a much larger area. Alphanumeric keyboards is interfaced to the transmitter to type the data and transmit, the messages can be transmitted to multipoint receivers.

However, the author [Zohedi.,2011] did a remarkable work of wireless electronics notice board. The system is based on an SMS remote controller. Their goal was to develop an embedded system which can control up to eight devices remotely by sending a specific SMS from a cell phone. The system consists of two modules; transmitter and receiver. The transmitter module is used by a user to place a message through an input module such as keypad or keyboard. The information is then transmitted using RF technology to the receiver. It then will be decoded and displayed on electronic notice board. The user controls the notice board within a 25m range and information is transmitted using RF as wireless technique. The only obvious limitation of this system is that it does not allow for remote access for the control of the board.

All the works discussed so far has two major limitations; their short range nature and the fact that they do not offer remote access. If one can find a way of controlling the board from a very far remote place, then it is possible to make it truly wireless. Also, we observed that there have been several works done on the use of SMS technology for remote control of devices. If GSM technology can be used in appliance control, this work argues that it can as well be used it to control a notice board. In [Lonn.S.,et al,2011], design and implementation of short message service based remote controller was considered. The work focused on controlling home appliances remotely when the user is away at home with the use of SMS.

The work in [Sri et al,2007], the presents a project which aims at integrating the expansiveness of a wireless cellular network and the ease of information transfer through the SMS with the coverage of public display boards. It facilitates a modest effort to realize the complete potential of public display boards in instantaneous information broadcast in swift response to events of interests. The display board used commercially is depicted in figure 4. The input requirement for such kind of display boards are 120/240 VAC 50//60 Hz with internal circuit breaker sized per sign layout.

In their work in [Sri R.M.,et al,2007], the display board is huge in size and so LCD displays was used for testing. The work used AT commands for interfacing a MODEM with a normal PC via Hyper Terminal window.

Though their MODEM interface requires a wired connection at one end and wireless at the other, and hence employed Philips P89C51RD2BN microcontroller with 64 Kb EEROM storage memory. It was observed that the complexity of the coding substantially increased, but still retained its functionality at its robust best since it is a dedicated embedded system. The design procedure involved identifying and assembling all the required hardware and ensuring fail safe interfacing between all the components. However, the work lacked security authentication, and failed to explain how data transmission errors can be mitigated.

Figure. 4: A Commercial display board [Sri et al,2007]

Again, designing a public display that could actively communicate with passerby people will gain wider acceptance index. Prior works [Vogel et al, 2004],[E. M. Huang, et al,2008],[J.Müller.et al,2010], and [ N. Streitz, T. et al, 2003] mostly focused on how a display can assist users in obtaining information. For example, Vogel et al.'s interactive display [Vogel. D. et al, 2004] showed calendar information in different levels of detail according to a user's presence in proximity regions. This system's main role was to present information in the optimum format for viewing at various locations, where it smoothly moves from a peripheral to foreground display as a result of satisfying a user's intent.

This paper seeks to develop a different design model whereby the display takes more control in Attention & Attraction (A&A).In this case, it tries to (more assertively) satisfy its goal of communicating its content to a the public citizens. The display takes the initiative by engaging people's behavior at each viewing and attention interaction phases. Our intent is to have the passerby focus on the public information content from any location.

Our approach in the implementation follows from the Audience Funnel and the Peddler Proxemic Frameworks[J.Müller.et al,2010],[W.Ju,et al, 2008].The Audience Funnel describes six phases [J.Müller.et al,2010], as shown by the first six positions in Figure 5: a) passing by, b) viewing & reacting, c) subtle interaction, d) direction interaction, e) multiple interactions, f) follow-up action. With the Peddler Framework, three extensions were made to the Audience Funnel framework that addresses the three limitations identified above: continuous interaction, users' interaction history, and user digression.

Having reviewed existing systems, this work firstly shows their limitations which greatly reduced efficiency and effectiveness viz:

### 2.1. Limitations of Existing Systems

- he existing display systems do not offer real time dissemination of information
- The existing systems do not offer remote access to the display board
- The systems lack Attention and Attraction frameworks hence creating little impact.
- The systems have high errors and poor resolutions resulting from the display technologies used.

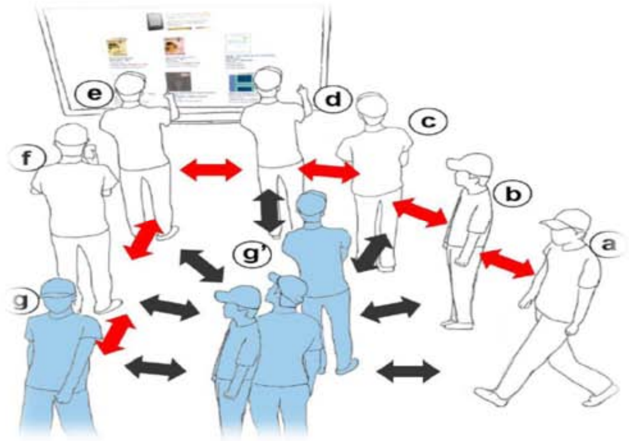


*Figure 5: A passerby in various different attentional states with respect to a public display: a) passing by, b) viewing & reacting, c) subtle interaction, d) direct interaction, e) multiple interaction, f) follow-up action, g') user digression, g)*

An e-governance smart display model (e-GSNB) is then proposed which has cognitive characteristics based on AFF, and proximity peddler in general. However, this paper will focus on the impact of the SPB on system. In our prototype design, the system will leverage SPB while utilizing composite algorithms to support intelligent continuous interaction, interaction history, and response to user digression. This extended modification will make the display system very intelligent while showing a new design foundation for a public display system that can attract and maintain users attentions.

## 3. METHODOLOGY

A concurrent engineering approach was employed in this research. Firstly, before implementing our system prototype as part of our future work, we first investigated on channel error constraints and bit error rate in the transmitter receive interfaces. It is well known that channel errors in the radio channel can affects the SMS text data quality, hence by considering independent radio characterizations of the transmitter and receiver units. In this regard, a simulation model for this senario is developed in MATLAB Simulink version 7.9 [http://www.mathworks.com] while a GSM simulation

senario was still built with OPNET Modeller 9.1[C.-H. Ng, et al, 2002] which demonstrates the flows in a typical GSM mobile architecture. For the Transceiver unit, we used the communication blockset in the MATLAB Simulink tool box to setup the model while introducing a two case scenario for SPBs. The simulation models (later in this work) demonstrated the impact of a SPB in addressing channel errors that could affect the SMS text data. (See figures 10).

The result of this research will led to developing a proposed low-cost embedded intelligent system that is based on AT82S89 controller processor. The system will comprise of GSM SIM 300 modem, MAX 232 and LCD digital display system for Smart e-governance.

### 3.1. DESIGN FORMULATIONS

*3.1.1. Transceiver GMSK Independent Radio Characterization*

The functional modulation block for our SMS data propagation is the Gaussian minimum shift key. In this research, an investigation into the design properties of GSM transceiver leading to the model for computing error performance after the IF and SPB is further discussed. The model basically accounts for:

1. Receiver sensitivity with different error measures (BER, RBER, FER)
2. Frequency and phase error of the modulator
3. Transmitter timing errors

From the baseband frequency, the ultimate goal of the GMSK modulation technique is to transport the SMS signal through a radio channel with the best possible quality while occupying the least amount of radio spectrum. Consider SMS message:

$$D(t) \rightarrow (t) = Acos(wt+\square) \rightarrow Channel.$$

where D(t) is the message, Acos(wt+θ) is the modulation. By using the GSMK for modeling the GSM Modem, its benefits are: constant envelope, spectral efficiency, good BER performance and self-synchronizing capability. GMSK is a spectrally efficient modulation scheme with an expression for the Modulated Signal x(t) is given by

$$x(t) = \cos(2\square\square\square\square + \square(\square))$$

Where θ(t)=Continous phase shift function, Hence the GMSK uses a frequency shaping filterlation index h =1/2, which is defined by the continuous phase shift function θ(t). After the signal is passed through the radio channel, at the receiver, the signal is received along with noise. After synchronization, down-sampling, and removal of the CP, the simplified baseband model of the received samples can be formulated [Yucek. T., et al, 2007] as:

$$y(n) = \sum_{\square\square\,\square}^{\square\square\,\square} \square\square\square - \square\square\square\square\square + \square(\square)$$

where L is the number of sample-spaced channel taps, w(n) is the additive white Gaussian noise (AWGN) sample and the h(l), is given as a time-invariant linear filter. It is worthy to note that perfect time and frequency synchronization is assumed. In this case, after taking FFT of the received signal y(n), the samples in frequency domain can be written as

$$y(i,k) = x(i,k)H(i,k) + W(i,k)$$

where H and W are FFTs of h and w respectively.

This work considered AWGN channel optimization for miminal SMS drop rate or channel reliability. From figure 7 and figure 8, the introduced SPB is modeled as a Raised Cosine (RC) filter which belongs to the class of filters which satisfy the Nyquist criterion.

## 4. SIMLULATION FORMULATIONS

### 4.1. Radio Model For Data Propagation

In this research, addressing reliable delivery of SMS data for the proxemics display system now focused our design of the GMSK Modem for SMS text reliable data delivery. The transmitter model was modeled to include convolutional coding and GMSK modulation. In the receiver model, SPB was introduced with a test branch consisting of two parallel paths, one that uses soft decisions (SPB Soft decisions) and another that uses no SPB soft decisions. The model depicts SMS transmission by the GMSK transmitter and a GSM GSMK receiver module with a coded GMSK SMS signal. The radio model of an SMS text transmitter reciever model is developed with MATLAB Simulink 2009b using the parameters of Table 4.1. The two cases above were harnessed in the MATLAB Simulink model.

### 4.2. Physical Layer Model For Composite SPB

In this case, the SMS data source is a bernoulli binary generator configured to generate output vector which goes to the radio encoder module for modulation process using convolutional encoder (encodes binary data) to generate modulation symbols. This is passed to the GSM transmitter for noise error normalization by the transmitter baseband filtering block (SPB) and then fed to the air interface channel which have multipath response or fading. As shown in figure 8, the receiver model is designed with matched IF, complex phase shift and matched amplitude pulse. The matched filter independently filters each channel of the input over time using a direct form digital filter implementation. The demodulator block was designed with sensitivity or error vulnerability in mind considering the SPB senarios. At the receiver, the SMS data from the channel is reprocessed by the reciever baseband filtering for normalization with a submodule rake receiver before the final demodulation process for bit error (BER) and frame (SMS) quality analysis while the model display gives the run time responses as shown in figure 10. Table 4.1 shows the optimal parameters for the GSM radio model.

*Table 4.1: Modeling parameters [Kumarabhijeet .S., 2008], [Deshpande .N.,2003]*

| S/N | Parameters | Specifications |
|---|---|---|
| 1. | Source SMS Input | Bernoulli binary-126characters |
| 2. | Convolutional Encoder | Poly2trellis Continous |
| 3. | M-ary Number | 2 |
| 4. | Modulator | GMSK baseband |
| 5. | BT | 0.3 |
| 6. | Pulse length | 4 |
| 8. | Channel | AWGN |
| 9. | Channel Mode | SNR-$E_b/N_o$ |
| 10. | Input Signal Power | 1Ohm |
| 11. | Demodulator | Serial Receiver |
| 12. | Matched Filter | Direct Form |
| 13. | SPB_Quantizing Encoder | 2 |
| 14. | SPB_Viterbi Decoder | 2 |
| 15. | FFT length | 126 |
| 16 | Number of Spectral Averages | 10 |

### 4.3. Performance Evaluation (SPB)

From figure 10, the SPB impact is shown in the transceiver model. This is expected as SPB with soft decisions enable the system to retain more information with less error vulnerability from the demodulation

Operation at the receiver unit. Hence From figure 10, the display block (vulnerability response) illustrate that the SPB soft decision receiver performs better (that is, has a smaller BER) for error reductions at the receiver demodulation unit. In this case, channel error vulnerability uses the bit error rates for the two paths to illustrate that the SPB with soft decision receiver performs better.

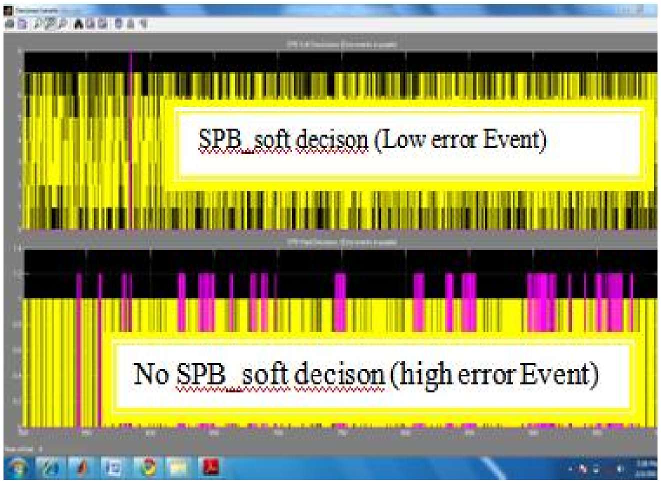

SPB_soft decison (Low error Event)
No SPB_soft decison (high error Event)

Figure 10: Influence of SPB on the Bit error sensitivity.

## 5. CONCLUSIONS

A portable low-cost embedded intelligent system based on AT82S89 controller processor with GSM SIM 300 modem, MAX 232 and LCD digital display system is proposed for Smart e-governance. This is believed to be cost effective and very flexible for the Nigerian environment. This research mainly focused on the independent radio parameter (SPB) for channel error corrections which in turn accounts for effective throughput, latency and coding gain. Future work will present the validations of the SPB and the prototype design of the e-Governance SmartNotice display systems, that will satisfy all dimensions of e-governance.

## REFERENCES

A. Fujioka, T. Okamoto & K. Otha: A practical secret voting scheme for large scale elections, Advances in Cryptology - AusCrypt '92, pp.244-251.

Abe: Universally verifiable MIX net with verification work independent of the number of MIX centers; proceedings of EuroCrypt 98, Springer Verlag LNCS.

AdemAlpaslan andMetin BĐLGĐN: " Web based secure e-voting system with fingerprint Authentication" In Scientific Research and Essays Vol. 6(12), pp. 2494-2500, 18 June, 2011. Available online at http://www.academicjournals.org/SRE.

B. V. K. Vijaya Kumar;. Biometric encryption using

Image processing. In Proc. SPIE, Optical Security and Counterfeit Deterrence Techniques II, vol. 3314, pages 178-188, 1998.

C. Soutar. Biometric system security. Available At:http://www.bioscrypt.com/assets/security soutar.pdf.

C. Soutar, D. Roberge, S. A. Stojanov, R. Gilroy, and

Cramer, R. Franklin M. Schoenmakers B. and Yung M. (2006), Multi-authority secret ballot elections with linear work. In: Advances in Cryptology, EUROCRYPT'96, Lecture Notes in Computer Science, pp.72-83.

Cranor L. and Cytron R. (2007) Sensus: a security-conscious electronic polling system for the Internet. In: Proceedings of the Thirtieth Hawaii International Conference on System Sciences, Vol.3, pp.561-570.

G.J. Tomko, C. Soutar, and G.J. Schmidt. "Fingerprint controlled public key cryptographic system". U.S.Patent 5541994, July 30, 1996 (Priority date: Sept. 7, 1994).

Indrajit Ray, Indrakshi Ray, Natarajan Narasimhamurthi: "An Anonymous Electronic Voting Protocol for Voting Over The Internet".

Ivan Damgard, Jens Groth and Gorm Salomonsen, TheTheory and Implementation of an Electronic,Voting System, July 31, 2002.

J.L, Wayman, "fundamentals of biometric authentication technologies" Int. Image graphics, vol.1, no.1, pp. 93-113, 2001.

Ohkubo and Abe: A Length-Invariant Hybrid Mix Proceedings of Asia Crypt 00, Springer Verlag LNCS.

Oleg Murk,Electronic Voting Schemes, M.Sc term paper,2000.

Shane, P. (2004) Democracy Online: The Prospects for Political Renewal through the Internet. New York: Routledge.

Uludag U, Pankanti S, Prabhakar S, Jain AK: "Biometric cryptosystems: issues and challenges. Proc IEEE 2004, 92(6):948 -960.

www.computer.org/security: Evaluating Electronic Voting Systems Equipped with Voter-Verified Paper Records. IEEE Security & Privacy, 2008.

Full Paper

# EMBRACING E-GOVERNMENT FOR A SUSTAINABLE HEALTH SYSTEM: AN IMPERATIVE FOR NATION BUILDING

**Z.O. Omogbadegun**
Department of Computer & Information Sciences,
Covenant University, Ota, Ogun State, Nigeria
zacchaeus.omogbadegun@covenantuniversity.edu.ng

## ABSTRACT

Nigerian governments are inexorably committed to enhance harmonized implementation of essential health services in line with national health policy goals. Nevertheless, traditional communities' health is still embarrassingly threatened. In nation building, revitalizing integrated health services delivery towards the provision of equitable and sustainable access to quality healthcare is an indispensable imperative. Maintaining communications networks' availability to ensure delivery of the best possible patient-oriented healthcare among all providers is desirable. This paper presents a developed collaborative virtual framework for a multidisciplinary team of healthcare services delivery stakeholders for seamless information exchange towards augmented well-being in sustainable nation building. This framework provides an evidence-based platform for policy makers seeking to have better understanding of traditional health practices. It also supports research activities to gain more insight and evaluate them. Organizing traditional medicine practitioners into bodies/organizations that are easy to regulate and actually regulate their practice is an outcome, too. Adopting traditional practices and technologies of proven value into State's health care system and discourage those that are harmful are facilitated. Training traditional health practitioners to improve their skills, to know their limitations, and ensure their use of the referral system would be implementable with this framework. Where applicable, seeking the cooperation of traditional practitioners in promoting health programmes in such priority areas as nutrition, environmental sanitation, personal hygiene, immunization and family planning would be achievable using this platform. Discouraging traditional health practitioners from advertising themselves and making false claims in the public media would be realisable using this framework. This gap-filling and implementable collaborative mechanisms framework involving all partners in the development and sustenance of the health sector for

## 1. INTRODUCTION

Governance refers to the relationship between those who govern and those who are governed. On a political level it is the relationship between the government and its citizens and includes three requirements: (1) to know the present state, (2) to know where it needs to go, and (3) to know how it is progressing in the journey—somewhat analogous to what consultants call a gap analysis. It also involves three areas of decision making: who is governing, who is being governed, and what resources/assets are to be deployed in the process.

Increasingly, governments are making use of electronic methods to deliver public services. Governments are therefore expected to be responsive to social change, address public concerns, deliver effective government programmes, manage public funds efficiently, implement the principles of good governance, etc. Significantly, the systemic arena for e-government has advanced from global and regional, to in-country national, state, provincial, county and local levels of government (RIPA, 2008). Responsive governance has become the guiding principle for transforming and revitalizing public services in order to ensure their effective, efficient and transparent delivery.

Nation building translates to improvement of the quality of life in the town in all its dimensions including strategic areas, but not limited to i) Building the digital community; ii) Local government and local public services; iii) Schools and education community; iv) University and academic community; v) Health services; vi) Social services; vii) Economic sector; viii) Culture and leisure. One key area for nation building is the provision of equitable access to healthcare to justify the common saying that the health of nation's citizens determines her wealth. Patients in Nigeria's rural areas (where over 51% of population reside) lack access to healthcare facilities (HCFs) and human resources (Onwudiegwu and Awowole, 2012).

Nigeria's maternal health indicators and statistics sourced from UNICEF by (RFPD, 2012) are as presented in Table 1.

Yearly in Nigeria, about 1,000,000 children die before their fifth birthday (FMOH, 2007). Nigeria is currently ranked 18th on the under-5 mortality list, with under-five mortality rate of 230 per 1,000 live births in 1990, 207 per 1,000 live births in 2000 and 186 per 1,000 live births in 2009. Nigeria single-handedly contributes about 8% of the world's annual mortality in neonates with an annual figure of 242,000 neonates' death thereby comfortably and sadly leading the neonatal mortality chart in Africa. With this high level of perinatal mortality in Nigeria, if decisive steps are not urgently taken and implemented with tenacity of purpose, might mean that her dream of achieving MDG-4 by the year 2015 might after all be a mirage. Nigeria increasingly records over 59,000 maternal deaths yearly with a maternal mortality ratio of 1,100 per 100,000 per live births (second highest worldwide after India), following her weak and inequitable health systems (Onwudiegwu and Awowole, 2012).

*Table 1: Maternal Health: Indicators & Statistics (RFPD, 2012)*

| Maternal mortality ratio†, 2005-2009*, reported | 550 |
|---|---|
| Maternal mortality ratio†, 2008, adjusted | 840 |
| Maternal mortality ratio†, 2008, Lifetime risk of maternal death: 1 in: | 23 |
| Life expectancy: females as a % of males, 2009 | 102 |
| Contraceptive prevalence (%), 2005-2009* | 15 |
| Antenatal care coverage (%), At least once, 2005-2009* | 58 |
| Antenatal care coverage (%), At least four times, 2005-2009* | 45 |
| Delivery care coverage (%), Skilled attendant at birth, 2005-2009* | 39 |
| Delivery care coverage (%), Institutional delivery, 2005-2009* | 35 |

Nigeria's maternal mortality rate means that 144 women die each day and one woman every 10 minutes from conditions associated with child-birth. Maternal mortality rates are higher in rural areas, where the rate is estimated to be around 828 per 100,000 live births. In urban Nigeria, the average is 351 (Musbau, 2012). The maternal mortality rate in Lagos State, Southwest Nigeria, has hit 1.1 million annually (Idris, 2012). From these quite frightening and disheartening available health statistics for Nigeria as at December 2012, it is very safe to say "If Health is Wealth, we are indeed a poor country".

Building an inclusive information society is a necessary and complementary measure to reforming governance. It empowers citizens to access information, register their demands and shape public services to meet these demands. Recognizing the limits of the state and the market, development thinking turned to catalyzing and leveraging community knowledge, creativity, and capital to promote grassroots development. Sustainable development depends on local participation, community empowerment, and multi-stakeholder partnership.

Research argues that e-government technologies have positive influences on politics and democracy, improving citizens' environment as well as their engagement with their government. Although much research indicates that e-government technologies have increased citizen participation, there is much more than can be developed (Reddick, 2010). E-Government is about integrating ICT strategically and organically into development policy and public sector reform processes (Hanna, 2010).

### 1.1. Government Leadership Challenges

For sustainable nation building, there is a demonstrated need to empower the top level policy-and-decision-makers with information and communications technologies' tools (e-governance) in examining the challenges facing the public sector from the demands of citizens and businesses for improved services, reduced bureaucracy, greater responsiveness from government organizations and greater involvement in the political and democratic processes. Governments at all levels worldwide face several overarching challenges in designing and implementing successful ICT-enabled programmes. These challenges include: Driving government-wide transformation; Managing the people impact of ICT enabled transformation; Funding and managing inter-departmental initiatives; Sharing information across government departments; Fostering public confidence; Delivering efficiency savings while maintaining inclusivity; and Measuring Impact. Required to be put in place include the mapping of all categories of private health care providers by operational level and location, development of guidelines and standards for regulation of their practice and their registration, performance monitoring mechanism for the private sector, and adaptation and implementation of the national policy on traditional medicine at all levels (FMOH, 2010). For sustainable nation building to be achieved, therefore, policy makers need to foster collaboration with the private sector through e-governance.

### 1.2. Goals and benefits of e-Government

ICT is a key enabler for new policies and business process transformations aimed at providing better and more efficient Public Services. ICT-enabled government offers four potential benefits to business, citizens and frontline civil servants: Accessibility - the ability to interact with government through new channels and new ICT-enabled service routes; Flexibility - the ability to interact at more convenient times; Efficiency - more efficient government leading to better services and better use of available resources; and Inclusion - the ability to reach a greater percentage of the target population with a service.

New information technologies are being applied swiftly to all levels of government service: local, county, regional and even national and international. Information technology (IT) is being used to improve data management and data sharing, planning and decision support, service delivery, and more. Application areas affected by government mandates to improve e-government service include healthcare and safety; law enforcement, security, and justice; education; land use; and many others. Information technology is being used to increase public access to information, to provide more convenient and timely transaction services, and to increase citizen participation in the establishment of government regulations and other processes.

IT is being used to increase public access to information, to provide more convenient and timely transaction services, and to increase citizen participation in the establishment of government regulations and other processes. In so doing, digital government also supports the larger goals of streamlining processes and increasing efficiency, sustaining and strengthening democracy, and improving government accountability and transparency (Chen et al. 2008).

ICT-enhanced government requires ICT solutions for the following areas primarily: technology to support policy creation; the recording and retrieval of ethical and legal questions; tools for policy enforcement and legal issues; public-government communications; technology for security and privacy; and tools to improve general government data processing efficiency. Its special roles as trusted controller of force and as holder of private personal information make government a primary consumer of normative Digital Government research and ICT developments. eHealth highlights the areas of data capture, storage, and management; privacy and security; and health-related communications and broadcasting. As for government, eHealth workers are in possession of private personal information and also need normative research (Hovy, 2008).

## 2. OBJECTIVE

A paradigmatic approach to collaboration and Complementary and Alternative Medicine (CAM) integration could create a common basis for scientific dialogue, encourage exchanges between medical communities, and establish policies for the development of a true multidisciplinary healthcare cooperative that is consistent with the current public health model (Giordano et al. 2003).

The main objective of this paper is to present a collaborative virtual framework (platform) for a multidisciplinary team of healthcare services providers, CAM practitioners and scholars for seamless information exchange in healing process for augmented well-being, using Ondo State of Nigeria as a case study.

## 3. CHALLENGES FOR HEALTHCARE DELIVERY SYSTEMS

The aim of healthcare is to achieve the best health outcomes in the most efficient manner. Patients' requirements for healthcare include treatment and care that work, good relationship with practitioner, provision of information, and remaining in control of treatment. Health disparities have been widely recognized as a problem throughout the world. The frequency of non-optimal patient care, the wide variations in practice, and the inefficiencies, dangers, and inequalities have been reported in literature. ICTs are needed in addressing the global challenges of healthcare worldwide (Omogbadegun et al. 2011). The challenge for today's health delivery systems is to how to provide improved services to an increasing number of people using limited financial and human resources for increased productivity and quality of care without increasing the economic costs (Varshney, 2006; de Leiva, 2008). The increasing prominence of health promotion theory and a corresponding shift toward emphasizing wellness and empowerment, holistic and family-friendly design, and empirically supported treatment were exploited to drive this research.

The African region – home to only 3% of the estimated 59.2 million health workers in the world but having 24% of the global burden of disease – is the area hardest hit by health worker shortfalls and imbalances worldwide. The global shortage is estimated at around 2.3 million physicians, nurses and midwives, and over 4 million health workers overall. In some parts of the world, notably in sub-Saharan Africa, the current workforce needs to be scaled up by almost 140% in order to overcome the crisis (Fapohunda et al. 2009; Poz et al. 2009).

It has been proved that responsive governance impact could be realized transparently with ICT-enablement in the following areas of public services: Health - ICT enabling new or better provision of public healthcare delivery, including hospitals and general practices; Education - provision of services using ICT in higher education, schools and in adult education; Revenue / tax - using ICT to improve collection of tax revenue from citizens and businesses; Work and benefits - ICT-enabled transformation of services related to work and benefits provision (social support, pensions) and job search assistance to citizens; Transport - provision of services using ICT in government-owned transport networks and for private users, such as car registrations, driver and vehicle licensing; and Public protection - using ICT in maintaining law and order in society.

From the National Health Bill 2009 (Draft), one of the functions of the Ministry of Health (MOH) is: "Developing public health IEC infrastructure and programmes for mass public health campaigns and activities, with institutionalized involvement of educational institutions, non-governmental organizations, community based organizations, associations of medical providers, traditional health care practitioners, mass media (including privately owned mass media), and all other stakeholders in promotion of public health;". In doing this, FMOH is expected to be: "ensuring that harmful social or traditional practices do not interfere with access to appropriate medical treatment;" and "promoting medical research and health education, as well as information campaigns, particularly with respect to HIV/AIDS, sexual and reproductive health, traditional practices, …" (FMOH, 2009).

General physicians with a biomedical focus have remained the dominant professional group in integrative healthcare settings. Complementary and Alternative Medicine (CAM) practitioners are generally excluded from patient charting; prohibited from ordering diagnostic tests; and not allowed to refer patients to biomedical physicians. Conventional physicians misappropriated CAM modalities or excluded CAM practitioners from group rounds. Many CAM practitioners are also disadvantaged because they don't understand biomedical language which dominates group meetings and patients' charts. Despite growing interest among physicians for CAM therapies, they lack understanding of CAM and have little awareness that their patients seek CAM providers (Mior et al. 2010).

Securing improvements in the size and quality of the health workforce is important for achieving regional and country-specific Millennium Development Goals in health. Overcoming human resources for health shortages and imbalances requires strengthening education and training programmes for health workers, improving health sector working conditions (including staff salaries and benefits) and forging cooperation and collaboration in health workforce management within and across countries. Evidence-based monitoring of health workforce dynamics is important for ensuring that policy and programmatic inputs lead to the expected outcomes (Fapohunda et al. 2009).

The goals of sustainable development cannot be achieved when there is a high prevalence of debilitating illness and poverty, and the health of a population cannot be maintained without a responsive health system and a healthy environment.

### 3.1. National Strategic Health Development Plan (NSHDP)

NSHDP's Mission Statement is "To develop and implement appropriate policies and programmes as well as undertake other necessary actions that will strengthen the National Health System to be able to deliver effective, quality and affordable health".

The overarching goal of the National Strategic Health Development Plan (NSHDP) is "to significantly improve the health status of Nigerians through the development of a strengthened and sustainable health care delivery system". To achieve this mission statement with the overarching goal,

NSHDP is committed, among others, to:

1. increasing budget allocations to health at the Federal, State and LGAs from the present level by at least 25% each year towards achieving the 2009 National Partnership on Health Declaration target of 15% (a.k.a. 15% Abuja Declaration 2009); committing to at least 90% budget release and 100% utilization by the end of the year;
2. establishing and strengthening partnerships with the private sector and other health service providers such as

non-governmental organizations, military, etc. towards improved access and service coverage;

3. Committing to strengthening the National Health Information System to serve as the backbone for managing for results;
4. Ensuring effective coordination and collaboration with development partners in the health sector at federal, State and Local Government levels, as well as private sector, CSOs, Traditional and Religious Institutions, and the communities, particularly on demand creation for health services (FMOH, 2010).

In recent years, there has been a substantial reduction in the availability of health professionals in developing countries, which has been accompanied by a rise in the demand for high-quality healthcare. Incredibly, a shortage of almost 4.3 million doctors, midwives, nurses, pharmacists, and support workers worldwide is most severe in the poorest countries, especially in sub-Saharan Africa, where they are most needed to direct and guide everyone who becomes ill on the correct use of medications. Drug manufacturers have not helped matters as their chief concern is to promote the sale of their medicines without giving adequate information to the public on such drug if possible in the local language. This is compounded by high illiteracy level, poverty and inadequate HCFs and personnel. Self-medication offers a way out as people begin to sense the positive benefits of multiplying their options in healthcare. This combination has forced healthcare institutions to collaborate and share their resources to provide comprehensive, high-quality and accessible healthcare at a reasonable cost (WHO, 2006; Wootton, et al. 2009; Afolabi, 2012).

### 3.2. Human Resources for Health

Human resources for health are the cornerstone of the health system. No health intervention can be successful without an effective workforce. Every country should therefore have a national workforce plan to build sustainable health systems to address national health needs. These plans should aim at providing access for every family to a motivated, skilled and supported health worker; and optimizing health system performance, workers should be recruited from, accountable to and supported for work in their community where feasible (FMOH, 2010).

Human Resources for Health (HRH) is usually high on the global health agenda as one of the core building blocks of Health System. There is a strong belief that "human resources development is the foundation of nation building". Focused interventions such as developing and increasing the human resources for health (building professional training facilities, curriculum development, improving the working environment to retain the health workforce, etc); improving the quality of the existing health workforce through in‐service training; and establishing efficient and effective management systems (making policies and systems for the training and recruiting of health personnel, developing databases on human resources, etc) would address shortages of healthcare workforce towards ensuring equitable access to health care (Kodera, 2011).

The main categories of human resource in the Nigerian health care system are doctors, nurses, midwives, laboratory staff, public health nurses, public health nutritionists and the community health and nutrition workers (community health officers, community health extension workers, community health assistants – etc.) (see Table 2).

There are presently 14 professional regulatory bodies charged with the responsibility of regulating and maintaining standards of training and practice for various health professionals. However, they are limited by weak structures and institutional capacities to carry out statutory functions of effective monitoring and accreditation of training institution programmes. There are about 39,210 doctors, 124,629 nurses and 88, 796 midwives registered in Nigeria. It is difficult to judge these numbers alone. The aggregated numbers hides a large variation between areas and States/Zones.

Nigeria has one of the largest stocks of human resources for health in Africa comparable only to Egypt and South Africa. In 2005, there were about 39,210 doctors and 124,629 nurses registered in the country, which translates into about 39 doctors and 124 nurses per 100,000 populations (Table 3) as compared to the Sub-Sahara African average of 15 doctors and 72 nurses per 100,000 populations As at December 2007 there were 52,408 Nigerian Doctors, 128,918 nurses, 90,489 midwives, 13,199 pharmacists, 840 radiographers, 1,473 physiotherapists, 12,703 medical laboratory scientists, and 19,268 Community Health Officers on the medical register. 94.6% of the 128,918 Nurses and 100% of the 90,489 Midwives were females (see Table 3) (AHWO, 2008).

The health workers are poorly distributed and in favour of urban, southern, tertiary health care services delivery, and curative care (see Figure 2).

For some cadres of health workers more than 50% work in the South Western part of the country with the majority living in the commercial city of Lagos. Efforts have been made to make health workers available in the rural areas. About 60% of the states in Nigeria provide rural incentives to health workers that volunteer to serve in the rural areas, while others make rural service a condition for some critical promotion.

Health workers are produced in designated health training institutions. There is poor distribution of these training institutions in favour of southern parts of the country. In Nigeria, there are 26 accredited medical schools, 86 approved schools of nursing, 77 approved school of midwifery, 12 medical laboratory schools, 6 schools of physiotherapy, 5 schools of radiography, 9 schools of pharmacy, 19 schools of pharmacy technology, 40 schools of health records, 13 schools of community health officers, 43 schools of community health extension workers, 4 schools of dental technology, 6 schools of dental therapy, 3 schools of optometry (see Tables 4 and 5) (AHWO, 2008).

*Table 2: Health worker population ratios at national level (AHWO, 2008)*

| Health occupational categories | 2005 | | 2006 | | 2007 | |
|---|---|---|---|---|---|---|
| | Number | HW / 1000 Pop. | Number | HW / 1000 Pop. | Number | HW / 1000 Pop. |
| Physicians | 39, 210 | 3.0 | 49, 612 | 3,54 | 52, 408 | 3,70 |
| Physicians (aliens) | - | - | - | - | 2, 968 | 0,21 |
| Prof/Registered Nurses | 124, 629 | 10.0 | 125, 292 | 8,95 | 128, 918 | 9,10 |
| Registered Midwives | 88, 796 | 6.8 | 88, 996 | 6,36 | 90, 489 | 6,39 |

| | | | | | | |
|---|---|---|---|---|---|---|
| Dentists | 2, 113 | 2 | 2, 241 | 0,16 | 2, 356 | 0,17 |

*Table 3: Statistics of Professional Health Workers as at December 2007 (AHWO, 2008)*

| S/N | Type | Total No | In good Standing | Public | Private | Unemployed | Abroad | Female | Male |
|---|---|---|---|---|---|---|---|---|---|
| 1 | Doctors (Nigerians) | 52408 | 14000 | na | na | na | na | 11546 | 40862 |
| 2 | Dentists (Nigerian) | 2356 | na | na | na | na | 962 | 1596 | |
| 3 | Doctors (Aliens) | 2968 | 2968 | na | na | na | na | 853 | 2115 |
| 4 | Dentists (Aliens) | 215 | 215 | na | na | na | na | 91 | 124 |
| 5 | Alternative Medicine Practitioners | 10 | 10 | 0 | 10 | 0 | 0 | 1 | 9 |
| 6 | Nurses | 128918 | na | na | na | na | na | 121929 | 6989 |
| 7 | Midwives | 90489 | na | na | na | na | na | 87164 | 7 |
| 8 | Pharmacists | 13199 | 6,744 | na | na | 0 | 296 | 4327 | 9872 |
| 9 | Radiographers | 840 | 600 | na | na | 0 | 47 | 271 | 528 |
| 10 | Physio-Therapists | 1,473 | 1,276 | 433 | 86 | 746 | 363 | 599 | 901 |
| 11 | Occupational Therapists | 29 | 18 | 10 | 0 | 4 | 7 | 13 | 5 |
| 12 | Speech Therapists / Audiologists | 26 | 26 | 17 | 0 | 4 | 5 | 17 | 9 |
| 13 | Health Records | 1,187 | 367 | 845 | 342 | 0 | 5 | 562 | 625 |
| 14 | Dental Technologists | 505 | 350 | 382 | 41 | 38 | 17 | 92 | 370 |
| 15 | Dental Therapists | 1,012 | 936 | 720 | 249 | 11 | 76 | 577 | 425 |
| 16 | Pharm. Tech | 5,483 | | na | na | na | na | na | na |
| 17 | Environmental Health Officers | 4,280 | 1,500 | na | na | na | na | 1,447 | 2,833 |
| 18 | Community Health Officers | 19,268 | na | 18,494 | 279 | 495 | 0 | 11,437 | 7,831 |
| 19 | Medical Laboratory Scientists | 12,703 | 5,548 | na | na | na | na | 1813 | 3,735 |
| 20 | Medical Laboratory Assistants | 7,044 | na | na | na | na | na | na | na |
| 21 | Medical Laboratory Technicians | 2,936 | na | na | na | na | na | na | na |
| 22 | Chartered Chemists | 1,503 | 1503 | na | na | 0 | 0 | 476 | 1,027 |
| 23 | Public Analysts | 500 | 313 | na | na | 0 | 12 | 123 | 377 |
| 24 | Optometrists | 1,415 | 205 | 1,120 | na | na | na | 750 | 665 |

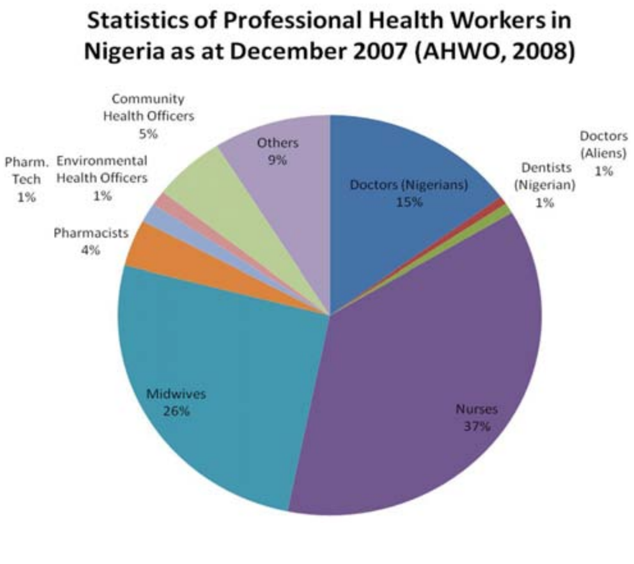


*Figure 1: Professional Health Workers in Nigeria (Source of Data: AHWO, 2008)*

There is a need to integrate health services in Nigeria. Efforts to integrate services can improve the efficiency of the total workforce. The emergence of Strategic Health Development plans at State and federal level with an overarching national framework and plan now provide the highest level of commitment and platform for the execution of the integration, harmonization and alignment of vertical programs within existing national systems and government policies (FMOH, 2010).

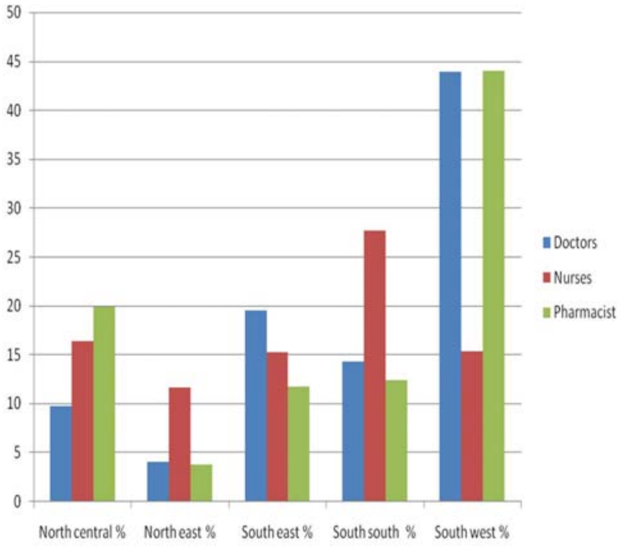


*Figure 2 Regional Distribution of Health Workforce (Extracted Data Source: AHWO, 2008)*

*Table 4: Training inputs in the Health Training Institutions from 2004 to 2007 (AHWO, 2008)*

| Cadre being trained | Actual Annual Inputs | | | | Total Input |
|---|---|---|---|---|---|
| | 2004 | 2005 | 2006 | 2007 | |
| Physicians | - | - | - | - | - |
| Nurses | 4483 | 4078 | 1888 | 3494 | 13943 |
| Midwives | 3089 | 2960 | 1189 | 2042 | 9280 |
| Pharmacists | - | - | - | - | - |
| Health Records Officers | 762 | 924 | 2144 | 1698 | 5528 |
| Dental Therapists | 36 | 32 | 46 | 47 | 161 |
| Optometrists | 364 | 445 | 306 | - | 1115 |

*Table 5: Statistics of Nurses with general and post basic training (December 2007) (AHWO, 2008)*

| Category | Total | Female | Male |
|---|---|---|---|
| General Nurses | 128918 | 121929 | 6989 |
| General Midwives | 90489 | 90470 | 19 |
| Mental Health Nurses | 6005 | 5186 | 819 |
| Public Health Nurses | 4308 | 4219 | 89 |
| Public Health Nurses Educators | 162 | 150 | 12 |
| Nurse Educators | 2102 | 1806 | 296 |
| Midwife Educators | 716 | 716 | 0 |
| Nurse Administrators | 1228 | 1107 | 121 |
| Orthopaedic Nurses | 721 | 406 | 315 |
| Nurse Anaesthetics | 517 | 215 | 302 |
| Peri-Operative Nurses | 1794 | 1031 | 763 |
| Ophthalmic Nurses | 418 | 256 | 162 |
| Accident And Emergency Nurses | 656 | 412 | 244 |
| Paediatric Nurses | 226 | 213 | 13 |

### 3.3. Utilization rate of delivery services in Nigeria

Only about 37% of deliveries in Nigeria take place in health institutions, while 57% of deliveries takes place at home by NDHS (2003). By NDHS (2008) the percentage of deliveries in a health facility went down to 35%, while 62.1% were recorded at home. Out of 28,100 deliveries, 20.0% (public hospital), 15.0% (private hospital), 62.1% (Home), 1.9 % (Other), 1.0 % (Missing) (NPC, 2009) (see Figure 3).

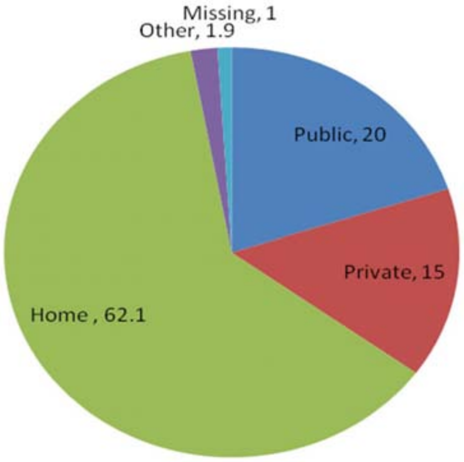


*Figure 3 Nigeria's Place of Deliveries (Source: NPC, 2009)*

In Nigeria, only 39% births take place with assistance of medically trained personnel, and immunization coverage ranges between 32.8 to 60%. The low coverage rates translate into high rates of child and maternal mortality. In many health facilities across the country, there is shortage of skilled attendants (skilled attendance of antenatal care and births are 58 and 39%, respectively) and this has been reported to impact negatively on utilization of services by women. The importance of skilled attendant at every birth for improving maternal health has been severally highlighted in various safe motherhood conferences and technical sessions (Ogunjimi et al. 2012).

## 4. COMPLEMENTARY AND ALTERNATIVE MEDICINE

Complementary and Alternative Medicine (CAM) tends to include those healthcare approaches not commonly accepted as part of conventional medicine, and access and costs vary between countries. To ensure delivery of the best possible patient-oriented healthcare, communication is critical (Robinson, 2011). Vast arrays of natural healing modalities—both ancient and new—have emerged, and some are even challenging orthodox medicine for part of the middle ground (Pengelly, 2004).

Growing drug resistance, in part caused by the misuse of medications, has rendered several antibiotics and other life-saving drugs useless. Scientists and pharmaceutical companies are urgently looking for new drug sources and are increasingly turning their eyes to CAM (Shetty, 2010). Increased use of African medicinal plants on the continent and in international trade has stimulated new efforts to monitor the quality of these botanical materials with the formation of the African Herbal Pharmacopoeia project (Blumenthal, 2009).

To ensure and regulate medical best practice, Boards of Traditional Medicine Practitioners (BTMP) have been established by Lagos and Ondo State Governments in Nigeria, among others, in recognition of CAM practitioners' role in healthcare services delivery with increasingly and undeniably patients' patronage. Herbal and other plant derived remedies have been estimated by the World Health Organization (WHO) to be the most frequently used therapies worldwide. Plant-derived remedies contain chemicals with potent pharmacologic and toxicologic properties (Afolabi, 2012). Research efforts in Western countries have been largely concerned with the interrelated issues of quality, safety and efficacy of only certain forms of CAM, especially biologically-based form (Omogbadegun et al. 2011).

Medicinal and Aromatic Plants (MAPs) are increasingly recognized worldwide as an alternative source of efficacious and inexpensive medications to synthetic chemo-therapeutic compound. Medicinal plants are used in treatment and prevention of various health problems from simple to complex disease situations among rural populations globally, thereby improving the quality of life (Elufioye et al. 2012).

### 4.1. Patient-Provider Relationship

The deterioration of the patient-provider relationship, the overutilization of technology, and the inability of the medical system to adequately treat chronic disease has contributed to rising interest in CAM. CAM therapies are used in an effort to prevent illness, reduce stress, prevent or reduce side effects and symptoms, or control or cure disease. Patients are also demanding less aggressive forms of therapy, and they are especially leery of the toxicity of pharmaceutical drugs. Adverse drug reactions have become the sixth leading cause of death in hospitalized patients. Emerging new infectious, chronic and drug-resistant diseases have prompted scientists to look towards medicinal plants as agents for treatment and prevention. Conventional physicians are unable to appreciate the imperative of CAM in collaborative healthcare delivery due to paucity of their knowledge of CAM's underlying epistemology and methodologies. Research shows that people find complementary approaches to be more aligned with "their own values, beliefs, and philosophical orientations toward health and life. Nigeria is a country stepped in the use of and belief in traditional medicines in which plants play a major role. The low accessibility or inaccessibility and non-affordability of modern drugs among the rural populations of tropical Africa have made a large proportion of rural people depend on traditional herbal drugs in order to be healthy and economically productive (Omogbadegun et al. 2011; Elufioye et al. 2012; Idu and Onyibe, 2007; Kayode and Ogunleye, 2008; Ekanem and Udoh, 2010; Oladele et al. 2011).

Driven by consumer demand, integrating conventional and CAM practices has gained popularity. The lack of disclosure by patients of their CAM use to their physicians and the potential impact on health (e.g. drug interactions) is a primary reason for the integration of conventional and CAM therapies at the primary care level. This is supported by some evidence that CAM therapies are effective in treating chronic pain or disease, typically high cost conditions (Suter, 2007).

## 5. STUDY SETTING

The New Ondo State of Nigeria was created October 1, 1996 (from Old Ondo State created February 3, 1976). She has Akure as the State Capital, Land Area of 14,798.8 Sq. Km; Population (2006 Census) - 3,640,877; Projected Population (2010) - 3,895,367; Estimated Growth Rate: - 2.87%; and 18 Local Government Areas in three Senatorial Districts as shown in Figure 4. Ondo State has 22 Ministries, 25 Boards / Commissions / Corporations, and 203 Political Wards.

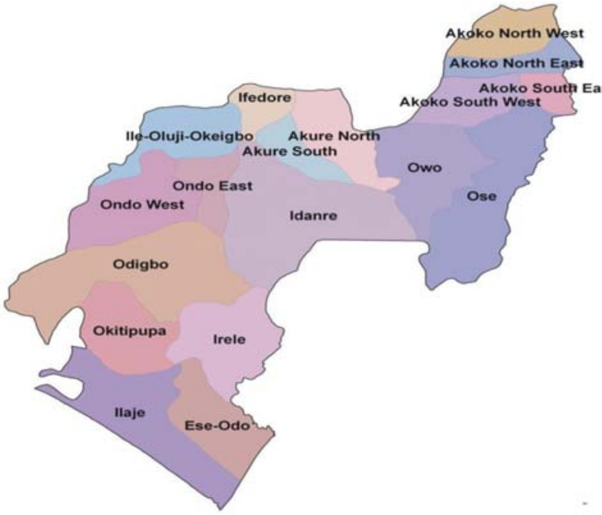


*Figure 4 Map of LGAs in Ondo State of Nigeria (NPC , 2010*

Ondo State of Nigeria has 111 Medical Officers, 767 Nurses/Midwives, 37 Pharmacists (i.e. total principal medical officers = 915) providing services in her General and State Specialist Hospitals unevenly distributed in the 18 LGAs as shown in Table 6; 808 health institutions (Primary: 458 Public, and 308 Private; Secondary: 19 Public, and 21 Private; and Tertiary: 2 Public, and 0 Private) consisting 166 Hospitals (Federal and State), 391 Health Centres (41 Comprehensive Health Centres and 350 Basic Health Centres), 126 Clinics, 33 Maternity Centres and Homes, 92 Other HCFs as at 2008/2009 as shown in Table 7. Ondo State also has a Board of Alternative Medicine, Health Management Board, School of Midwifery, Health System Fund, School of Nursing, and School of Health Technology in place (DPRS_ONDO, 2012).

Current trends favour enhanced cooperation among various healthcare services providers and the integration of CAM therapies into conventional medical treatments. However, the reality is that it is difficult for any one conventional or CAM practitioner to comprehensively learn the nuances of other disciplines. In recent years the use of CAM has exploded, with adult usage as high as 62% and paediatric usage ranging from estimates of 10% to 15% to as high as 40%. However, researchers have also suggested that merging concepts and practices from local medicinal knowledge and Western science have the potential to improve public health and support medical independence of local people (Calvet-Mir et al. 2007).

The above translates to a principal medical officers-population ratio of 3,942 as against WHO's standard of 23 doctors, nurses and midwives (principal medical officers) per 10,000 population. There were 414,083 patients (377,347 out-patients and 36,736 in-patients) documented representing a doctor-patient ratio of 3,730 (DPRS_ONDO, 2012). The percentage of deliveries at Home is still on the rising side in Nigeria. Ondo State recorded the highest percentage of deliveries at home (48.5%) in the South West from her 528 births. In Ondo State, 46.9% delivered in a health facility, while 48.5 % delivered at home. From 528 deliveries, 31.5% (public hospital), 15.4 % (private hospital), 48.5 % (Home), 3.4 % (Other), and 1.2% (Missing) (NPC, 2009) (see Figure 5).

Ogun State's 34.2% of Home deliveries came second to Ondo State in Home deliveries but recorded 63.9% deliveries in health institutions out of 703 births. In Ondo State, both conventional and

CAM practices predominantly feature and are used by patients thereby making these two approaches to human well-being aggressively compete for the centre.

Typically, Akoko South-West has an area of 226 km² and a population of 228,383 (114,733 males and 113,650 females) at the 2006 census. The LGA's Headquarters are in the town of Oka. Collaboration among healthcare services providers is inevitable. The Healthcare Facilities distribution for Akoko South West LGA is shown in Table 8.

## 6. METHODS

Relevant literature on the communication protocol between GPs and CAM Practitioners. Microsoft Visio, Unified Modeling Language (UML), and other software engineering tools were suitably used for modelling the behaviour of static aspects of the framework. The emerging video-conferenced software made use of Adobe Flash Media Server 4 provided by Adobe Corporation to serve as the streaming media server, and Adobe Flash was chosen to develop the video module ActionScript for the client software. WampServer (Window, Apache, ORACLE, and PHP Server) was the web server, while PHP code for the web module was developed with Adobe Dreamweaver. WampServer handles user management

*Table 6: Human Resources by Hospitals in 2007*

| | Medical Officers | Nurses/midwives | Pharmacist | Pharmacy Tech. | Med. Lab. Technlogy Scientist | Med. Lab Technician | Radiograp | Xray Tech. | Med. Records Officers | Med. Records Technician | Dieticia | Physiother | Optoeri | Clerical Staff | Health Attendant | Gadners/Messengers/Cl | Others | Dental Te | Dentis | Dental Therap | Dental Health Techni | Dental Nur | Total Workforce |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| SSH, Ondo | 17 | 113 | 5 | 9 | 7 | 11 | 1 | 10 | 4 | 15 | 1 | 2 | 1 | 22 | 83 | 0 | 0 | 2 | 2 | 3 | 19 | 0 | **327** |
| SSH, Okitipupa | 11 | 57 | 3 | 2 | 4 | 8 | 0 | 3 | 1 | 4 | 1 | 0 | 0 | 2 | 47 | 9 | 0 | 0 | 2 | 0 | 6 | 0 | **160** |
| SSH, Ikare | 11 | 69 | 4 | 3 | 5 | 7 | 0 | 3 | 1 | 9 | 1 | 0 | 0 | 6 | 52 | 6 | 13 | 1 | 2 | 2 | 12 | 0 | **207** |
| GH, Igbokoda | 2 | 20 | 1 | 1 | 1 | 2 | 0 | 0 | 0 | 4 | 0 | 0 | 0 | 0 | 12 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | **43** |
| GH, Igbekebo | 1 | 7 | 1 | 0 | 0 | 1 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 1 | 9 | 5 | 4 | 0 | 0 | 0 | 0 | 0 | **30** |
| SSH, Akure | 36 | 303 | 13 | 15 | 20 | 36 | 1 | 18 | 10 | 33 | 1 | 3 | 1 | 52 | 167 | 13 | 32 | 0 | 0 | 0 | 0 | 0 | **754** |
| GH, Idanre | 5 | 38 | 1 | 2 | 1 | 3 | 0 | 3 | 0 | 5 | 0 | 0 | 0 | 9 | 42 | 3 | 8 | 0 | 0 | 0 | 0 | 0 | **120** |
| GH, Ore | 7 | 26 | 2 | 2 | 2 | 3 | 0 | 6 | 0 | 4 | 0 | 0 | 0 | 3 | 13 | 2 | 9 | 0 | 0 | 0 | 0 | 0 | **79** |
| GH, Bolorunduro | 1 | 7 | 0 | 0 | 0 | 1 | 0 | 1 | 0 | 3 | 0 | 0 | 0 | 0 | 11 | 2 | 4 | 0 | 0 | 0 | 0 | 0 | **30** |
| GH, Ipe | 2 | 11 | 0 | 1 | 0 | 1 | 0 | 0 | 0 | 2 | 0 | 0 | 0 | 1 | 11 | 1 | 3 | 0 | 0 | 0 | 0 | 0 | **33** |
| GH, Idoani | 3 | 15 | 1 | 1 | 0 | 1 | 0 | 2 | 1 | 2 | 0 | 0 | 0 | 2 | 18 | 4 | 4 | 0 | 0 | 0 | 0 | 0 | **54** |
| GH, Iju | 2 | 21 | 1 | 3 | 0 | 4 | 0 | 0 | 1 | 3 | 0 | 0 | 0 | 6 | 28 | 0 | 4 | 0 | 0 | 0 | 0 | 0 | **73** |
| GH, Ode Irele | 2 | 11 | 1 | 1 | 2 | 0 | 0 | 0 | 0 | 2 | 0 | 0 | 0 | 2 | 8 | 3 | 7 | 0 | 0 | 0 | 0 | 0 | **39** |
| GH, Irun | 1 | 16 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 2 | 0 | 0 | 0 | 9 | 10 | 2 | 1 | 0 | 0 | 0 | 0 | 0 | **42** |
| GH, Igbara-Oke | 2 | 18 | 2 | 2 | 0 | 4 | 0 | 4 | 0 | 3 | 0 | 0 | 0 | 5 | 18 | 10 | 4 | 0 | 0 | 0 | 0 | 0 | **72** |
| GH, Owo | 2 | 16 | 0 | 2 | 0 | 2 | 0 | 2 | 0 | 3 | 0 | 0 | 0 | 11 | 33 | 0 | 3 | 0 | 0 | 0 | 0 | 0 | **74** |
| GH, Ileoluji | 5 | 12 | 1 | 2 | 1 | 2 | 0 | 4 | 0 | 7 | 0 | 0 | 0 | 11 | 33 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | **79** |
| **TOTAL** | **111** | **767** | **37** | **47** | **43** | **87** | **2** | **56** | **18** | **103** | **4** | **5** | **2** | **142** | **601** | **60** | **97** | **3** | **6** | **5** | **37** | **0** | **2,233** |

*Source: (DPRS_ONDO, 2012)*

*Table 7: Distribution of Healthcare Facilities in Ondo State (2008/2009)*

| SUMMARY | | | | | | | |
|---|---|---|---|---|---|---|---|
| **LGA** | **PRIMARY** | | **SECONDARY** | | **TERTIARY** | | **TOTAL** |
| | **PUBLIC** | **PRIVATE** | **PUBLIC** | **PRIVATE** | **PUBLIC** | **PRIVATE** | |
| AKOKO NORTH EAST | 17 | 16 | 1 | 2 | 0 | 0 | **36** |
| AKOKO NORTH WEST | 18 | 8 | 1 | 0 | 0 | 0 | **27** |
| AKOKO SOUTH EAST | 17 | 4 | 1 | 0 | 0 | 0 | **22** |
| AKOKO SOUTH WEST | 24 | 19 | 1 | 0 | 0 | 0 | **44** |
| AKURE NORTH | 22 | 11 | 1 | 0 | 0 | 0 | **34** |
| AKURE SOUTH | 19 | 120 | 2 | 7 | 1 | 0 | **149** |
| ESE-ODO | 26 | 0 | 1 | 0 | 0 | 0 | **27** |
| IDANRE | 43 | 10 | 1 | 2 | 0 | 0 | **56** |
| IFEDORE | 26 | 0 | 1 | 0 | 0 | 0 | **27** |
| ILAJE | 26 | 3 | 1 | 1 | 0 | 0 | **31** |
| ILE OLUJI - OKEIGBO | 30 | 7 | 1 | 2 | 0 | 0 | **40** |
| IRELE | 14 | 5 | 1 | 0 | 0 | 0 | **20** |
| ODIGBO | 46 | 28 | 1 | 1 | 0 | 0 | **76** |
| OKITIPUPA | 28 | 11 | 1 | 0 | 0 | 0 | **40** |
| ONDO EAST | 21 | 0 | 1 | 0 | 0 | 0 | **22** |
| ONDO WEST | 38 | 41 | 1 | 6 | 0 | 0 | **86** |
| OSE | 21 | 6 | 1 | 0 | 0 | 0 | **28** |
| OWO | 22 | 19 | 1 | 0 | 1 | 0 | **43** |
| **TOTAL** | **458** | **308** | **19** | **21** | **2** | **0** | **808** |

*Source: (DPRS_ONDO, 2012)*

module and conference room management module. Oracle 11g Relational Database System holds the tables used in conference functions module as the data source so that it could be integrated to other collaborative systems easily.

## 7. CONTRIBUTIONS

An aggregated collaborative virtual healthcare services delivery framework was developed as depicted in Figure 6. Figure 6 shows typical collaborative virtual healthcare reference architecture for implementing an e-Health integration solution between two general hospital locations, say, Akure (State capital) and Iwaro-Oka (Akoko South West LGA Headquarters) in Ondo State. The Reference Architecture is centered round the use of the Connected Health Services Hub, which enables the provision of a number of services including: Collaboration services and Communication Services. The communication infrastructure (mobile telecommunication technologies) included Bluetooth and wireless local area networks technologies. The device types used to collect medical data included Personal Digital Assistance (PDA), smart phones, or tablet PC. This framework exchanges health delivery information among physicians, CAM practitioners, scholars, and researchers in a collaborative virtual manner.

### 7.1. Aggregated Collaborative Virtual Healthcare Services Delivery Framework

The aggregated collaborative virtual healthcare services delivery framework shows the communications infrastructure and the principal stakeholders including: (1) CAM Practitioners from Traditional Pharmacopedia, and Prayer Houses being facilitated to exchange clinical/referral notes with GPs via network. (2) Payers (Regulatory/Government/Patients) such as Hospitals Management Boards (HMB), Boards of Traditional Medicine Practitioners (BTMP), Nigeria Natural Medicine Development Agency (NNMDA), Nigerian Medical Association (NMA), National Resident Doctors of Nigeria (NRDN), National Agency for Food, Drug Administration and Control (NAFDAC), Nigeria Communications Commission (NCC), Medical and Dental Council of Nigeria (MDCN), Nigerian Medical Association (NMA), Association of General and Private Medical Practitioners (AGPMP), National Association of Nigerian Nurses and Midwives (NANNM), Nursing Council of Nigeria (NCN), Community Health Practitioner Association (CHPA) and Pharmaceutical Society of Nigeria (PSN) to ensure higher efficiencies produce lower costs; standardization of care producing healthier (cheaper) patients; and better knowledge of outcomes. The regulatory bodies are also to ensure secured availability of Health Level 7 (HL7) networks and also ensure that harmful social or traditional practices do not interfere with access to appropriate medical treatment. (3) Patients demanding better healthcare; real choice; enhanced services; professional record keeping; and lower cost. (4) Doctors / Nurses / Hospitals / Labs' expectations are diagnosis with resultant higher efficiencies produced at lower costs (more value); focus on core competencies; and new, more lucrative, more rewarding roles. (5) Researchers/Pharmacy from universities, health institutions of learning, and pharmaceutical companies' drug research and development units are undertaking healthcare research activities in data mining; epidemiology; healthcare outcomes; drug development; drug interactions in the population; better targeted, faster, drug trials; and accessible historic record.

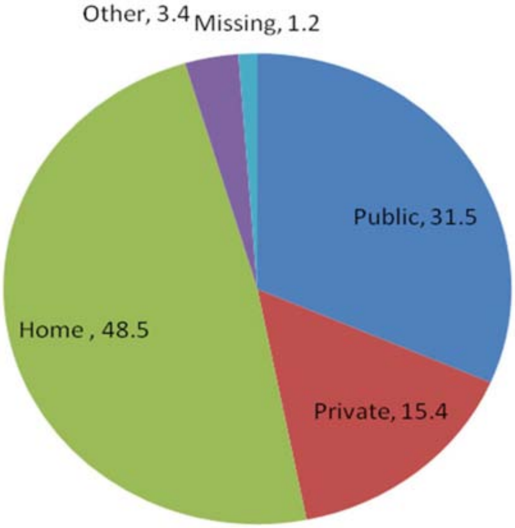


*Figure 5: Ondo State's Place of Deliveries (Source: NPC, 2009)*

*Table 8: Healthcare Facilities in Akoko South West*

| WARD | NAME OF HEALTH FACILITY | FACILITY TYPE | OWNERSHIP (PUBLIC/ PRIVATE) |
|---|---|---|---|
| Akungba1 | Basic H. Centre, Akungba | Primary | Public |
| Akungba11 | Health Post, Akungba | Primary | Public |
| Ikun | Health Centre, Ikun | Primary | Public |
| Oka 11B | Health Post, Ikanmu | Primary | Public |
| | Comp. H. Centre, Owase | Primary | Public |
| Oka 11A | Health Post Iroho | Primary | Public |
| | Health Centre, Uba | Primary | Public |
| | Health Centre Okia | Primary | Public |
| | Health Centre Simerin | Primary | Public |
| | FSP clinic Ikese | Primary | Public |
| | Health Post, Agba | Primary | Public |
| Oka Va | Health Centre, Iwaro Owalusi | Primary | Public |
| | Health Post Oka-Odo | Primary | Public |
| Oka Vb | General Hosp.Iwaro-Oka | Secondary | Public |
| | Health Centre, Ayegunle | Primary | Public |
| Oka 1 | Health Centre, Sabo | Primary | Public |
| Supare | Health Centre, Akowonjo | Primary | Public |
| | Health Post, Etioro | Primary | Public |
| Supare 1 | Health Centre, Supare | Primary | Public |
| | Compreh. H. Centre Supare | Primary | Public |
| | Model PHC | Primary | Public |
| Supare 11 | Health Post, Igbegun | Primary | Public |
| Oba 1 | Health Centre, Ose-Oba | Primary | Public |
| | Basic health Centre, Oba | Primary | Public |
| | Health Centre, Oba | Primary | Public |
| | Adekanye Mem. Hosp. Ifira akoko | Primary | Private |
| | Akuloju Mem. Hospital, Akungba A | Primary | Private |
| | Anu-olu Clinic Okda | Primary | Private |
| | Bolorunduro Clinic, Oka Akoko | Primary | Private |
| | Dedam clinic & Mat. Home Iwaro O | Primary | Private |
| | Ijadunni Mat. Home & Clinic Oka | Primary | Private |
| | Iloju Mem. Hosp., | Primary | Private |
| | Ireti Clinic, Iwaro - Oka | Primary | Private |
| | Joyce Medical Clinic Oka Akoko | Primary | Private |
| | Kajola Med. Clinic Supare Akoko | Primary | Private |
| | Lanwo Med. Clinic Supare Akoko | Primary | Private |
| | Moye Clinic, Oke Oka Akoko | Primary | Private |
| | Ore-Ofe Clinic Iwaro Oka | Primary | Private |
| | Poly Clinic, Iwaro - Oka | Primary | Private |
| | Reedom clinic, Oka Akoko | Primary | Private |
| | St. Joseph Clinic, Supare Akoko | Primary | Private |
| | Tolu Med. Clinic Oka Akoko | Primary | Private |
| | Tolulope Md. Clinic Oka Akoko | Primary | Private |
| | Victory Clinic Ose Oba Akoko | Primary | Private |

*Source: (DPRS_ONDO, 2012)*

The implementations of this framework using the developed video-conferenced software are ongoing in a number of clinical and CAM settings in South West Nigeria.

## 8. CONCLUSIONS

The development of system architectures utilizing new computing technologies that support Collaborative Virtual Environments (CVEs) in CAM is a growing necessity just as continuity of care requires a cooperative environment among autonomous complementary medical departments in terms of data and functions. It is expedient to increase access to essential healthcare services, especially for rural and underserved populations. Collaborative virtual complementary and alternative healthcare systems' success depends on enabling ubiquitous computing, ubiquitous communication, and intelligent user-friendly interfaces technologies towards integrative healthcare systems. Strengthening the technical capacities and collaboration among practitioners of traditional medicine to further strengthen and improve CAM infrastructure will be rewarding. This will foster greater information exchange towards improving and increasing the understanding, dissemination, and use of CAM for healthier nation where over 51% of the population residing in the rural and underserved areas rely on CAM interventions for their health needs.

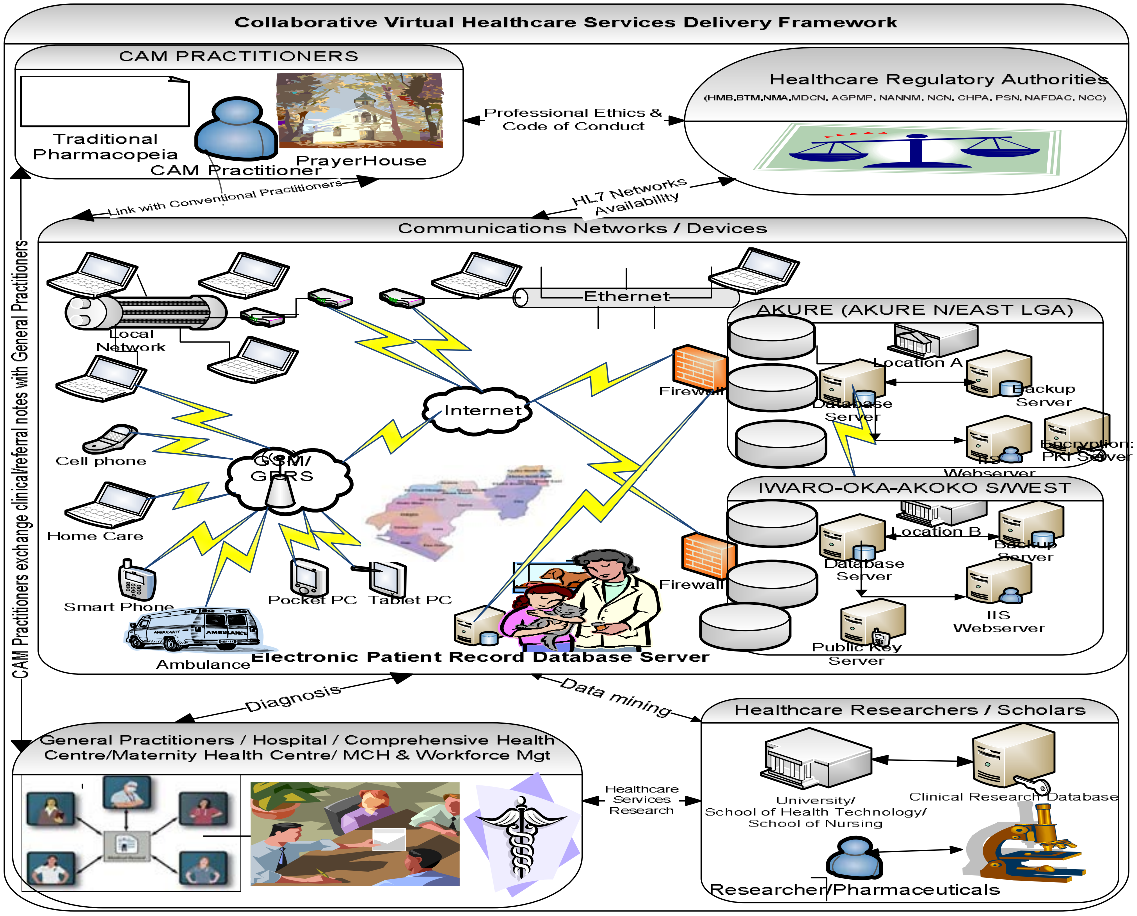

Collaborative Virtual Healthcare Services Delivery Framework
CAM PRACTITIONERS
Traditional Pharmacopeia
CAM Practitioner
PrayerHouse
Professional Ethics & Code of Conduct
Healthcare Regulatory Authorities
(HMB,BTM,NMA,MDCN, AGPMP, NANNM, NCN, CHPA, PSN, NAFDAC, NCC)
Link with Conventional Practitioners
HL7 Networks Availability
Communications Networks / Devices
Local Network
Ethernet
Internet
Cell phone
GSM/ GPRS
Home Care
Smart Phone
Ambulance
Pocket PC
Tablet PC
Electronic Patient Record Database Server
Firewall
Firewall
AKURE (AKURE N/EAST LGA)
Location A
Database Server
Backup Server
IIS Webserver
Encryption: PKI Server
IWARO-OKA-AKOKO S/WEST
Location B
Database Server
Backup Server
IIS Webserver
Public Key Server
CAM Practitioners exchange clinical/referral notes with General Practitioners
Diagnosis
Data mining
General Practitioners / Hospital / Comprehensive Health Centre/Maternity Health Centre/ MCH & Workforce Mgt
Healthcare Services Research
Healthcare Researchers / Scholars
University/ School of Health Technology/ School of Nursing
Clinical Research Database
Researcher/Pharmaceuticals

*Figure 6 Aggregated Collaborative Virtual Healthcare Services Delivery Framework*

## ACKNOWLEDGEMENT

ZOOmogbadegun appreciates Dr. Godwin Adebose Olawale (Physician, Public & Reproductive Health, Ministry of Health, Akure, Ondo State), Dr. Michael Adeboro Alabi (Physician, St. Michael Medical Centre, Akure, Ondo State), Dr. Funsho Oladipo (Physician, RJolad Hospital Nig. Ltd, Bariga, Lagos), Dr. Toogun (Physician & Chief Medical Director, Covenant University Health Centre Services, Ota, Ogun State), Engineer Reuben Olanipekun Aladetoyinbo (Director, Ministry of Agriculture, Akure, Ondo State - posthumously); Professor Adetokunbo Babatunde Sofoluwe (Professor of Computer Sciences & Vice-Chancellor, University of Lagos, Lagos - posthumously); Professor Charles Onuwa Uwadia (Professor of Computer Sciences, University of Lagos, Lagos); Professor Charles Korede Ayo (Professor & Researcher of Computer & Information Sciences, Covenant University, Ota, Ogun State); Professor Louis Osayenum Egwari (Professor of Biological and Medical Sciences Research, Covenant University, Ota, Ogun State); Professor Victor W. Mbarika (Professor of Management Information Sciences & Healthcare Informatics Research, Southern University and A&M College, Baton Rouge, Louisiana, USA); Chief Pius Oluwole Akinyelure (Idanre, Ondo State); Dr. (Mrs) Mary Adeyanju (Registered Nurse, Diabetes / HIV Educator, and Director of Nursing Services Department, Ministry of Health, Ado-Ekiti, Ekiti State), Mrs Chikaodili Amalachi Ukegbu (Pharmacist, The Federal

Polytechnic Medical Centre, Ado-Ekiti, Ekiti State), Miss Oluwayemisi 'Tosin Oluwasusi (Registered Nurse, Government State Hospital, Ado-Ekiti, Ekiti State); and Dr. S.A. Fewesola (CAM Practitioner, Ota, Ogun State); Mr Ehis Idiahi (CAM Practitioner, Benin City, Edo State); Mr. Fidelis Tapfuma (Johannesburg, South Africa); Pastor Olu Ayeni (Nestle Nig. Plc, Lagos); staff of NAFDAC (Lagos, Nigeria); International Institute of Tropical Agriculture (IITA), Ibadan; staff of Forestry Research Institute of Nigeria (FRIN), Ibadan; National Institute of Horticultural Research (NIHR), Ibadan; University Botanical Garden, Ibadan; CAM Patients (names withheld); and Traders, herbs hawkers, numerous CAM practitioners in Akungba-Akoko, Idanre, Oba-Akoko, Oka-Akoko, Ondo, Owo, and Supare-Akoko (Ondo State of Nigeria) for their time, input, support and cooperation.

## REFERENCES

Afolabi, A. O; 2012. "Self Medication, Drug Dependency and Self-Managed Healthcare – A Review". In Maddock, Jay (Ed.), Public Health – Social and Behavioral Health, pp. 234-253, InTech, Croatia

AHWO – Africa Health Workforce Observatory, 2008. Human Resources for Health Country Profile - Nigeria, Federal Ministry of Health, Federal Secretariat Phase 3, Shehu Shagari Way, Maitama, Abuja.

Blumenthal, M; 2009. African Natural Plant Products: A Foreword to the Science and Challenges, In Juliani, H. Rdolfo; Simon, James E; and Ho, Chi-Tang (Eds). African Natural Plant Products: New Discoveries and Challenges In Chemistry and Quality (American Chemical Society Symposium Series), Oxford University Press, USA, 2019, pp. 3-5

Calvet-Mir, L. et al. 2008. "Is there a divide between local medicinal knowledge and Western medicine? a case study among native Amazonians in Bolivia", Journal of Ethnobiology and Ethnomedicine, 4:18, Biomed Central Ltd.

Chen, H. et al. 2008. Digital Government: E-Government Research, Case Studies, and Implementation (Integrated Series in Information Systems), Springer

Dawes, S.S. and Pardo, T; 2002. Building Collaborative Digital Government Systems: Systemic constraints and effective practices, in McIver, William J. Jr. and Elmagarmid, Ahmed K (Eds.), Advances in Digital Government: Technology, Human Factors, and Policy, Kluwer Academic Publishers, New York, , pp. 270-284

de Leiva, A. et al. 2008. "Quality of care for the woman with diabetes in pregnancy". In: Moshe Hod, Lois JovanoviC, Gian Carlo Di Renzo,Alberto de Leiva, and Oded Langer (Eds), Textbook of Diabetes and Pregnancy, Second Edition, Informa UK Ltd.

DPRS_ONDO, 2012. Ondo Coding, State Health Manpower, and FMOH-DPRS Ondo State, Department of Public Health, Ministry of Health, Akure, Ondo State

Ekanem, A.P. and Udoh, F.V; 2010. "The Diversity of Medicinal Plants in Nigeria: An Overview". In: Ho, Chi-Tang (Ed), African Natural Plant Products: New Discoveries and Challenges in Chemistry and Quality (ACS Symposium Series), Oxford University Press, USA

Elufioye, T.O. et al. 2012. "Ethnomedicinal Study and Screening of Plants Used for Memory Enhancement and Antiaging in Sagamu, Nigeria", European Journal of Medicinal Plants, 2(3), pp. 262-275

Fapohunda, B. et al. 2009. Use of facility-based assessments in health workforce analysis. In Poz, Mario R Dal; Gupta, Neeru; Quain, Estelle; and Soucat, Agnes LB (Eds.), Handbook on Monitoring and Evaluation of Human Resources for Health with special applications for low- and middle-income countries, pp. 79-101, WHO-USAID

FMOH - Federal Ministry of Health, Nigeria, 2007. Integrated Maternal, Newborn and Child Health (IMNCH) Strategy: A Handbook For Building Capacity of Core Technical Teams for IMNCH Roll Out By States & Local Governments, November 2007

FMOH – Federal Ministry of Health, 2009. National Health Bill (Draft) - MoHFW, GoI Working Draft: Version January '09, pp. 34 and 49, Federal Ministry of Health, Abuja, Nigeria

FMOH – Federal Ministry of Health, 2010. National Strategic Health Development Plan (NSHDP), Federal Ministry of Health, Abuja, Nigeria.

Giordano, J; et al. 2003. "Complementary and Alternative Medicine in Mainstream Public Health: A Role for Research in Fostering Integration", The Journal of Alternative and Complementary Medicine. June 2003, 9(3), pp. 441-445. doi:10.1089/107555303765551660

Hanna, N.K; 2010. Transforming Government and Building the Information Society: Challenges and Opportunities for the Developing World, pp. 24-25, Springer

Hovy, E; 2008. An Outline for the Foundations of Digital Government Research, in Chen, Hsinchun; Brandt, Lawrence; Gregg, Valerie; Traunmüller, Roland; Dawes, Sharon; Hovy, Eduard; Macintosh, Ann; and Larson, Catherine A (eds.), Digital Government: E-Government Research, Case Studies, and Implementation, pp. 97-113, Springer

Idris, J; 2012. Lagos Maternal Deaths Hit 1.1M, PMNews, pmnewsnigeria.com/news/metro/ October 17, 2012. Accessed December 20, 2012.

Idu, M. and Onyibe, H.I; 2007. "Medicinal Plants of Edo State, Nigeria", Research Journal of Medicinal Plant, 1 (2), pp. 32-41

Jia, W. and Zhou, W; 2005. Distributed Network Systems: From Concepts to Implementations, Springer Science + Business Media, Inc.

Kayode, J. and Ogunleye, T.O; 2008. "Checklist and Status of Plant Species Used as Spices in Kaduna State of Nigeria", African Journal of General Agriculture, 4 (1), March 31, 2008.

Kodera, K; 2011. JICA's Cooperation on Human Resources for Health, Japan International Cooperation Agency (JICA), Tokyo

Mior, S; et al. 2010. "Designing a framework for the delivery of collaborative musculoskeletal care involving chiropractors and physicians in community-based primary care", Journal of Interprofessional Care, November 2010; 24(6), pp. 678–689

Musbau, R; 2012. Tackling Maternal Mortality, PMNews, pmnewsnigeria.com/news/metro/ October 17, 2012. Accessed December 20, 2012.

NPC – National Population Commission. 2009. NDHS – Nigeria Demographic and Health Survey (2008), National Population Commission, Federal Republic of Nigeria, Abuja, Nigeria, November 2009

NPC – National Population Commission. 2010. Federal Republic of Nigeria, 2006 Population and Housing Census Priority Table Volume III Population Distribution By Sex, State, LGA & Senatorial District, National Population Commission, Abuja, Nigeria, April, 2010, pp. 9, 46

Ogunjimi et al. 2012. Curbing maternal and child mortality: The Nigerian experience, International Journal of Nursing and Midwifery, Vol. 4(3), pp. 33-39, April 2012, DOI: 10.5897/IJNM11.030, Academic Journals.

Oladele, A.T; et al. 2011. "Medicinal plants conservation and cultivation by traditional medicine practitioners (TMPs) in Aiyedaade Local Government Area of Osun State, Nigeria", Agriculture and Biology Journal of North America, doi:10.5251/abjna.2011.2.3.476.487, ScienceHuβ, http://www.scihub.org/ABJNA

Omogbadegun, Z. et al. 2011. “Multimedia-based Medicinal Plants Sustainability Management System”, IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 5, No 3, 492-503

Onwudiegwu, U. and Awowole, I; 2012. Current Trends in Perinatal Mortality in Developing Countries: Nigeria as a Case Study. In: Ezechi, Oliver C. and Odberg - Petterson, Karen(Eds.), Perinatal Mortality, pp 26-37, InTech, Croatia

Pengelly, A; 2004. The Constituents of Medicinal Plants: An introduction to the chemistry and therapeutics of herbal medicine, Allen & Unwin, Sunflower Herbals, Australia

Poz, M.D. et al. 2009. Monitoring and evaluation of human resources for health: challenges and opportunities. In Poz, Mario R Dal; Gupta, Neeru; Quain, Estelle; and Soucat, Agnes LB (Eds.), Handbook on Monitoring and Evaluation of Human Resources for Health with special applications for low- and middle-income countries, pp. 3-12, WHO-USAID

Reddick, C. G; 2010. Politics, Democracy and E-Government: Participation and Service Delivery Premier Reference Source.

RFPD - Rotarian Action Group for Population & Sustainable Development. 2012. Maternal health in Nigeria. Accessed December 20, 2012 at http://www.maternal-health.org/nigeria/maternal-health-in-nigeria/index.html

RIPA International. 2008. 2008 Course Directory: Adapting Global Training to the Local Context. Available at www.ripainternational.co.uk

Robinson, N; 2011. “Integrative Medicine - Traditional Chinese Medicine, A Model?”, Chinese Journal of Integrative Medicine, 2011 Jan; 17(1), pp. 21-25

Shetty, P; 2010. Integrating modern and traditional medicine: Facts and figures, Science and Development Network, 30 June 2010. Accessed November 26, 2011. Available at http://www.scidev.net/en/features/integrating-modern-and-traditional-medicine-facts-and-figures.html

Suter E. et al. 2007. Health Systems Integration, Definitions, Processes & Impact: A Research Synthesis

Varshney, U; 2006. Pervasive Healthcare Communications, Department of Computer Information Systems at Georgia State University.

WHO - World Health Organization, 2012. Health Service Delivery. Available at www.who.int/healthsystems/topics/delivery/en/index.html. Accessed 19/09/2012

WHO - World Health Organization. 2006. Working Together for Health, April 7, 2006, World Health Organization, Geneva

Wootton, R. et al. 2009. Telehealth in the Developing World, Royal Society of Medicine Press/IDRC

Full Paper

# ENHANCING SERVICE DELIVERY THROUGH THE DEVELOPMENT OF ARTIFICIAL INTELLIGENT BRAIN

**O.E Oduntan**
Department of Computer Science,
The Federal Polytechnic Ilaro, Ogun State

**ABSTRACT**

Service Delivery reform is driven by the recognition that the current model for government service delivery has not kept pace with community expectations around convenient access and quality of services and advances in technology. The Human race at large have lost the contribution of highly intelligent scholars, politicians, educators which death have taken to the world beyond. This paper looked into how the great ideas of our great men could be preserved and still be functional in their absence and after their death. The approach adopted by this research work is the development of an artificial intelligent brain making use of a simulator program and a nanorobot which serves as an interface between the human brain and the computer, it runs through the entire system of the body and downloads information about the natural brain into the computer system, which could be stored and used in the absence of the individual. The outcome of this paper is the ability of the computer to function as a virtual brain. This paper recommends that prominent citizens should be encouraged to use the nanorobots when designed, so that there absence does not eliminate the degree of service delivered.

Keyword: *Simulation. Simulator. Artificial Intelligent.*

## 1. INTRODUCTION

Different groups in society will have different visions about what makes "good" service delivery. In the education sector, clients (parents/learners) want low-cost, easy-to-access, safe, high-quality schooling that improves their children's/their life chances. Policy makers and political leaders want to deliver social benefits at low cost, with high propaganda value and political rewards. The providers (teachers) care about technically sound curricula, high salaries, respect and safety. Thus, the effectiveness of service delivery – and in turn, the legitimacy of the political order – depends on addressing competing goals and expectations in ways that satisfy the stakeholders. The result may or may not involve the state providing services directly, as long as the services are in fact delivered.

The state (or more precisely, the governing regime) plays a political "game" when it struggles to secure power; its success in doing so depends on, among other things, legitimacy. The source of legitimacy might be the leaders' ability to deliver economic growth, national prestige, or public services.

Alternatively (a more partial) legitimacy might derive from signals of special allegiance to certain traditions or ethnic groups. Thus, legitimacy may or may not relate to equitable service delivery. Even well-established states can fail to provide services capably and equitably.

Public investments in services are always constrained by a range of influences reflecting a given state's social and historical context. These include limits on voters' knowledge and information, polarisation of the electorate and (especially) the credibility of political commitments. Such constraints have the strongest effect in low-income countries, accountability is weak, as government does not "listen to the people".

Where credibility is low (the case in many developing countries), instead of making broadly beneficial policy commitments, politicians may focus their attention on specific localities or individuals, and devise special projects and patronage jobs.

Artificial Intelligent Brain also refered to in this paper as the "Virtual brain" is an artificial brain, which is not actually the natural brain, but can act as the brain. It can think like brain, take decisions based on the past experience, and response as the natural brain can. It is possible by using a super computer, with a huge amount of storage capacity, processing power and an interface between the human brain and this artificial one. Through this interface the data stored in the natural brain can be up loaded into the computer. So the brain and the knowledge, intelligence of anyone can be kept and used for ever, even after the death of the person.

Human brain, the most valuable creation of God, a man is said to be intelligent because of his brain and the ability to reason and take decision. Today we are developed because we can think and take decisions on key issues of life. But we loss the knowledge of a brain when the body is destroyed after the death of man, knowledge which might have been used for the development of the human society.

This papers looks into creating of an artificial brain that can think, response, take decision, and keep anything in memory. The main aim is to upload human brain into machine, so that man can think, take decision without any effort. After the death of the body, the virtual brain will act as the man. Hence, the knowledge, intelligence, personalities, feelings and memories of that man that can be used for the development of the human society and to enhance service delivery even after his death.

## 2. RELATED WORKS:

In 1952, Hodgkin and Huxley published the highly successful model of ionic currents that allowed simulation of the action potential. These simulations revealed the emergent behaviour of ion channels, and showed how only two types of ion channel can give rise to the action potential — the currency of the brain. These insights fuelled experiments and simulations for decades, and now explain how different combinations of ion channels underlie electrical diversity in the nervous system.

Wilfred Rall realized that the complexity of the dendritic and axonal arborizations of neurons would profoundly affect neuronal processing, and developed cable theory for neurons. Despite fierce resistance from the entire community, which argued against the need to consider such complexity. Rall's framework explains the 'passive' spatiotem-poral integration in neurons and is key to understanding 'active' integration due to nonlinear conductances in dendrites.

This has been fundamental to understand-ing synaptic transmission, integration and plasticity, the significance of ion channel densities and distributions in dendrites, and active electrical generation and electro-chemical compartmentalization in spines and dendrites. Neurons themselves are anatomically and electrically highly diverse, and the next step was to place the neurons in their natural environment with other neurons. A natural progression is then to simulate neurons embedded in microcircuits, microcircuits in the local circuits of brain regions, and circuits within regions and the whole brain.

This progression began by incorporating Hodgkin–Huxley-type active properties in Rall-type neuronal models to simulate realistic microcircuits carrying out realistic neural operations, such as feedback and lateral inhibition (The Human Brain Project, 2005). In the cortex, a pioneering series of simu-lations of oscillatory behaviour of hippocam-pal circuits was initiated by Roger Traub and colleagues, beginning with 100 neurons and progressing to 1,000 pyramidal cells, each with 19 branches (compartments), and 200 inhibitory interneurons. Since then, increas-ing computational capacity has spawned various multi-neuron, multi-compartment cortical, thalamocortical and cerebellar models from many laboratories. (Traub, 2005).

The current state-of-the-art is a model of a thalamocortical column comprising 3,650 multi-compartment neurons (~100 compartments) represent-ing diverse types, including superficial and deep pyramidal neurons, spiny stellates, fast-spiking interneurons, low-threshold spiking interneurons, thalamocortical relay neurons and reticular nucleus neurons.

Traub(2005) has given insight into the neu-ral properties that underlie diverse cortical circuit operations such as gamma oscillations, spindles and epileptogenic bursts. These studies provide sound proof of principle that multi-compartment, multi-neuron circuit simulations are possible, and give valuable insight into cortical network properties. The size of the current models seemed a remote prospect in the early days of modelling. They provide a strong founda-tion for taking the next quantum step, to further increase the size of the modelled network to an unprecedented level.

At this point, some may ask, why not use this computing power to simulate cortical circuits with artificial neural networks, in which the entire neuron is represented by one summing node (point neuron), connectivity is simplified to reciprocal interactions between all nodes, and functional properties are simplified as 'integrate and fire' types of activity. Such simulations provide a powerful exploratory tool, but the lack of biological realism severely limits their biological inter-pretation. The main problem is that there are always many ways to engineer a function, and which model is correct is always open debate (NeoCortical Simulator (2005).

A new approach is now possible that involves a quantum leap in the level of biological accuracy of brain models: (The Blue Brain Project, 2005).

The quantum leap: Neurons receive inputs from thousands of other neurons, which are intricately mapped onto different branches of highly complex dendritic trees and require tens of thousands of compartments to accurately represent them. There is therefore a minimal size of a microcircuit and a minimal complexity of a neuron's morphology that can fully sustain a neuron. A massive increase in computational power is required to make this quantum leap .an increase that is provided by IBM's Blue Gene supercomputer2 (FIG. 1). By exploiting the computing power of Blue Gene, the Blue Brain Project1 aims to build accurate models of the mammalian brain from first principles(Blue Gene, 2005)

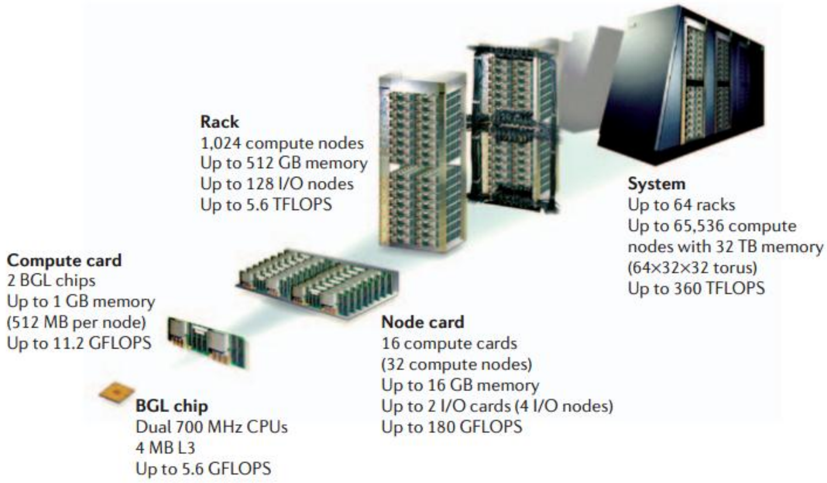


*FIG 1: The Blue Gene/L supercomputer architecture.*

## 3. METHODOLOGY:

Models and softawre will be designed by modeling the electrical structure of neural circuits repeated throughout the brain by mapping and modelling their behavior, then the molecular model of the neurons involved and a complete neocortex (the largest and most complex part of the human brain) before modelling the rest of the rain will be created. A Nanorobot which will be small enough to travel throughout the circulatory systems, traveling into the spine and brain, they will be able to monitor the activity and structure of our central nervous system. They will be able to provide an interface with computers that is as close as human mind can be while still residing in the biological form. Nanorobots could also carefully scan the structure of the brain, providing a complete readout of the connections between each neuron. They would also record the current state of the brain. This information, when entered into a computer, could then continue to function as the human himself. All that is required is a computer with large enough storage space and processing power. Many people believe firmly that human being possesses a soul, while some very technical people believe that quantum forces contribute to human awareness. However, there is a need to know how the brain actually functions, and then transfer it to a computer.

Hardware and Software Requirment

- 22.8 TFLOPS peak processing speed.
- 8,096 CPUs at 700 MHz (downgraded to handle massive parallel processing).
- 256MB to 512MB memory per processor.
- Linux and C++ software
- 100 kilowatts power consumption.
- Very powerful Nanorobots to act as the interface between the natural brain and the computer.

## 4. SIMULATION/IMPLEMENTATION/RESULTS ANALYSIS

### 4.1. How the natural brain works?

The human ability to feel, interpret and even see is controlled, in computer like calculations, by the magical nervous system. Yes, the nervous system is quite like magic because we can't see it, but its working through electric impulses through your body.

One of the worlds most "intricately organized" electron mechanisms is the nervous system. Not even engineers have come close to making circuit boards and computers as delicate and precise as the nervous system. To understand this system, one has to know the three simple functions that it puts into action: sensory input, integration, motor output.

#### *4.1.1. Sensory input:*

When our eyes see something or our hands touch a warm surface, the sensory cells, also known as Neurons, send a message straight to your brain. This action of getting information from your surrounding environment is called sensory input because we are putting things in your brain by way of your senses.

#### *4.1.2. Integration:*

Integration is best known as the interpretation of things we have felt, tasted, and touched with our sensory cells, also known as neurons, into responses that the body recognizes. This process is all accomplished in the brain where many, many neurons work together to understand the environment.

#### *4.1.3. Motor Output*

Once our brain has interpreted all that we have learned, either by touching, tasting, or using any other sense, then our brain sends a message through neurons to effecter cells, muscle or gland cells, which actually work to perform our requests and act upon our environment. The word motor output is easily remembered if one should think that our putting something out into the environment through the use of a motor, like a muscle which does the work for our body.

### 4.2. How we see, hear, feel, smell, and take decision:

#### *4.2.1. Nose*

Once the smell of food has reached your nose, which is lined with hairs, it travels to an olfactory bulb, a set of sensory nerves. The nerve impulses travel through the olfactory tract, around, in a circular way, the thalamus, and finally to the smell sensory cortex of our brain, located between our eye and ear, where it is interpreted to be understood and memorized by the body.

#### *4.2.2. Eye*

Seeing is one of the most pleasing senses of the nervous system. This cherished action primarily conducted by the lens, which magnifies a seen image, vitreous disc, which bends and rotates an image against the retina, which translates the image and light by a set of cells. The retina is at the back of the eye ball where rods and cones structure along with other cells and tissues covert the image into nerve impulses which are transmitted along the optic nerve to the brain where it is kept for memory.

#### *4.2.3. Tongue*

A set of microscopic buds on the tongue divide everything we eat and drink into four kinds of taste: bitter, sour, salty, and sweet. These buds have taste pores, which convert the taste into a nerve impulse and send the impulse to the brain by a sensory nerve fiber. Upon receiving the message, our brain classifies the different kinds of taste. This is how we can refer the taste of one kind of food to another.

#### *4.2.4. Ear*

Once the sound or sound wave has entered the drum, it goes to a large structure called the cochlea. In this snail like structure, the sound waves are divided into pitches. The vibrations of the pitches in the cochlea are measured by the Corti. This organ transmits the vibration information to a nerve, which sends it to the brain for interpretation and memory.

### 4.3. Simulating the Natural Brain to Develop an Artificial Intelligent Brain(Blue Brain)

The diagram below gives an illustration on how the Natural Human Brain functions and a Simulated Artificial Intelligent Brain:

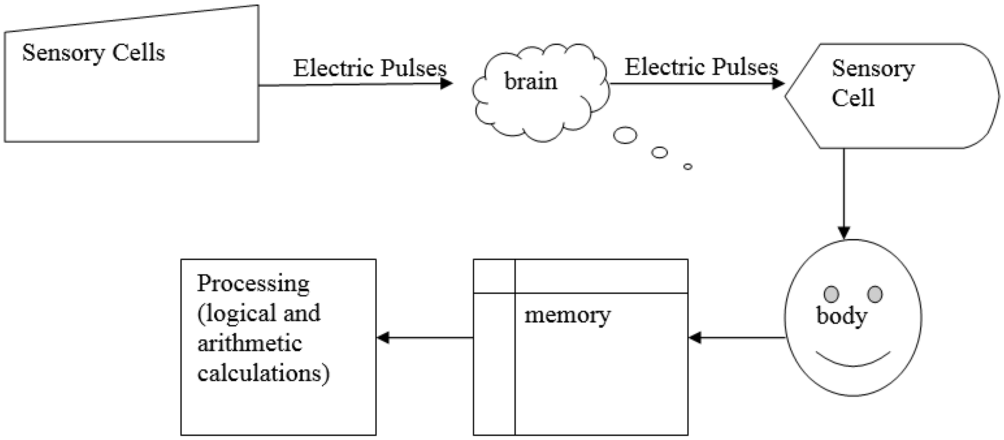


*FIG 2: An illustration of how the Natural Brain Works*

**4.4. Implementation:**

*4.4.1. Uploading human brain:*

The uploading is possible by the use of small robots known as the Nanorobots. These robots are small enough to travel through out our circulatory system. Traveling into the spine and brain, they will be able to monitor the activity and structure of our central nervous system. They will be able to provide an interface with computers that is as close as our mind can be while we still reside in our biological form. Nanorobots could also carefully scan the structure of our brain, providing a complete readout of the connections. This information, when entered into a computer, could then continue to function as us. Thus the data stored in the entire brain will be uploaded into the computer.

**4.5. Result Analysis**

1. We can remember things without any effort.
2. Decision can be made without the presence of a person.
3. Even after the death of a man his intelligence can be used.
4. The activity of different animals can be understood. That means by interpretation of the electric impulses from the brain of the animals, their thinking can be understood easily.
5. It would allow the deaf to hear via direct nerve stimulation, and also be helpful for many psychological diseases. By down loading the contents of the brain that was uploaded into the computer, the man can get rid from the mad ness.

## 5. CONCLUSION:

Great heroes have served the economy of the world at large in the past decade whose inmense contribution to life and society in all sectors have brought the world to what it is today, Examples are Lord Lugard who almagated the Nigeria in 1914, prominent people like Pa Obafemi Awolowo, Nelson Mandela and many other who have served this nation and humanity with high level of intelligent. The God endowored brain of this great men could not continue to be loss to the mother earth. Hence the once that are still living can be mortalised by creating a virtual brain of these highly intelliegent individuals.

Today we are developed because of our intelligence. Intelligence is the inborn quality that can not be created. Some people have this quality, so that they can think up to such an extent where other can not reach .Human society is always need of such intelligence and such an intelligent brain to have with. But the intelligence is lost along with the body after the death. The virtual brain is a solution to it. The brain and intelligence will be alive even after the death.

We often face difficulties in remembering things such as people's names, their birthdays, and the spellings of words, proper grammar, important dates, history facts, and etcetera. In the busy life every one want to be relaxed .Can’t we use any machine to assist for all these? Virtual brain may be the solution to it.

Service delievered to humanity by genius and highly intelligent personality is key to the development of any society. Hence, there is a need for such brains to be kept alive. Therefore, the development of an artificial brain will help to enhance the developement of citizens of a country and the world at large. It is thereby recommended that:

1. Awareness be created to the citizens of the country especially, those whose impact on the economy development of the country is paramount.
2. The Government to sponsor the design and implementation of this Nanobot.
3. Managerial Staff of various organizations and parastals should be encouraged to use the nanorobots when designed, so that there absence does not bring a pause to mode of operation.

**REFERENCE**

Blue Gene[online] (2005) Retrieved from: <http://www.research.ibm.com/bluegene>

Deep Blue[online] (2005) Retrieved from: <http://www.research.ibm.com/deepblue>

London, M. & Hausser, M. (2005) Dendritic computation. Annu. Rev. Neurosci. 28, 503–532

Markram, H. (2005) Dendritic object theory: a theory of the neural code where 3D electrical objects are formed across dendrites by neural microcircuits. Swiss Soc. Neurosci.Abstr. 196

NeoCortical Simulator[online] (2005). Retrieved from: <http://brain.cse.unr.edu/ncsDocs>

SGI[online] (2005).Retrieved from: <http://www.SGI.com>

The Blue Brain Project[online] (2005). Retrieved from: <http://bluebrainproject.epfl.ch>

The Human Brain Project[online] (2005). Retrieved from: <http://www.nimh.
nih.gov/neuroinformatics>

Traub, R. D. et al(2005)..Single-column thalamocortical network model exhibiting gamma oscillations, sleep spindles, and epileptogenic bursts. J. Neurophysiol. 93, 2194–2232

Full Paper

# FACTORS INFLUENCING THE ADOPTION OF E-GOVERNMENT SERVICES IN NIGERIA

**G. O. Ogunleye**
Redeemer's University(RUN)
Department of Mathematical Sciences (Computer Science Programme)
KM 46, Lagos-Ibadan Expressway, 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**

The rise of e-government has been one of the most striking developments on the web with the increased deployment of Information Technology (IT) by governments through the advent of the World Wide Web. E-government is an initiative aimed at reinventing how the Government works and to improve the quality of interactions with citizens and businesses through improved connectivity, better access, furnishes high quality services and better processes and systems. Nevertheless, e-government enterprise is still in their growing stage in the developing countries and is being confronted with numerous problems which limits its widespread use. Past research works showed that lots of works have been done on the e-government services in developing countries from the organizational perspective while the citizen's view is yet to be seriously examined.. The success of any e-government services depends on government support as well as on citizen's adoption. This paper therefore focuses on the exploration of the challenges and barriers of e-government services from the user's perspective. An amended version of the Unified Theory of Acceptance and Use of Technology (UTAUT) model is used to investigate the factors influencing the acceptance of e-government services in Nigeria. The results show that the factors influencing the adoption of e-government services in Nigeria are associated with ease of use, usefulness, social influence, technological issues, lack of awareness, data privacy, and trust

## 1. INTRODUCTION

The development of information and communication technology (ICT) has brought a considerable change to human life. Almost all governments worldwide are formulating more sophisticated ways to promote citizens' active involvement in governmental activities, offering them more effective access to e-government services. With this change and the fast growth of ICT, the paradigm has shifted from traditional government to electronic government. Around 98 percent of governments worldwide have websites and 173 out of 190 countries use contemporary information and communication technologies to deliver services to their citizens (UN, 2010). E-government offers the public service to be accessed 24 hours, whenever, and wherever the user is located. E-government can be defined as "the complete optimization of service delivery, constituency participation and governance by transforming internal and external relationships through technology, the Internet and new media" (Gartner Group, 2000). E-government related services include e-information, e-procurement, e-health; e-education and e-tax systems, and so on. E-government services offer citizens transparency in the process of governance, such as the following: time savings through efficient services; simplification of procedures; improved office management; and friendly attitudes of personnel (Monga, 2008). The success of e-government depends upon the citizens' willingness to adopt this innovation (Carter and Belanger, 2005). There is need for various governments across boards to examine and understand the factors that influence or could encourage citizens to use e-government services instead of traditional communication. Wang, 2003 revealed that many governments still face the problem of a low-level of adoption of e-government services by their citizens. Reddick (2005) observed that most e-government research focuses on the supply side (e.g., government infrastructures and policies), not on the demand side (the citizen's perspective). Parent et al. (2004) identified a range of factors that determine the adoption of e-government services, such as ease of use, perceived risk, reliability, relative advantage, trust, image, and facilitating conditions.

Moreover, Chen et al., (2006) investigated Information Technology(IT) adoption in different cultures and e-government services in the developed and developing world . Other studies have concentrated on gender differences and technology adoption (Venkatesh et al., 2003); lack of awareness and self-efficacy and computer anxiety. Despite the immense wealth and innovations, Nigeria's e-government status is still low. Nigeria's e-government status is determined by its e-Government development index of

1.02, an index measure below the UN's benchmark measure of 1.62 (Ifinedo, 2005). This can be verified by Nigeria's growth of Internet literacy, an important factor for e-government application being "very slow and the coverage, small" (Amalu, 2011). Internet penetration rates are very slow in Nigeria too with it being listed within the 120 low internet penetration countries. From recent statistics, Nigeria has 10,000,000 internet users, 500 broadband subscribers, 6.8 per cent internet penetration, and $2,300 GDP. Existing analyses of the e-government adoption have shown that a large segment of the published research was conducted in developed countries, such as the US (Carter & Belanger, 2005) and the UK (Carter & Weerakkody, 2008). Hence, little research has been done on factors influencing the adoption of e-government in developing countries (Alhujran and Chatfield, 2008), such as Nigeria. This paper examines the factors that influence the adoption of e-government services by citizens, which is an unexplored area in the demand side of e-government (i.e., the citizen's perspective). In order to achieve the objective of this research, a survey-based quantitative research strategy is acquired, using the amended unified theory of acceptance and use of technology (UTAUT) model. Using UTAUT, the study explores the factors that influence the adoption of e-government services in Nigeria, which is an example of a country where e-government services are in the development stage. Realizing these factors will help decision makers to ensure the satisfaction of citizens.

The paper is organised as follows: Section 2 introduces the context of the research by presenting a review of e-government in Nigeria, giving an overview of the adoption of e-government adoption in the context of technology acceptance models in developing countries in Africa. Furthermore, it introduces the outline of the theoretical model used in the research, and then presents the empirical background of the research. Section 3 sets presents the methodology used to explore the influential factors in the adoption of e-government services. Section 4 reports the results in the context of a review of the relevant literature. Section 5 presents the conclusions of the research and discusses its implications for future research. References are given in Section 6.

## 2. LITERATURE REVIEW

### 2.1. Nigeria and e-government

The emergence of e-Government in Nigeria can be traced to the advent of democracy in 1999. The first real activity in this regard was the development of government websites. These efforts were uncoordinated and only a few agencies with resources could establish an online presence although government continues to seek policies and strategies that will accelerate the deployment of the necessary infrastructure. Challenges to Nigeria's e-Government efforts are well documented (Ifinedo, 2005), of which the socio-economic inadequacies that exist in countries belonging to the Sub-Sahara region are highlighted. Other identified challenges include, poor organizational skills, inadequate infrastructural support and poor or limited human capital resources (ibid). Local e-Government initiatives have also been examined, but from a macro level where identification of policies and initiatives has occurred and the impacts measured using surveys (Ogbomo, 2009).

With e-government existence being reliant upon a telecommunications infrastructure and despite supply provisions in Africa, it is still not being used. This can be attributed to economic factors such as, pricing and costs incurred by consumers and awareness) and viewed as factors accounting for the slow diffusion of e-Government and ICT projects (Bagchi et al, 2007). Additional factors leading to e-government failure can be attributed to social factors such as, gender inequality and cultural issues. Studies show that especially in Africa, the younger-educated classes and men, use the internet more frequently, so that the result could be a one-sided concentration leading to the further systematic exclusion from online services of women and of the lower social classes (Nakafeero, 2005).

### 2.2. E-government adoption

Different investigators have referred to the adoption and use of e-government services as 'intention' (Carter and Bélanger, 2005; Warkentin et al., 2002) or 'willingness' (Gilbert et al., 2004). According to Kumar et al. (2007) adoption is "a simple decision of using, or not using, online services." Furthermore, Warkentin et al. (2002) elaborated that e-government adoption is "the intention to 'engage in e-government', which encompasses the intentions to receive information, to provide information and to request e-government services." The successful implementation of these e-government services is very important for governments of developing countries. Akman et al. (2005) explained that the success of e-government adoption depends on citizens. Like any other innovation, the beginning of e-government brings a number of challenges for citizens as well as for governments (Zakareya and Irani, 2005). These challenges include lack of awareness of e-government services, access, trust, security concerns, and the digital divide (Cater and Weerakkody, 2008; Huang, 2007; Carter and Belanger, 2005) and are hurdles that citizens must surmount in the usage and adoption process. Some researchers (Choudrie and Dwivedi, 2005) identified that the effect of these challenges varies in different countries in the implementation of e-government services.

According to a number of investigators (Choudrie and Dwivedi, 2005; Kumar et al., 2007; Wang, 2003), there is an explicit problem with the adoption of these services by citizen users. Belanger and Carter (2008) found that even though governments are increasing e-services, citizens are still more likely to use traditional methods. Moreover, Kumar et al. (2007) emphasized this dilemma, finding that the rate of adoption of e-government has fallen below expectations around the world, although some countries are doing better than others. Hence, low rates of adoption and usage are serious, continuing problem for governments.

*Table 1. Adoption of various e-government services in countries Source: Kumar et al., 2007*

| Country | Usage of e-gov services |
|---|---|
| Australia | 46% |
| Canada | 48% |
| Finland | 49% |
| Ireland | 26% |
| Poland | 27% |
| Hungary | 23% |
| Singapore | 53% |
| Kuwait | 23% |
| Taiwan | 40% |
| US | 52% |

Previous research (Kumar et al., 2007; Al-Adawi et al., 2005) provided empirical evidence of less e-government adoption worldwide. As shown in Table 1, adoption of e-government services is less than expected, at below 30 percent in Ireland, Poland, and

Kuwait and less than 50 percent in Australia, Canada, and Finland. Similarly, the adoption of an e-tax filing system in Taiwan was investigated twice, first by Wang (2003) who found less than 8 percent of citizens use the system. The second and later investigation (Fu et al., 2006), showed that 40 percent of taxpayers used the system. Both studies found that although this tax system was introduced in 1998, the tax payers in Taiwan still prefer a paper-based_filing_method. A similar survey conducted by Choudrie and Dwivedi (2005) inspected citizen awareness and adoption of e-government services in the UK. Unexpectedly, the researchers found that 76 percent of the respondents were not even aware of the "government gateway" in the UK. The study showed that only 6 percent of the respondents in the sample had registered for the "government gateway."

On the other hand, according to Gallant et al. (2007), in the US the proportion of citizens adopting e-government services is higher. In 2005, 52 percent of tax payers filed their tax forms electronically. Nevertheless, this proportion is far from the aim of having 80 percent of tax returns filed electronically by 2007. Another study by Carter and Belanger (2004b) showed that in the US, 52 percent of the respondents were using the Internet to gather information about or from the government.

According to the UN (2010), most developed countries benefit from e-government services, but there is still much room for improvement globally. Many challenges involved in the adoption of e-government services still exist, which leads to the low levels of the adoption of e-government services universally. Numerous researchers (UN, 2010; Cater and Weerakkody, 2008; Gupta, 2008; Kumar et al., 2007; Fu et al., 2006; Tung and Rieck, 2005; Gilbert et al., 2004) have suggested the necessity for more research in the area of e-government adoption. The above discussion shows that governments across the globe still face problems from the citizen's perspective, which demonstrates the need for studies that investigate the adoption rate of e-government services.

### 2.3. Technology Adoption Theory

Governments in both developed and developing countries spend huge amounts of financial resources on new information and communication technologies in order to make business run smoothly and connect to related bodies. These investments should result in acceptance and adoption of these technologies. Researchers use different types of technology acceptance models. According to Agarwal (2000) there is a very large body of research regarding the adoption of information technologies, which can be defined as the use or acceptance of a new technology or a new product (Karahanna et al., 2006).

A range of theories and models explain user acceptance and adoption of technology in the information systems domain. These include the theory of reason action (Fishbein and Ajzen, 1975), the technology acceptance model (TAM) (Davis et al., 1989), the motivational model (Davis et al., 1992), the model of pc utilization (Thompson et al., 1991), the diffusion of innovations (DOI) (Rogers, 1995), the theory of planned behavior (Taylor and Todd, 1995), social cognitive theory (Compeau & Higgins, 1995) and the unified theory of acceptance and use of technology (UTAUT) (Venkatesh et al., 2003). In order to avoid the limitations of the models named above, the UTAUT model combines constructs from each of them. UTAUT has four direct constructs: performance expectancy, effort expectancy, social influence, and facilitating condition. These explain 70 percent of technology acceptance and usage behaviour. Venkatesh et al. (2003) argued that the four constructs play a significant role as direct determinants of user acceptance and usage (Venkatesh et al., 2003). The UTAUT model is used and suggested for use in a similar context by many researchers. According to Rosen (2005), the UTUAT model should now serve as a benchmark for the acceptance literature because it explains user acceptance in a more complete and realistic manner than previous models. Although the UTAUT model is relatively new, it has proven to be valid and reliable in different context of technology adoption studies (e.g., e-government adoption), as shown in Table 2. Because of its suitability and uses the strengths of previous models, we use UTUAT model for this study.

Table 2:UTAUT model usage in various studies

| Usage | Details |
|---|---|
| Fahad Al Harby, et al. (2012) | End-Users' Acceptance of Biometrics Authentication to Secure E-Commerce within the Context of Saudi Culture: Applying the UTAUT Model |
| Venkatesh, V. et al., (2011) | Just What the Doctor Ordered: A Revised UTAUT for EMR System Adoption and Use by Doctors |
| Schaupp, et al., (2010) | E-file adoption: A study of US taxpayers' intentions |
| Wang, et al., (2009) | Why do people use information kiosks? A validation of the Unified Theory of Acceptance and Use of Technology |
| Alhujran et al., (2008) | Toward a Model for E-government Services Adoption: The Case of Jordan |
| Hung, Y et al., (2007) | User Acceptance of E-Government Services. Kaohsiung |
| Fu et al., (2006) | Acceptance of Electronic Tax Filing: A Study of Taxpayer Intentions |
| Ebrahim, (2005) | The adoption of e-government in the Kingdom of Bahrain |

## 3. RESEARCH METHODOLOGY

This section presents the methodology used for the research. We adopt a technology acceptance models approach to study the factors that affect e-service adoption in Nigeria. The data collection was conducted using a web survey. According to the UTAUT model, the four factors that affect technology adoption are performance expectancy, effort expectancy, social influence, and facilitating conditions. Following the UTAUT model, it can be expected that these main factors also affect e-government adoption in Nigeria. The applied research model is presented in Figure 1.

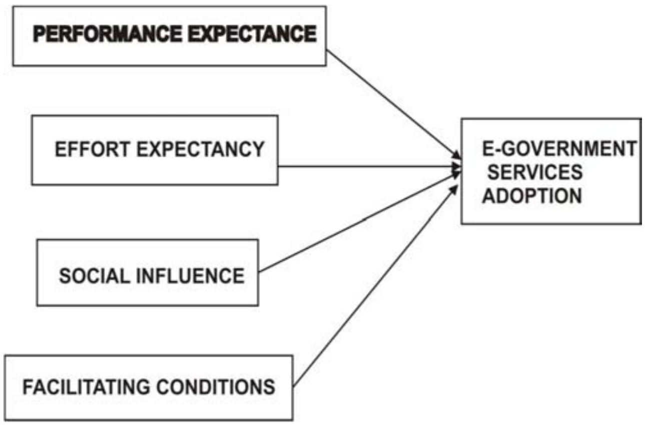


*Figure 1. Research model*

In this study, performance expectancy indicates that users believe that e-government services enhance their job performance. Users will adopt e-government services if they perceive them as helping them improve their performance. In previous theories of technology acceptance, the determinant of performance expectancy plays a key role. Effort expectancy measures that users perceived the usefulness, ease of learning and use e-government services. The existing theories and models show that the more effortless a technology is, the greater the usage and acceptance. Therefore it is important to determine the level of complexity of e-government services in terms of the degree to which a technology is perceived difficult to understand and use. Social influence is referred to as the users' perceptions of significance when they are required to use e-government services. The factor facilitating conditions elaborates on the necessary environment and whether help is available for the usage of e-government services or not.

The four determinants in the UTAUT model were evaluated in the survey using constructs that consist of corresponding groups of questions. Our questions were contrived based on past works of early researchers. The measurement was based on five-point ranging from 1 (strongly disagree) to 5 (strongly agree). The questions for the four constructs are shown in Table 3.

*Table 3: UTAUT model*

| Constructs | Measurement Items ( ___: Name of the technology) |
|---|---|
| Performance Expectancy | Using the _____ enables me to accomplish tasks more quickly.<br>Use of the _____ can decrease the time needed for my important job responsibilities.<br>Using the _____ would make it easier to do my job. |
| Effort Expectancy | Learning to operate the _____would be easy for me.<br>I would find it easy to get the _____to do what I want it to do.<br>I would find the _____easy to use.<br>My interaction with the _____is clear and understandable.<br>Overall, I believe that the _____is easy to use. |
| Social Influence | People who are important to me think that I should use the _____.<br>People in my organization who use the _____have more prestige than those who do not. |
| Facilitating Condition | I have the resources necessary to use the _____.<br>Specialized instructions concerning the _____was available to me.<br>A specific (or group) is available for assistance with _____difficulties. |

The survey included other questions concerning the relevant background of the participants. These questions were related to, for example, age, gender, internet usage and proficiency, and knowledge and previous usage of e-government services.

Nigerian University students were selected as the survey population because they are among the adult population for whom the internet has become part of a daily routine.

The questionnaire was distributed through different communication channels, such as personal email and various groups on social media websites for Nigerian students. The questionnaire was distributed to university students in Nigeria, and a total of 110 answered questionnaires were returned of which eight were discarded because of incorrect and missing information. In total, 102 survey respondents were used for the analysis. The respondents adopted a range of e-government services.

## 4. RESULTS

Of the 102 respondents used for the analysis, about 38 (37%) are adopters and 64 (62%) are non-adopters of e-government services. Of the Bachelor (39%), Master (53%) and PhD (8%) degree students from various departments, 80 percent are male respondents and 20 percent are female respondents. Over half the respondents are studying computer science, engineering and the other half, art and humanities. Almost all respondents (93%) have an internet connection and their internet proficiency is typically very good. Most respondents spend more than fifteen hours a week on the internet for information retrieval, transactions, and social networking. Seventy-eight percent of respondents prefer using e-services for communicating with government agencies and believe that existing e-government services are useful for them. Some participants still prefer traditional communication (i.e., direct office visit, 22%) because e-government is not fully implemented in Nigeria and is still in the growing stage.

### 4.1. Performance Expectancy

The performance expectancy factor was measured by three questions, leading to the three variables shown in Table 4. These questions were asked only of respondents who are currently using e-government services (n=38). These respondents feel that e-government services are used because they enable easier contact with government (mean=4.13), they allow quick completion of tasks (mean=3.82) and save time (3.71). The relatively high performance expectancy of the e-government service users group can be seen as allowing the users to avoid waiting in long queues and dealing with uncooperative staff in government offices. The average mean of the performance expectancy construct is 3.88, which indicates that users have a positive attitude towards using Nigeria's e-government services because they are more efficient. Similar results were found by different researchers.

*Table 4. Mean Score - Performance Expectancy*

| Performance Expectancy (n=38) | Mean | Median | Mode | Std. Deviation |
|---|---|---|---|---|
| Quick Task completion | 4.13 | 4.0 | 4 | 0.82 |

| | | | | |
|---|---|---|---|---|
| Easier contact | 3.82 | 4.0 | 4 | 1.04 |
| Time Saver | 3.71 | 4.0 | 4 | 1.09 |

*Scores range from 1 to 5, where 1 = Strongly Disagree and 5 = Strongly Agree.

### 4.2. Effort Expectancy

The effort expectancy factor was measured by five questions, leading to the five variables shown in Table 5. These questions were asked only of respondents who are currently using e-government services (n=38). The empirical results show that respondents share favourable views concerning effort expectancy (average mean=3.86). The overall perception of effort expectancy of the participants was that e-government services are easy to learn (mean=3.93); easy to use (mean=4.20); useful (mean=4.01); cost effective (mean=3.88) and provides clear interaction (mean=3.71). This analysis is also corresponding to the results of various researchers.

*Table 5. Mean Score - Effort Expectancy*

| Effort Expectancy (n=38) | Mean | Median | Mode | Std. Deviation |
|---|---|---|---|---|
| Easy to learn | 3.52 | 4.0 | 4 | 1.07 |
| Easy to use | 4.20 | 4.0 | 4 | 0.93 |
| Useful | 4.01 | 4.0 | 4 | 0.95 |
| Cost Effective | 3.88 | 4.0 | 4 | 1.02 |
| Clear Interaction | 3.71 | 4.0 | 4 | 1.04 |

*Scores range from 1 to 5, where 1 = Strongly Disagree and 5 = Strongly Agree.

### 4.3. Social Influence

The social influence factor was measured by two questions, leading to the two variables shown in Table 6. These questions were asked only of respondents who are currently using e-government services (n=38).

*Table 6. Mean Score - Social Influence*

| Social Influence (n=38) | Mean | Median | Mode | Std. Deviation |
|---|---|---|---|---|
| More prestige by using e-government services | 3.37 | 3.5 | 4 | 1.01 |
| People who are important suggest me to use | 3.20 | 3.5 | 4 | 1.08 |

The findings show that participants prefer to use e-government services, but some factors might influence adoption and usage. For instance, nearly half the participants (43%) agreed or strongly agreed that they obtain more prestige (mean=3.37) when they use e-government services and that their peers and families (mean=3.20) prefer them to use these services. They believed that these e-services make their life easier.

The average mean of social influence is 3.28, which shows that service users experience a positive social influence in using Nigeria e-government services. The findings show that the adopters of e-government services in Nigeria are socially influenced.

### 4.4. Facilitating condition

The respondents (n=102) of the survey mentioned the following stumbling block to the adoption of e-government services in Nigeria, as shown in Figure 2. Majority of the respondents (65%) mentioned that there is a lack of awareness, and more than half (50%) of the respondents emphasized the lack of assistance and effective guidelines. The respondents also blamed government personnel and the media for not broadcasting lots of existing services along with their benefits. The findings show that lack of awareness, proper help, and guidelines influence the acceptance and adoption of e-government services by Nigeria citizens. Therefore, the government should run rigorous advertising campaigns to ensure that people are aware of the use the services.

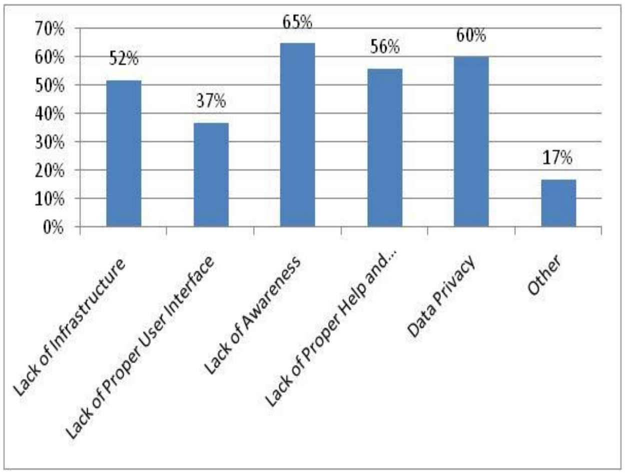


*Figure 2. Facilitating condition*

More than half of the respondents (52%) mentioned various technical problems in internet connections, such as disconnection/interruption during transactional services, frustrating delays, and slow processing. This result indicates that the National Database and Registration Authority (NADRA) of Nigeria is yet to gain the confidence of the people in respect to effective managing of e-government services to maintain the privacy of the citizens. In general, 60% of the respondents worried about their personal information and data privacy, which brings up the issue of the trustworthiness of e-government services.

Cronbach's coefficient alpha values were selected to study the internal consistency of the measure. Internal consistency can be determined by the procedure developed by Cronbach (1951). Hinton et al., (2004) had proposed four different points of reliability, excellent ranges (0.90 and above), high (0.70- 0.90), high moderate (0.50-0.70) and low (0.50 and below). The reliability for each construct is shown in Table 7, which shows that some constructs have high reliability.

*Table 7: Reliability measurement*

| Constructs | No. of items | Cronbach's Alpha |
|---|---|---|
| Performance | 3 | 0.724 |

| | | |
|---|---|---|
| Expectancy | | |
| Effort Expectancy | 5 | 0.833 |
| Social Influence | 2 | 0.705 |

The results of Cronbach's alpha were between 0.705 in social influence construct and 0.833 in the effort expectancy construct, indicating that the constructs are internally consistent and the reliability is measured for the same construct.

## 5. CONCLUSION

The primary focus of this paper is to study the broad factors of e-government adoption from a user's perspective in the Nigeria context. The user's adoption of e-government services in Nigeria can be studied based on the UTAUT model constructs, which introduce the factors affecting technology acceptance. These constructs are performance expectancy, effort expectancy, social influence, and facilitating conditions.

The finding reveals that there is a low level of adoption of e-government services in developing countries such as Nigeria. One reason is that the citizens lack knowledge about the new e-government services. The results showed that respondents considered awareness an important issue for the use of e-government services. The Nigeria government should raise awareness throughout the country regarding their e-services through different advertising channels. The empirical results demonstrated out that the respondents share adverse views about updated websites and the satisfactory provisions of electronic resources in Nigeria. In this respect, the government e-services and websites should be updated on a regular basis and incorporated with online chats in which citizens can communicate with experts to gain immediate information about all e-government services of Nigeria. Furthermore, online help facilities should also be incorporated on the websites, which would allow more users to adopt Nigeria e-government services. This research also highlighted that respondents share favourable views concerning friendly interfaces with existing e-government services. On the other hand, greater authentication and identification procedures are necessary for citizens to develop high levels of trust since the present research found that respondents share unfavourable views regarding lack of awareness, security, and privacy of personal information.

The adoption of e-government services and technology acceptance theories has been widely studied in developed countries. However, few studies have been done in Nigeria, which is a developing country.

The present study is unique in the Nigeria context because it focuses on the user's perspective, which can serve as a starting point for other e-government adoption researches in Nigeria. In addition, the practical significance of this study is that it can be helpful for government policy and decision makers in the design and implementation of e-government services in Nigeria and other developing countries. For example, they should implement policies and strategies that emphasize awareness, security, privacy, and user trust in e-government services. The implementation of Nigeria e-government services is in the early stage, so understanding these factors would help to improve planning and deployment. Although the results of this study are interesting, they are limited to a group of adopters of e-government services. For that reason, the perceptions of the non-adopters of e-government services should be studied in future research. Furthermore, this study can be extended by incorporating the UTAUT model moderators (i.e., age, gender, experience) and other determinants, such as culture, trust, and socio-economic constraints. Hence, further research is required to overcome these limitations.

## REFERENCES

Agarwal, R., Sambamurthy, V., and Stair, R.M. (2000). "Research report: The evolving relationship between general and specific computer self-efficacy - An empirical assessment". Information Systems Research, 11(4): 418-430.

Akman, I., Yazici, A., Mishra, A., and Arifoglu, A. (2005). 'E-Government: A global view and an empirical evaluation of some attributes of citizens'. Government Information Quarterly, 22(2): 239-257.

Al-Adawi., Z, Yousafza., S and Pallister, J. (2005). "Conceptual model of citizen adoption of e-government" . Proceedings of the Second International Conference on Innovations in Information Technology, 26(28): 1-10.

Alhujran, O., and Chatfield, A. (2008). "Toward a Model for E-government Services Adoption: The Case of Jordan". Proceedings of the 8th European Conference on e-Government, Ecole Polytechnique, Lausanne, Switzerland, 13-22.

Amalu, C.(2011). E-Government Strategy: How prepared Is Nigeria? Published byLeadership Newspaper, http://leadership.ng/nga/articles/1859/2011/07/12/e-govt_strategy_how_prepared_nigeria.html (Accessed date: 10/04/2011)

Bagchi, K., Udo, G. and Peeter, K. (2007). Global Diffusion of the Internet Xi: The Internet Growth in Africa: Some Empirical Results. Communications of the Association of information Systems, 19:325-51.

Carter, L and Weetakkody, V. (2008). "E-government adoption: A culture comparison, Information Systems Frontiers", Springer, 10(4): 473-482.

Carter, L., and Bélanger, F. (2004b). 'The Influence of Perceived Characteristics of Innovating on e-Government Adoption'. Electronic Journal of e-Government, 2(1): 11-20.

Carter, L., and Bélanger, F.( 2005). "The Utilization of E-Government Services: Citizen Trust, Innovation and Acceptance Factors". Information Systems Journal, 15(1): 5-25.Reddick, C. "Citizen Interaction with E-government: From the Streets to Servers? " Government Information Quarterly. 22(1): 38-57.

Chen,Y., Chen, H., Huang, W., and Ching, R. (2006). "E-government strategies in developed and developing countries: an implementation framework and case study". Journal of Global Information Management, 14 (1): 23-46.

Choudrie J. and Dwivedi Y. (2005). Investigating the research approaches for examining technology adoption issues. J Res Pract 1(1):1–12

Compeau, D., and Higgins, C. (1995a). "Computer self-efficacy: Development of a measure and initial test". MIS Quarterly, 19(2): 189-211.

Cronbach, L. J. (1951) "Coefficient alpha and the internal structure of tests. " Psychometrika 22:3, pp. 297-334.

Davis F, Bagozzi, D. Paul, R., and Warshaw. (1989).

"User Acceptance of Computer Technology: A Comparison of Two Theoretical Models".Management Science, 35 (8):982-1003.

Davis,F., R. Bagozzi., and P, Warshaw. (1992)." Extrinsic and intrinsic motivation to use computers in the workplace".Journal of Applied Social Psychology, 22(14):1111-1132.

Ebrahim, Z. (2005). "The adoption of e-government in the Kingdom of Bahrain. School of Information Systems", Computing and Mathematics: Brunel University.

Fahad, AL, Rami Q. and Mumtaz K. (2012), End-Users' Acceptance of Biometrics Authentication to Secure E-Commerce within the Context of Saudi Culture: Applying the UTAUT Model, International Journal of Cloud Applications and Computing, ppg 10-21.

Fishbein. M and Ajzen, I. (1975). “Belief, attitude, intention and behaviour: an introduction to theory and research”, Addison-Wesley, Reading, MA. Gupta, B, Dasgupta, S., and Gupta, A. 2008. 'Adoption.

Fu, J, Farn, C and Chao, W. 2006. 'Acceptance of Electronic Tax Filing: A Study of Taxpayer Intentions'. Information & Management, 43(1):109-126.

Gallant, L., Culnan, M., and McLoughlin, P. (2007). “Why People e-File (or Don’t e-File) their Income Taxes”. Proceedings of the 40th Hawaii International Conference on System Sciences,107-112

Gartner Group (2000). E-government strategy: cubing the circle. Research Notes, Strategic Planning Assumption, 20 April 2000. [WWW document].

Gilbert, D., Balestrini, P., and Littleboy, D. (2004). “Barriers and Benefits in the Adoption of E-government”. International Journal of Public Sector Management, 17(4):286-301.

Hinton, P., Brownlow, C., McMurvay, I., and Cozens, B. (2004). SPSS explained , East Sussex, England: Routledge Inc.

Hung, Y., Wang, Y. and Chou, S. (2007). “User Acceptance of E-Government Services. Kaohsiung”. Natl Sun Yat-Sen Univ.

Ifinedo, P. (2005). Measuring Africa's e-readiness in the global networked economy: A nine-country data analysis International Journal of Education and Development using ICT. Available at: http://ijedict.dec.uwi.edu/viewarticle.php?id=12.

intentions’. Computers in Human Behavior, 26(4), 636-644.

Karahanna, E., Agarwal, R., and Angst, C. (2006). 'Reconceptualising compatibility beliefs in technology acceptance'. MIS Quarterly, 30(4): 781–804.

Kumar, V., Mukerji, B., Butt, I., and Persaud, A. (2007). 'Factors for Successful E-government Adoption: a Conceptual Framework'. Electronic Journal of e-Government, 5(1): 63-76.

Monga, A. (2008), “E-government in India: Opportunities and challenges”, Journal of Administration & Governance, Vol. 3. No. 2.

Nakafeero, A.(2005). Women and ICTs tools in Uganda: Bridging the Gender Digital Divide. In J. Hellstrom(Ed.), ICT- A tool for Poverty Reduction? Challeges for Development Cooperation (pp. 27-32). Uppsala: The Collegium for Development Cooperation. Uppsala University.

Ogbomo, M. (2009). Information and Communication Technology (ICT) in Local Government Administration: The Case of Oshimili North Local Government Area of Delta State. Library Philosophy and Practice July.

Parent. M , Vandebeek C. and Gemino. A. (2004). 'Building trust through e-government'. Government Information Quarterly, 22: 720-736.

Reddick, C. (2005).”Citizen Interaction with E-government: From the Streets to Servers?'”overnmentInformation Quarterly. 22(1):
38-57.

Rogers, E. (1995). 'Diffusion of Innovation (3rd ed.) '. Free Press, New York.

Rosen, P., (2005), ‘The effect of personal innovativeness on technology acceptance and use’, PhD Dissertation, Oklahoma State University.

Schaupp, L., Carter, L. and McBride, M. (2010). ‘E-file adoption: A study of US taxpayers

Taylor, S., and Todd. P. (1995). ”Understanding information technology usage: A test of competing
Models”.Information Systems Research, 6(2):144-176.

Thompson, R., Higgins. C., and Howell. J.(1991).”
Personal computing: toward a conceptual model of
Utilization”.MIS Quarterly, 15(1):124-143.

Tung, L., and Rieck, O. (2005). “Adoption of electronic government services among business organizations in Singapore”. Journal of Strategic Information Systems. 14(4): 417-440.

UN, (2010). “United Nation E-Government survey”, Retrieved by <http://unpan1.un.org/ intradoc/ groups/public/documents/UN-DPADM/ UNPAN038853.pdf >, [Accessed 15.01.2011].

Venkatesh, V., Morris, M., Davis, G. and Davis, F. (2003). User Acceptance of Information Technology: Toward a Unified View. MIS Quarterly, 27(3), pp. 425-478.

Venkatesh, V.; Sykes, T.; Xiaojun Zhang. (2011). 'Just What the Doctor Ordered: A Revised UTAUT for EMR System Adoption and Use by Doctors‘. System Sciences (HICSS), 44th Hawaii International Conference on , pp.1-10.

Wang, Y. (2003). 'The Adoption of Electronic Tax Filing Systems: An Empirical Study'. Government Information Quarterly, 20(4): 333-352.

Wang, Y. S. and Shih, Y. W. (2009). ‘Why do people use information kiosks? A validation of the Unified Theory of Acceptance and Use of Technology’. Government Information Quarterly, 26(1), 158-165.

Warkentin, M., Gefen, D., Pavlou, P., and Rose, G. (2002). “Encouraging citizen adoption of e-government by building trust”. Electronic Markets, 12(3): 157-162.

Zakareya, E., and Irani, Z. (2005). “E-government adoption: Architecture and barriers”. Business Process Management Journal, 11(5): 589-611.

Full Paper

# IMPLEMENTING AN E-DEMOCRACY SYSTEM IN NIGERIA

**A.A. Azeta**
Department of Computer and Information Sciences,
Covenant University, Ota, Nigeria
azetaambrose@gmail.com

**V. I. Azeta**
National Productivity Center, Kaduna, Nigeria
victaazeta@gmail.com

**O. Oluwaseun**
Department of Computer and Information Sciences,
Covenant University, Ota, Nigeria
oolaniyann@gmail.com

**A. E. Azeta**
Federal Institute of Industrial Research, Oshodi
azetaangela@yahoo.com

**G.A. Ayeni***
Department of Computer Science,
Allover Central Polytechnic, Sango Ota.
ayena1@hotmail.com

## ABSTRACT

E-Democracy basically comprises the use of electronic communications and technologies such as the internet resources, in enhancing and advancing the democratic process within a democratic republic. E-Democracy is an innovation still in its infant stage; and is still subject to much debate and activity within government, civic oriented groups and societies around the world. In most developing countries including Nigeria, there exists a low attitude of participation of the citizens in governance. Social, political, insecurity, Corruption and other forms of electoral manipulation discourage the electorate from getting involved in the government. From the various elections conducted since independence, about half the number of registered voters actually voted during elections. In addition, less than half of those who voted were involved in participatory governance. This paper developed a web-based system that will foster and encourage active citizenship participation by implementing democratic practices like voting and election campaign. The system was developed using PHP as front end, Apache as web server and MySQL as back end Database.

The developed system will among other things reduces the success of rigging during elections, reduces some undue electoral processes thereby saving time and allows for easy communication between the citizens and their elected candidates.

**Keywords:** *Citizen, E-Democracy, Election, E-Governance, Voting and Participation*

## 1. INTRODUCTION

Democracy as a form of governance and as a concept of free rule stretches beyond elections, voting and other electoral practices as its basic components. Interaction, cooperation and communication among all participants in a democratic setup are also a very critical component of a “working” democracy. Democracy actually entails the running of a nation by the people of the nation. People of the nation comprise both the elected and the ordinary citizens or voters. Putting an “e” in front of democracy means nothing more than using information technology tools to facilitate, improve and ultimately extend the exercise of democracy (Caldow, 2004). E-Democracy is positioned as a tool in enhancing and making the democratic process more accessible; ensuring citizen participation in public policy decision-making. This would enable broader influence in policy outcomes as more individuals involved could yield smarter policies; increasing transparency and accountability, and keeping the government closer to the consent of the governed, increasing its political legitimacy, especially in the Nigerian context where issues like lack of transparency and bad governance constitute hindrances to the development of our infant democracy. ICT has grown at an exponential rate, and does not only focus its attention on the internet but also spreads its wings to cover telecommunication, whereby people are connected and can communicate to themselves through cell phones, home personal computers and other medium. Internet, from statistics, has been discovered to be the most used and sort after medium of communication than the personal computers and the telephone put together.

ICT has the potential to engage people in all areas of the political process such as the generation of information, enhanced deliberation among citizens, and most of all enhance participation in decision making (Briony, 2003). ICT is one of the best means of bridging the communication gaps between the people and the government. Through the internet, it is now possible for the government to communicate with the citizens of the nation more effectively, and also aid the communication between citizens and their fellow citizens to discuss political and governmental issues which could be a resourceful contribution to the improvement of governance and most democracy.

Nigerian citizens continually express dissatisfaction over results of elections. The general opinion is that individuals who are declared as winners of the various elections must have rigged to win. No doubt, we are in a transition period after over a decade of military rule but we cannot continue to give excuses for our lack of coordination and inept to perfect the art of democracy. Bribery and corruption has been the order of the day at all levels of governance. Citizen-participation in governance is at its lowest level in the nation. This clearly indicates that the Nigerian democratic system is quite porous, inefficient and susceptible to negative infiltrations. Therefore, it will not be out of place to declare that our overall democratic process in Nigeria requires some “step up”.

The world of ICT provides a perfect “step up” solution as it makes available, a platform on which the “ills” of lack of citizen-participation and lack of transparency in governance can be adequately treated. E-Democracy as a concept is the fusion of ICT and traditional democratic practices in an attempt to involve the nation’s citizens in policy making.

It is not aimed at throwing out traditional democracy but its main aim is fulfilling the essence of democracy by involving the citizens fully through the use of the various technologies, methods, tools and systems made available by the internet. It is also aimed at developing digital citizenship through the use of ICT to create personal contact, dialogue and consultation among participants in democracy (Flavio, 2005). E-Democracy does not just stop at the levels of the citizens, but goes as far as fostering the communication among administrators, associations, public and private entities among the various tiers of governments. E-Democracy is a form of e-government. E-government is the use by government agencies of information technologies (such as Wide Area Networks, the Internet, and mobile computing) that have the ability to transform relations with citizens, businesses, and other arms of government.

These technologies can serve a variety of different ends: better delivery of government services to citizens, improved interactions with business and industry, citizen empowerment through access to information, or more efficient government management. The resulting benefits can be less corruption, increased transparency, greater convenience, revenue growth, and/or cost reductions (Godwin and Amodi, 2012).

In Nigeria, there is lack of trust, probity, transparency and accountability in the running of government. Access to government officials is low and interaction among players in the national democratic setup is lacking. The average Nigerian does not have a proper platform to clearly express his or her views, opinions and ideas in the light of moving the nation forward. This has led to lack of patriotism and national cooperation.

The objective of this study is to develop a web-based e-Democracy system for increased citizen participation in governance, building a stronger democracy and nationwide community through the power of information and communication technologies using Nigeria as a case study. The system will foster and encourage active citizen participation by implement democratic practices like voting and election campaign.

## 2. RELATED WORK

Over the years, e-Democracy systems have been adopted by various governments with respect to some peculiar features of the environment in which such governments operate in. Previous researches have discusses how information and communication technologies (ICTs) might be used to help engage people, both old and young, in the democratic process (Oates, 2003).

Examples of such systems include the following (OECD, 2003): (1) Electronic democracy New Zealand which has built a web site for easy communication between government officials with their citizens. The web also allows for suggestions, has links to different facilities like the electronic voting facility, political party sites and other features that enable the citizens to contribute. (2) Electronic Democracy USA, has fused her E-Democracy with its conventional system of government. They decided to make democracy more participatory, trustworthy and the results dependable. (3) Electronic democracy Australia, Australia also has adopted the electronic democracy system and according to reports has recorded some form of success though there are some forms of short comings. For the past twenty years, they have seen the acceleration and the intensification of the use of the computer and other digital means to improve and make significant impacts on the economic, social and political participation and democracy. In their own way, they have decided to make the software they use for this system an open source software, this free software allows and even encourages the source code to be modified and adapted, a more recent twist to the open source content is open content, or media created by witnesses and sent to wide audiences through various media channels, which make the citizens know that no form of manipulation takes place during the elections.

However, some factors have been identified by (Kamar and Ongondo, 2007) as barriers to effective E-Government implementation in developing countries such as Nigeria. These include (1) The government being faced with management challenges in the implementation of E-Government. The uncoordinated E-Government activities result from low level of public administration of E-Services as well as low quality and insufficient E-Content information from grassroots levels. (2) Low information technology literacy in a country which slows down the process of E-Government, among others. Notwithstanding, The most important anticipated benefits of e-government in a developing country include improved efficiency, increase in transparency and accountability of government functions, convenient and faster access to government services, improved democracy, lower costs of administrative services and these benefits can be realized (Adeyemo, 2011)

## 3. SYSTEMS DESIGN AND IMPLEMENTATION

The electronic democratic system was designed using unified modeling language (UML). The E-Democracy developed consists of the following modules:-e-mail, e-petition, e-voting, e-polls, e-campaign, e-forum, chat, news and information monitoring. This modules work hand in hand in the realization of the overall objectives of the e-Democracy system. The software administration module principally involves the operations and processes that focus on the general administration and management of the system. The module of the E-Democracy system includes the following:

E-voting module: comprises of the functionalities that enable users cast their vote during elections. Users cannot vote until the administrator has set the election date and other parameters.

E-campaign module: allows government officials and electoral candidates to campaign during elections.

E-mail module: is used to foster communication among participants in democracy. Citizens can send e-mails to one another and to government officials. This makes government officials very accessible. E-mails are sent using the national ID card number of the receiver as the e-mail ID. E-forum module: comprises of the facilities that enable users of the system post forum topics, discussing issues of national relevance, deliberating on government policy generation and implementation and other important issues. The forum also allows users reply and contribute to forum topics posted by other users.

News and information module: basically entails the provision for dynamic posting and monitoring of news on the system by all users and visitors to the site. The software administrator posts the news which can be viewed on the home page of the system.

Chat module: comprises of the facilities that enable users that are online interact in a public chat room.

E-petition module: provides functionalities for citizens to make complaints and state observations. A petition could be either public or confidential. A public petition is posted on the home page for all to view, while a confidential petition is viewed only by the administrator who handles the petition appropriately.

E-poll module: makes available functionalities for the creation of opinion polls for users to cast their vote on. This is a tool for the assessment and evaluation of government progress and public opinion on a particular issue.

The system is designed such that every Nigerian has a user account; however for security reasons, and to be registered on the system you would need to obtain your national ID card. Free registration on the E-Democracy Nigeria website will make the system susceptible to security attacks as miscreants could register fake individuals and so on. The system will be plugged on to the database of the federal government agency in charge of national ID cards. On the other hand, there is the administrator who has the privilege of registering users. What this implies is that immediately the national ID card is obtained by the Nigerian, he automatically has an account with the system. The default username for logging in is the national ID card number of the individual while the default password is the individual's surname; which can be changed at will.

Users of this system are: The citizens, the government officials and the system administrator. Every Nigerian who does not hold a political office falls under the category of users described as citizens. They have the privileges of voting, sending e-mails, adding and replying forum threads or topics, sending petitions, chatting and changing their login passwords which are by default their surnames. Individuals registered as government officials are those who are elected and sworn-in political leaders such as senators, governors, representatives, and the president. Electoral candidates are also registered as government officials. The government official has all the privileges of a citizen plus the privilege to campaign during elections.

The system administrator is the overall administrator of the system. He can register users, add electoral candidates, add political parties, view petitions, create opinion polls, edit member records, set election dates, upload news and other information, and publish election results. This system does not intend to totally remove the conventional system, but there is meant to be a fusion between the existing traditional system and E-Democracy system.

A formal model of the proposed system was built using Unified Modeling Language (UML). The UML is a modeling system which provides a set of conventions that are used to describe a software system in terms of functional design. It offers diagrams that provide different perspective views of the system parts. Figure 1 shows the activity diagram of the E-Democracy system. A user log into the system with a unique username and password to access all the modules that makes up the system. When done, he or she clicks on the logout button to exit the system.

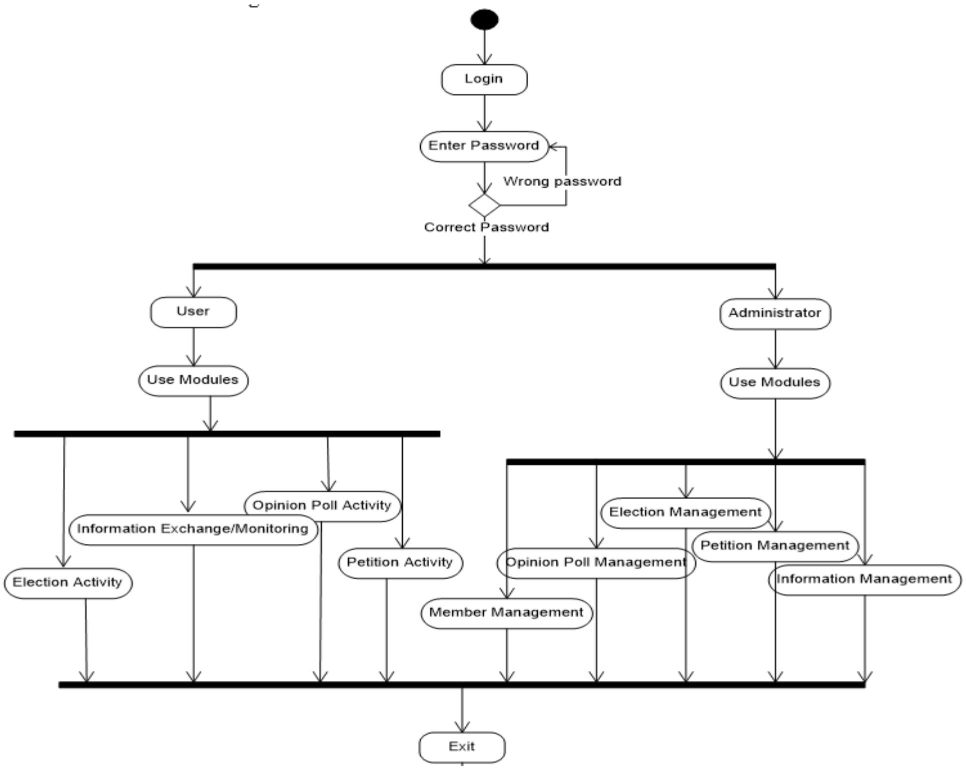
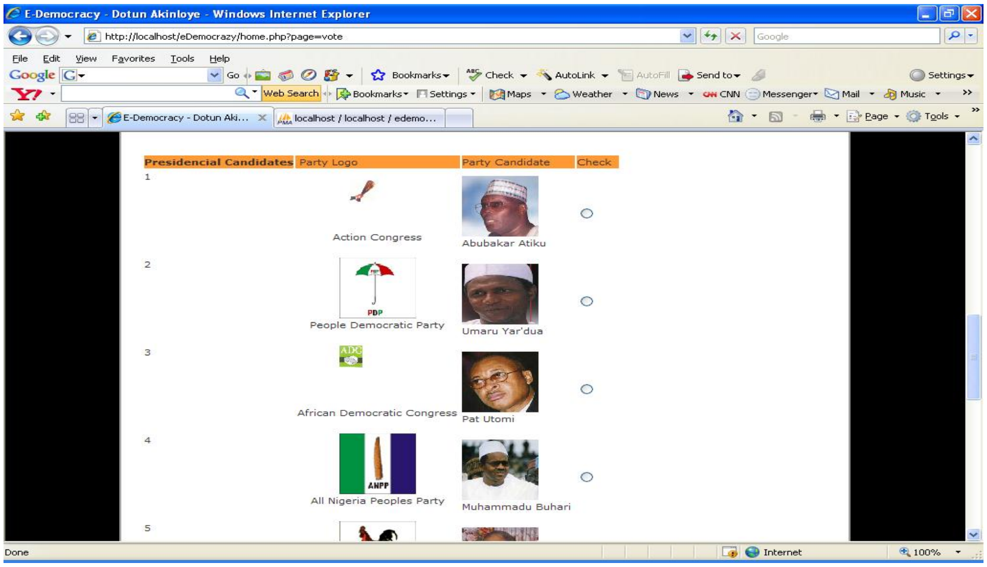
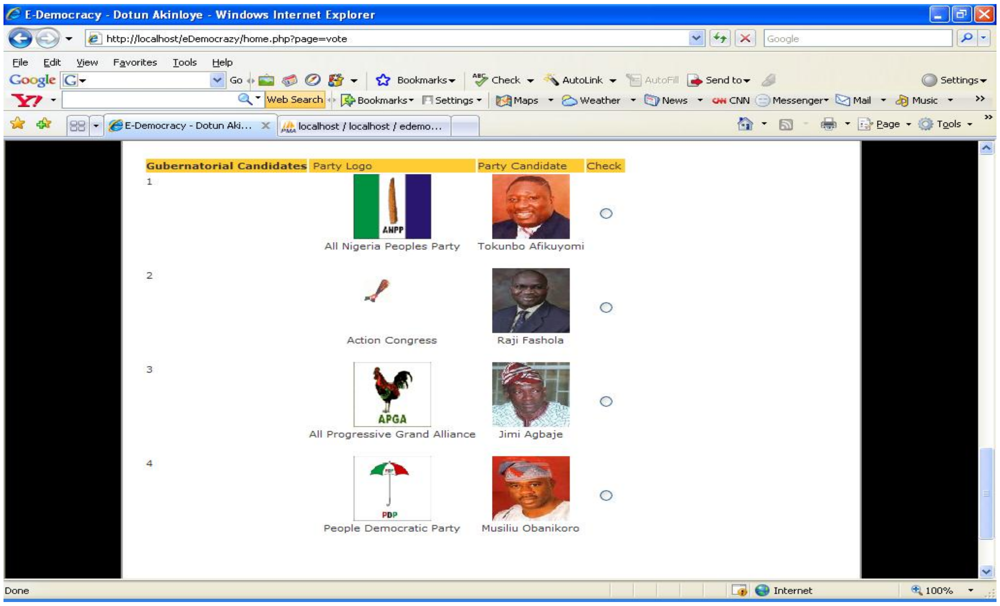


*Figure 1: Activity diagram for E-Democracy system*


E-Democracy - Dotun Akinloye - Windows Internet Explorer
http://localhost/eDemocrazy/home.php?page=vote
File Edit View Favorites Tools Help
E-Democracy - Dotun Aki...
localhost / localhost / edemo...
Done
Internet
100%

| Presidencial Candidates | Party Logo | Party Candidate | Check |
|---|---|---|---|
| 1 | Action Congress | Abubakar Atiku | ○ |
| 2 | People Democratic Party | Umaru Yar'dua | ○ |
| 3 | African Democratic Congress | Pat Utomi | ○ |
| 4 | All Nigeria Peoples Party | Muhammadu Buhari | ○ |
| 5 | | | |

*Figure 2: Voting Page for Presidential Election.*


E-Democracy - Dotun Akinloye - Windows Internet Explorer
http://localhost/eDemocrazy/home.php?page=vote
File Edit View Favorites Tools Help
E-Democracy - Dotun Aki...
localhost / localhost / edemo...
Done
Internet
100%

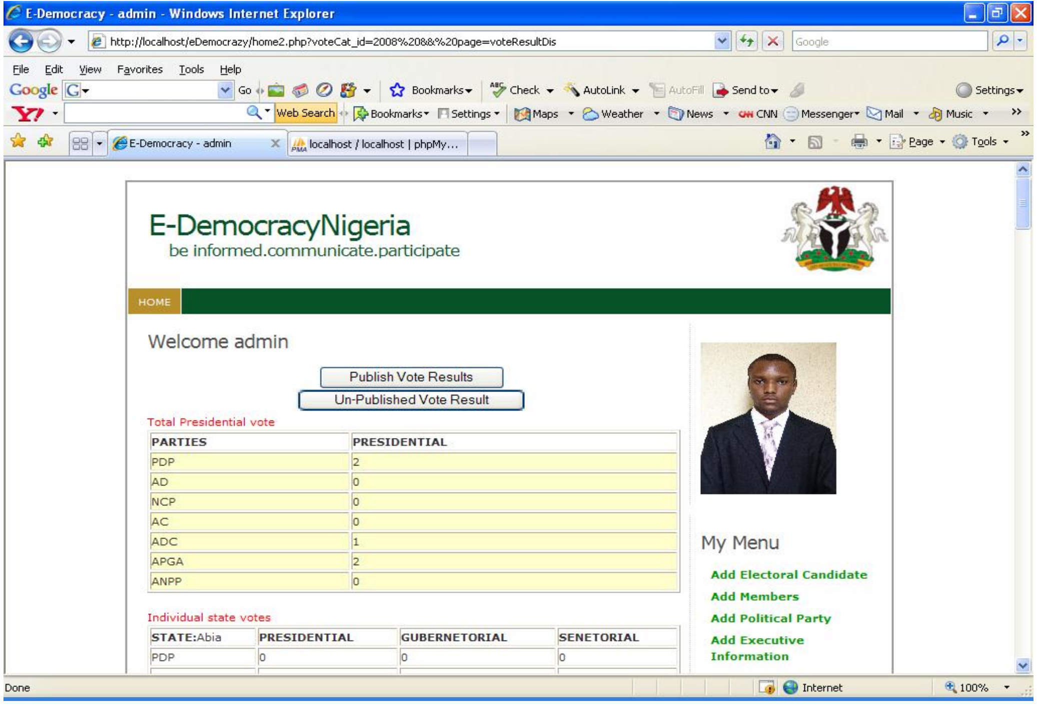
| Gubernatorial Candidates | Party Logo | Party Candidate | Check |
|---|---|---|---|
| 1 | All Nigeria Peoples Party | Tokunbo Afikuyomi | ○ |
| 2 | Action Congress | Raji Fashola | ○ |
| 3 | All Progressive Grand Alliance | Jimi Agbaje | ○ |
| 4 | People Democratic Party | Musiliu Obanikoro | ○ |

*Figure 3: Voting Page for Gubernatorial Election.*

The implemented E-Democracy system contains several screen shots, out of which the following five figures are reported. Figure 2 contains Voting Page for Presidential Election; Figure 3 shows Voting Page for Gubernatorial Election and Figure 4 includes View Election Result Page. Figure 5, Chat Page, enables registered users to chat, and Figure 6, Opinion Poll Result Page, shows the outcome of an opinion poll submitted by users of the system. For the e-Voting module of the system, the system administrator starts by authorizing the date of the election. Thereafter, the voters select the candidates of choice in both the presidential and gubernatorial elections. The results are automatically displayed by the system at the end of the election period.

## 4. RESULTS AND DISCUSSIONS

The Merits of the new system are as follows: (i) the process of rigging an election is minimized, (ii) it is time saving because some long electoral processes are eliminated, (iii) it allows for easy communication between the citizens and their elected candidates, (iv) it gives the citizens outside the country an opportunity to vote if they so please, (v) it automatically puts the tedious registration exercise aside and makes registration easier, (vi) It makes voting more interesting and more participatory since all the citizens are giving an opportunity to speak their mind, (vii) It tries to make all citizens know that they all have equal rights and opportunities, and(viii) it is more accessible to all kinds of people because of its global nature.


E-Democracy - admin - Windows Internet Explorer
http://localhost/eDemocrazy/home2.php?voteCat_id=2008%20&&%20page=voteResultDis
File Edit View Favorites Tools Help
E-Democracy - admin
localhost / localhost | phpMy...
E-DemocracyNigeria
be informed.communicate.participate
HOME
Publish Vote Results
Un-Published Vote Result
My Menu
Add Electoral Candidate
Add Members
Add Political Party
Add Executive Information
Done
Internet
100%

Welcome admin

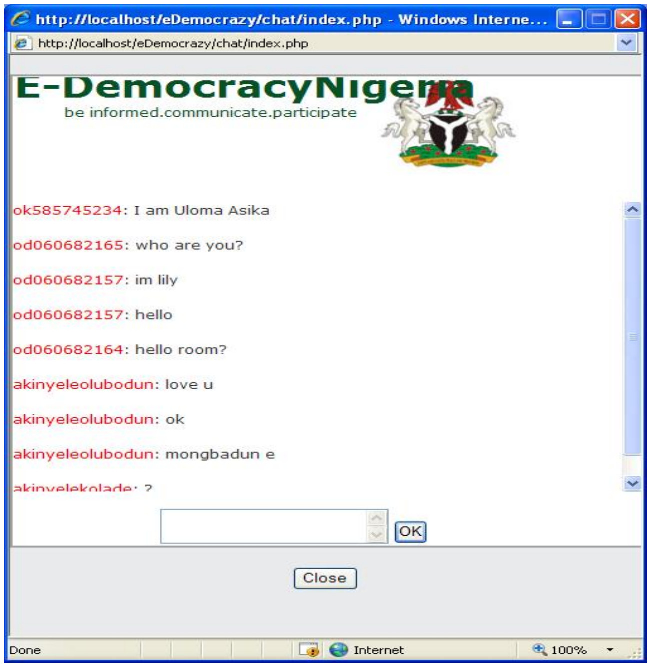
Total Presidential vote

| PARTIES | PRESIDENTIAL |
|---|---|
| PDP | 2 |
| AD | 0 |
| NCP | 0 |
| AC | 0 |
| ADC | 1 |
| APGA | 2 |
| ANPP | 0 |

Individual state votes

| STATE:Abia | PRESIDENTIAL | GUBERNETORIAL | SENETORIAL |
|---|---|---|---|
| PDP | 0 | 0 | 0 |

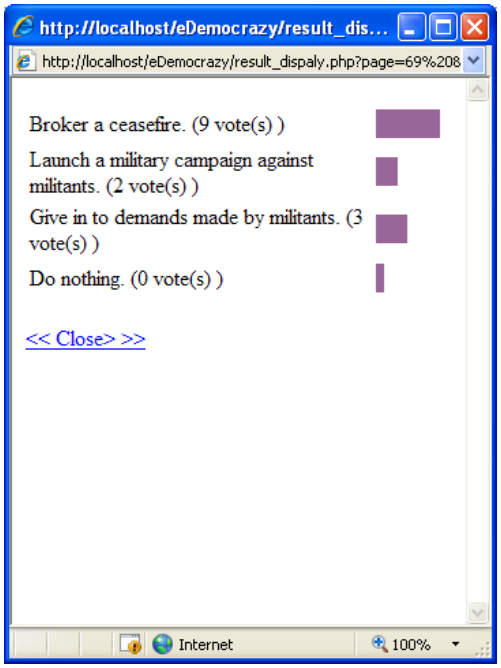
*Figure 4: View Election Result Page*


http://localhost/eDemocrazy/chat/index.php - Windows Interne...
http://localhost/eDemocrazy/chat/index.php
E-DemocracyNigeria
be informed.communicate.participate
OK
Close
Done
Internet
100%

ok585745234: I am Uloma Asika
od060682165: who are you?
od060682157: im lily
od060682157: hello
od060682164: hello room?
akinyeleolubodun: love u
akinyeleolubodun: ok
akinyeleolubodun: mongbadun e
akinyelekolade: ?

*Figure 5: Chat Page.*

This study has demonstrated that electronic solutions are available to solve the problems of election malpractice, lack of communication between the elected and the voter, and corruption in Nigeria as in other developing countries. It will be paramount to state that if this E-Democracy system is to be properly and efficiently implemented and deployed in the Nigerian context or in any other country, it will be expedient for the government of the nation to legally institute an E-Democracy agency and endorse it's activities by making some inclusions and adjustments on the constitution guiding the administration of the nation's democracy. We also recommend that the E-Democracy agency be charged with the duties of administering the E-Democracy system, ensuring it remains secure and safe from every form of security, making sure the system is up-to-date with any changes in policies or government administration.


http://localhost/eDemocrazy/result_dis...
http://localhost/eDemocrazy/result_dispaly.php?page=69%208
<< Close> >>
Internet
100%

Broker a ceasefire. (9 vote(s) )

Launch a military campaign against militants. (2 vote(s) )

Give in to demands made by militants. (3 vote(s) )

Do nothing. (0 vote(s) )

*Figure 6: Opinion Poll Result Page.*

As part of our recommendations, this system to be put to functional use, the government of Nigeria should set-up as many computer centers as possible in the local governments that are fitted with VSAT facilities to ensure reliable internet connectivity and instead of the traditional ballot system. Every Nigerians citizen can log on to his/her account on the e-Democracy system and vote. We also recommend that the government makes effort to improve the internet penetration in the nation so as to make the system accessible to the people. Some of the limitations of this study includes: Insufficient information resources available to us from the Nigerian government, Inadequate; and epileptic internet connectivity, and as a result access to online resources was strained.

## 5. CONCLUSION AND FURTHER RESEARCH

This study has led to the development of an e-Democracy system, achieving the basic objective of making available to all the participants in the democracy system the fundamental tools and resources that are required to adequately perform their individual roles in the running of the democratic state.

The citizens of the nation can communicate freely with elected government executives and political office holders through e-mails; they also have access to updated information on happenings in the government; can express their views on issues ranging from policy generation and execution to national development through a multi-dynamic forum; can engage in brainstorming sessions with other citizens online through a chat functionality; and some other functionalities that basically establish the individual as a relevant participant in the democracy of the nation. As regards the election module, voting at local government and House of Representative levels may be included in further research.

Another major enhancement that will be added to this research is to develop a speech-based e-Democracy module that allows users to access the system through telephone (mobile and land phones), as well as web interface. The inclusion of SMS-based module using the SMS-based e-participation framework (Ayo et al, 2010) is also considered as future works in this research.

As part of further works, the E-Democracy system can also be modified to be implemented on the mobile platform. This will increase the accessibility of the system as mobile phone use is wide spread in Nigeria today. A multi-lingual system can be developed to help people with English deficiency have access to the system. An advanced search module can be implemented on the system to enable users search for information about anything that pertains to Nigeria and Nigerian government.

## REFERENCES

Adeyemo A. B. (2011), "E-government Implementation in Nigeria: An assessment of Nigeria's global e-gov ranking", Journal of internet and information system Vol. 2(1), pp. 11-19, January 2011. Available online at http://www.academicjournals.org/JIIS

ISSN 1684–5315 ©2011 Academic Journals

Ayo C. K, Azeta A. A, and Oluwabusola O.G. (2010): "An SMS-based Framework for Citizen-Oriented Participation in e-Democracy", Proceedings of the 15th International Business Information Management Association Conference, November 6 - 7, 2010, Cairo, Egypt, pp1234-1238. ISBN: 978-0-9821489-4-5.

Briony, O. (2003): "The potential contribution of ICTs to the political process", The Electronic Journal of e-Government, Volume 1 Issue 1 / Mar 2003 . pp31 39

Caldow, J. (2004), "E-Democracy: putting down global roots, Institute for Electronic

Government, IBM. Retrieved 26 January 2013 from http://www01.ibm.com/industries/government/ieg/pdf/

e-democracy%20putting%20down%20roots.pdf

Flavio, C. (2005): "E-democracy: A solution for disadvantages territories". 5th European

Conference on E-Government, Remenyl D., editor., Antwerp (Belgium), 2005/06/16-17,

Academic Conferences Limited (UK), 101-109.http://www.cs.unicam.it/docenti/flavio.corradini/Lists/Pubblications/DispForm.aspx?ID =63

Kamar N, & Ongondo, M (2007). Impact of e-Government on Management and use of

Government Information in Kenya, World Library and Information Congress: 73rd IFLA general Confernce and Council, pp. 19-23 August 2007, Durban, South Africa

Godwin O. & Amobi P. C. (2012), " E-Governance and Public Administration in Nigeria: A Discourse ", "International Journal of Business and Management Tomorrow, Vol 2 Number 9. Published by SPIRI

Oates, B.(2003), "The potential contribution of ICTs to the political process" Electronic Journal of e-Government Volume 1 Issue 1, 2003, (pp31-39), available online at www.ejeg.com

OECD ( 2003): "Promise and problems of e-democracy. Challenges of online citizen

engagement", Organisation For Economic Co-Operation and Development.

http://www.oecd.org/governance/public-innovation/35176328.pdf

Full Paper

# ON IMAGE QUALITY ASSESSMENT USING STRUCTURAL SIMILARITY INDEX (SSIM)

**O. R. Vincent**
Department of Computer Science,
Federal University of Agriculture, P. M. B. 2240 Abeokuta, Nigeria
vincent.rebecca@gmail.com

**O. K. Adepoju**
Department of Computer Science,
Federal University of Agriculture, P. M. B. 2240 Abeokuta, Nigeria.
adepojukunle@gmail.com

**ABSTRACT**

Measurement of image quality is important for many image processing applications. Image quality assessment is closely related to image similarity assessment in which quality assessment is based on the differences or similarity between a lossy compressed image and the original image (uncompressed image). In this project a full- reference image quality assessment metric called structural similarity index metric (SSIM) was studied and is very useful in various image processing applications. This index (SSIM) models any kind of image distortion as a combination of three factors which are luminance distortion, contrast distortion and structural distortion. PSNR and MSE are the regular methods used for image quality assessment. This works shows that SSIM Index is a better alternate for effective quality assessment. In this work, SSIM was used to assess the image quality and the decision is better than the traditional error summation methods such as mean squared error (MSE) and peak signal to noise ratio (PSNR). This image quality assessment approach does not depend on the type or size of the testing image. It is also independent on pixel size of the testing image (original image).

**Keywords:** *Image Quality Assessment, MSE, PSNR, SSIM and*

## 1. INTRODUCTION

The field of image processing generally deals with signals that are meant for human consumption. An image may go through many stages of processing before being presented to a human observer and each stage of processing may introduce distortions that could reduce the quality of the final display. Images are acquired by camera devices that may introduce distortions due to optics, sensor noise, color calibration, exposure control, camera motion etc. (Soundararajan and Bovik, 2012). After acquisition, the image may be processed further by a compression technique that reduces the bandwidth requirements for storage or transmission. Such compression techniques are generally designed to achieve greater savings in bandwidth by allowing certain distortions happen to the signal. The compression techniques may be lossy or lossless, in lossless techniques there is no loss of information but in lossy compression technique there is degradation in the image quality during quantization process. (Ancibas, 2008). Similarly, bit errors which occur while an image is being transmitted over a channel or when it is stored, also tend to introduce distortions. Therefore one is obviously interested in being able to measure the quality of an image and to determine the distortion that has been added to it during the capturing period and the different processing stages. However the two major ways of assessing image quality are subjective assessment and objective assessment.

The subjective way of determining the quality of an image is to solicit opinion from human observers while Objective way of assessing the quality of an image is based on automatic and mathematical defined algorithms that could analyze the images and report their quality without human involvement (Pedersen, 2010). However, subjective evaluations are expensive and time-consuming, therefore objective assessment method has attracted more attentions since the methods could eliminate the need for expensive subjective studies. (Chaofeng, 2011).

The well-known objective evaluation algorithms for assessing image quality include mean squared error (MSE) and peak signal-to-noise ratio (PSNR). These are appealing because they are simple to calculate, have clear physical meanings, mathematically convenient and very fast and easy to implement. But MSE and PSNR lack a critical feature: the ability to assess image similarity across distortion types (Mittal et al, 2013; wang and Bovik, 2002). They are acceptable image assessment measures when the images in question differ by simply increasing distortion of a certain type. These assessment measures are failed to capture image quality when they are used to measure across distortion types (Vayssel et al, 2005). Therefore, this project proposes a Modified Structural Similarity Index Metric (SSIM) algorithm to assess the quality of image.

Image quality assessment plays a fundamental role in the design and evaluation of imaging and image processing systems. The goal of image compression algorithms is to reduce the amount of data required to store an image and at the same time, ensure that the resulting image is of sufficiently high quality (Simoncelli et al, 2003. Image enhancement and restoration algorithms attempt to generate an image that is of better visual quality from a degraded image. Quality assessment algorithms are also useful in the design of image acquisition systems and to evaluate display devices. Communication networks have developed tremendously over the past decade and images are frequently transported over optic fiber, packet switched networks like the Internet, wireless systems etc. Bandwidth efficiency of applications such as video conferencing and Video on Demand (VOD) can be improved using quality assessment systems to evaluate the effects of channel errors on the transported images (Wang et al, 2004).

## 2. RELATED MODELS

Image quality is a characteristic of images that measures the perceived image degradation (Li et al, 2011). It plays an important role in various image processing applications and the primary goal of image quality assessment is to supply the quality metrics that can predict perceived image quality automatically. Types of image quality assessment are subjective quality assessment and objective quality assessment.

Subjective image quality is concerned with how image is perceived by a viewer and gives his or her opinion on a particular image. An obvious problem that arises is that assessment criterion may vary from person to person. What one person sees as marginal, another may view as passable. In subjective quality measure the distorted image quality is specified by the Mean Opinion Score (MOS) which is the result of perception based on subjective evaluation. The MOS is generated by averaging the result of a set of standard subjective tests and it serves as an indicator of the perceived image quality. The 5-level grading scales of MOS implies 5-pleasant or excellent quality, 4-good, 3-acceptable, 2-poor quality and 1-unacceptable. The Mean Option Score is defined as:

$$\frac{?}{?}\sum_{?? ?}^{?}\mathrm{ip} \qquad (1)$$

where i = image score; p(i)=image score probability and S = number of observer. However, subjective quality measure is usually inconvenient, time-consuming and expensive. Therefore an objective quality measure that will eliminate the need for expensive subjective studies is needed.

Objective Quality Measures are mathematical algorithms and models for image quality assessment that could analyze images and report their quality without human involvement. These methods could eliminate the need for expensive subjective studies. (Narwarn and Lin, 2010). The objective quality measure plays variety of roles which include the following:

1. To monitor and control image quality for quality control systems
2. To benchmark image processing systems;
3. To optimize algorithms and parameters;
4. To help home users better manage their digital photos and evaluate their expertise in photographing. (Chen et al, 2010)

### 2.1. Classification of Objective Image Quality Measure

Objective image quality measure is classified according to the availability of an original image (distortion-free) with which distorted image is to be compared.

Full- reference (FR)
No- reference (NR)
Reduced- reference (RR)

1. Full-reference: This implies that a complete reference image is assumed to be known and the perfect version of the image (reference image) is being compared with the distorted version of the image. The most widely used full-reference image quality metrics during last 20 years are Mean Square Error (MSE) and Peak to Signal Noise Ratio (PSNR). Moreover Structural Similarity Index (SSIM) a new full reference image quality assessment metric suggested in 2004 shows better results than MSE and PSNR with reasonable computational complexity increasing. (Okarma, 2009).
2. No-reference: The quality assessment algorithm has access only to the distorted image signal and the quality of the signal is being assessed without any knowledge of the reference image. In many practical applications where the reference image is not available a no-reference quality assessment approach is desirable.
3. Reduced-reference: Reduced Reference Quality Assessment algorithms use the partial reference image information to assess the quality of the distorted image. The reference image is only partially available, in the form of a set of extracted features made available as side information to help the quality evaluation of the distorted image.

#### *2.1.1. Full-reference Image Quality Assessment Metrics*

1. Mean Squared Error (MSE)
   This full-reference image quality assessment metric involves computing an error signal by subtracting the test signal from the reference, and then computing the average energy of the error signal. The mean-squared-error (MSE) is the simplest and the most widely used full-reference image quality measurement (Bovik et al, 2004). This metric is frequently used in signal processing and is defined as follows:

$$\mathrm{MSE} = \frac{?}{?\ ?}\sum_{?? ?}^{?}\sum_{?? ?}^{?}(x?i,j?-\ y?i,j?)^{2}$$

From equation 2.2, x (i, j) represents the original (reference) image and y (i, j) represents the distorted (modified) image and M and N are the width and height of an image's is zero when x (i, j) = y (i, j) .

Property of MSE

- If the MSE decrease to zero, the pixel-by-pixel matching of the images becomes perfect.
- If MSE is small enough, this corresponds to a high quality decompressed image.
- MSE value increases as the compression ratio increases.

2. Peak Signal to Noise Ratio (PSNR)
The PSNR is evaluated in decibels and is inversely proportional the Mean Squared Error. It is given by the equation:

$$\mathrm{PSNR} = 10\log_{\text{⍰⍰}}\frac{\text{⍰}^{\text{⍰}}}{\sqrt{\text{⍰ ⍰⍰}}}$$

From equation 2.3, L is the dynamic range of the pixel values

Property of PSNR

- Higher PSNR value correlate to a higher image quality
- PSNR value decreases as the compression ratio increases.

### 2.3. Related Works

Chen and Bovik presented a paper on the design of real-time implementable full-reference image quality algorithms based on the SSIM index and multi-scale SSIM (MS-SSIM) index . The algorithms, which modify SSIM/MS-SSIM to achieve speed, are tested on the LIVE image quality database and shown to yield performance commensurate with SSIM and MS-SSIM but with much lower computational complexity. The algorithm achieves real-time performance with simple optimization (Chen and Bovik, 2010).

Another research suggested that a single strategy may not be sufficient; rather, we advocate that the HVS uses multiple strategies to determine image quality. For images containing near-threshold distortions, the image is most apparent, and thus the HVS attempts to look past the image and look for the distortions. For images containing clearly visible distortions, the distortions are most apparent, and thus the HVS attempts to look past the distortion and look for the image's subject matter. Here, we present a quality assessment method [most apparent distortion (MAD)], which attempts to explicitly model these two separate strategies. Local luminance and contrast masking are used to estimate detection based perceived distortion in high-quality images, whereas changes in the local statistics of spatial-frequency components are used to estimate appearance-based perceived distortion in low-quality images. We show that a combination of these two measures can perform well in predicting subjective ratings of image quality (Larson and Chandler, 2010).

Sakuldee, and Udomhunsakul proposed an objective image quality assessment to measure the quality of gray scale compressed image, which is correlation well with subjective quality measurement (MOS) and least time taken. The new objective image quality measurement is developed from a few fundamental of objective measurements to evaluate the compressed image quality based on JPEG and JPEG2000. The reliability between each fundamental objective measurement and subjective measurement (MOS) is found. From the experimental results, we found that the Maximum Difference measurement (MD) and a new proposed measurement, Structural Content Laplacian Mean Square Error (SCLMSE), are the suitable measurements that can be used to evaluate the quality of JPEG200 and JPEG compressed image, respectively. In addition, MD and SCLMSE measurements are scaled to make them equivalent to MOS, given the rate of compressed image quality from 1 to 5 which means from unacceptable to excellent quality (Sakuldee, and Udomhunsakul, 2007).

## 3. SSIM INDEX DESIGN

SSIM Index is introduced for assessing quality of JPEG compressed image. Though, MSE and PSNR are the common methods used everywhere, experiments conducted shows that SSIM Index can be used as a better and effective alternate. The system uses a PNG format image as reference image which is converted to a JPEG format (a lossy compression technique). The JPEG image format is used as the compressed image. The two images are used for calculating SSIM index. SSIM Index is calculated for compressed images with different compression ratio. PSNR of the compressed images also calculated.

The SSIM algorithm assesses three terms between two non-negative image signals x and y: the luminance l(x, y), contrast c(x, y), and structure s(x, y). Therefore to complete the definition of the structural similarity measure we need to define the following three functions l(x, y), c(x, y) and s(x, y), as well as their combination function. In addition, the similarity measure must satisfy the following conditions:

1. Symmetry: S(x, y) = S(y, x). When quantifying the similarity between two signals, exchanging the order of the input signals should not affect the resulting measurement.
2. Boundedness: S(x, y) ≤1. An upper bound can serve as an indication of how close the two signals are to being perfectly identical. Other algorithms like signal-to noise ratio type of measurements are typically unbounded.
3. Unique maximum: S(x, y) = 1 if and only if x = y. The perfect score is achieved only when the signals being compared are identical. In other words, the similarity measure should quantify any variations that may exist between the input signals.

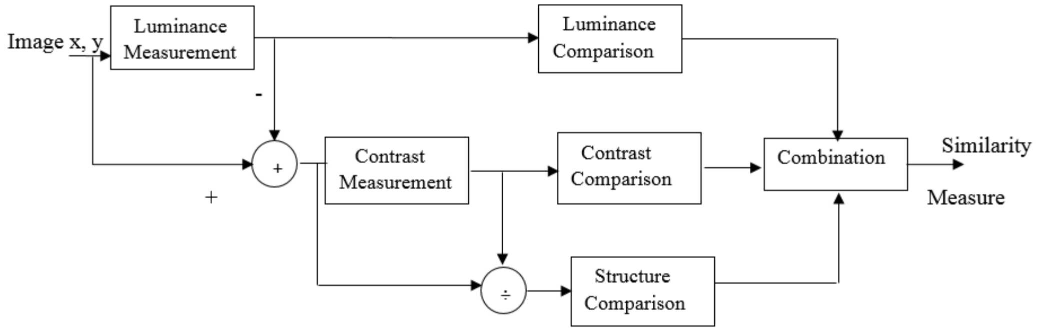


*Figure 2: The Structural Similarity Measurement System*

Let X represents the reference image sample, while Y represent the lossy compressed image sample and N = NxM array for simplicity.

The system separates the task of similarity measurement into three comparisons: luminance, contrast and structure. This is reflected in figure 2.

### 3.1. Luminance measurement and Comparison

The first step is to measure the luminance of x and y, which is understood as the average luminance value of all pixels in an image and respectively indicated as µx and µy:

$$\mu_x = \frac{1}{N}\sum_{i=1}^{N} x_i$$

$$\mu_y = \frac{1}{N}\sum_{i=1}^{N} y_i$$

Then, the function for the comparison of the luminance, l(x,y), is defined as follows:

$$l(x,y) = \frac{2\mu_x\mu_y + C_1}{\mu_x^2 + \mu_y^2 + C_1}$$

Where $C_1 = (K_1L)^2$, with $K_1$ is an arbitrary constant (<< 1) usually set to 0.01 and L is equal to the maximum possible pixel value of the image. So, if *8* bits per pixel is used, *$L = 2^8 - 1 = 255$*.

### 3.2. Contrast Measurement and comparison

$$\sigma_x = \left(\frac{1}{N-1}\sum_{i=1}^{N}(x_i - \mu_x)^2\right)^{1/2}$$

$$\sigma_y = \left(\frac{1}{N-1}\sum_{i=1}^{N}(y_i - \mu_y)^2\right)^{1/2}$$

Then, the contrasts are compared by using the following function:

$$C(x,y) = \frac{2\sigma_x\sigma_y + C_2}{\sigma_x^2 + \sigma_y^2 + C_2}$$

$C_2$ is a constant usually equal to $(K_2L)^2$, with $K_2$ << 1 and usually set to 0.03

### 3.3. Structure comparison

Thirdly the structure comparison function s(**x**,**y**) of the two image signals is calculated as:

$$S(x,y) = \frac{\sigma_{xy} + C_3}{\sigma_x\sigma_y + C_3}$$

With $C_3 = C_2/2$, and

$$\sigma_{xy} = \frac{1}{N-1}\sum_{i=1}^{N}(x_i - \mu_x)(y_i - \mu_y)$$

Finally, here is the SSIM Index:

$$\mathrm{SSIM}(x,y) = \frac{(2\mu_x\mu_y + C_1)(2\sigma_{xy} + C_2)}{(\mu_x^2 + \mu_y^2 + C_1)(\sigma_x^2 + \sigma_y^2 + C_2)}$$

It should be noted that as the index of structural similarity approaches 1, the greater the degree of fidelity of the compressed image is close to the original image.

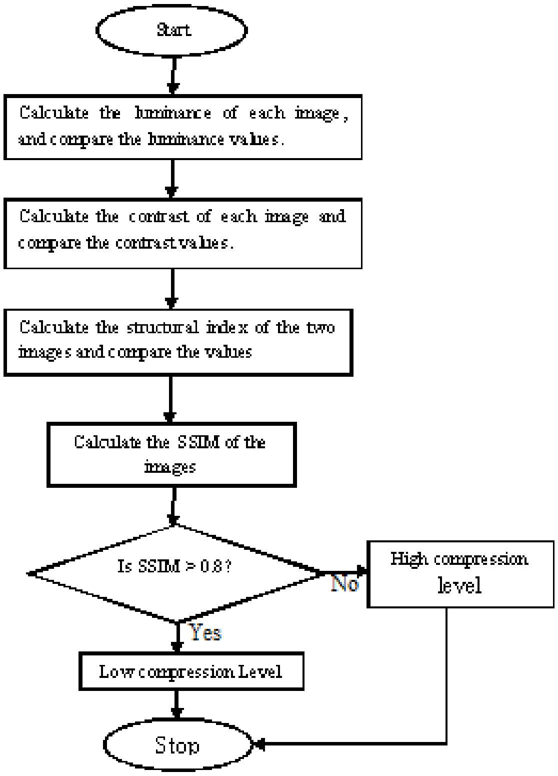

Start
Calculate the luminance of each image, and compare the luminance values.
Calculate the contrast of each image and compare the contrast values.
Calculate the structural index of the two images and compare the values
Calculate the SSIM of the images
Is SSIM > 0.8?
No
High compression level
Yes
Low compression Level
Stop

*Figure 4 : Chart for the Structural Similarity Index Metrics (SSIM)*

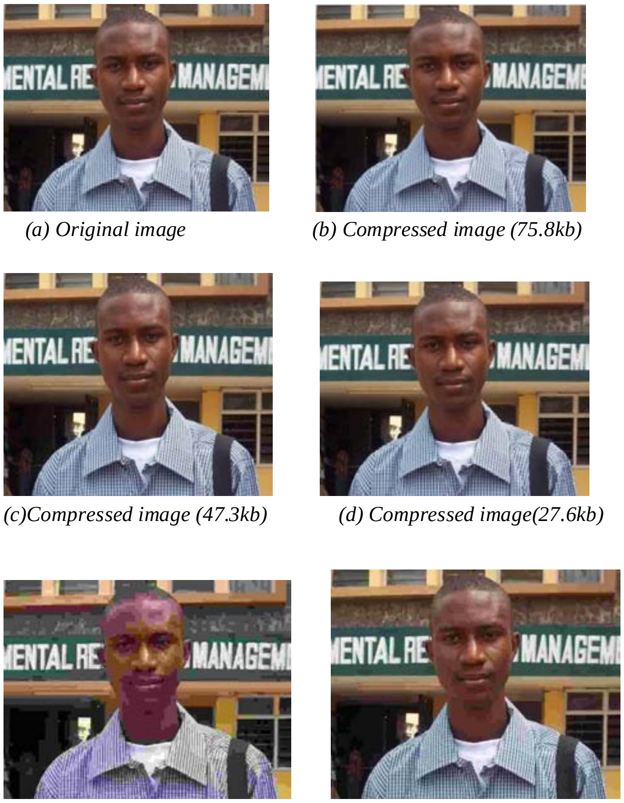
## 4. EXPERIMENTAL RESULTS AND DISCUSSION

The experiment was conducted using a single image with different compression ratio since the quality of image is affected more as the compression rate increases. The resolution of the reference image used is 716×550. The experiment was implemented in Microsoft visual C# 2010 express. The goal is to prove that the SSIM Index based quality measurement will provide a better result than PSNR for JPEG compressed image.

Figure 5 shows the original image and the compressed images used for the experiment. The SSIM Index and PSNR for all the compressed images mentioned here is found out. It is found that after certain compression level PSNR shows a sudden declination in the value whereas SSIM Index indicates a better degradation of image quality. The sudden declination in case of PSNR is because it is a measure of average error which is not consistent as the compression ratio increases. Table 1 Shows the SSIM Index value and PSNR value for each of the compressed image sample.

As shown in figure 5 where the original image is altered with a distortion (JPEG compression), the quality factor, compression ratio and SSIM values are related with one another. As quality factor increases, compression ratio decreases and SSIM value increases. As the value of structural similarity index approaches 1, the greater the degree of fidelity or similarity of the compressed image is close to the original image.

Table 2 shows the SSIM and PSNR values for the original image and the compressed image samples and it is found that after certain compression level PSNR shows a sudden declination in the value whereas SSIM Index indicate a better degradation of image quality. The sudden declination in case of PSNR is because it is a measure of average error which is not consistent as the compression ratio increases.



*(a) Original image* *(b) Compressed image (75.8kb)*

*(c)Compressed image (47.3kb)* *(d) Compressed image(27.6kb)*

*(e)Compressed image(18.3kb)* *(f) Compressed image(12.9kb)*

*Fig 5(a,b,c,d,e,f): Original image and Compressed image samples*

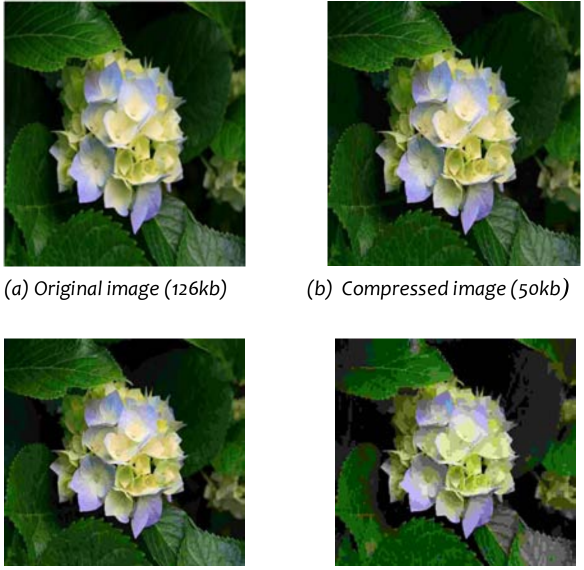
*Table 1: Value of SSIM and PSNR for different compressed image samples.*

| Compressed image size | SSIM | PSNR |
|---|---|---|
| 75.8 kb | 0.92067 | 50.4522 |
| 47.3kb | 0.90902 | 50.3221 |
| 27.6kb | 0.85223 | 50.0431 |
| 18.3kb | 0.80342 | 30.3423 |
| 12.9kb | 0.74322 | 10.3216 |

Table 2 shows the SSIM and PSNR values for the original flower image and the compressed flower image samples. The value of SSIM is increasing and gradually approaches 1 indicating how close the compressed image samples are to the original image as the compressed image size increases But there is sudden increase in the value of PSNR which may not indicate closeness of the compressed image samples to the original image.

## 5. CONCLUSION AND FUTURE WORK

Conclusively, Structural Similarity Index in image quality assessment is more efficient as it is more consistent with human eye observation. The boundedness property of Structural Similarity Index (S(x, y) ≤1) which serve as an indication of how close the two image signals are also enhance the effectiveness of SSIM in assessing image quality.



*(a) Original image (126kb)* *(b) Compressed image (50kb)*

*(c) Compressed image (20kb)* *(d) Further Compressed image (15kb)*

*Fig 6 (a, b,c,d): Original image and Compressed flower image samples*

Experimental results indicated that MSE and PSNR are very simple, easy to implement and have low computational complexities. But these metrics do not show good results since the results are not in close agreement with human judgments therefore MSE and PSNR are widely criticized for not consistent with subjective human evaluation. SSIM is a better alternative method for image quality assessment. It works accurately can measure better across distortion types as compared to MSE and PSNR and more consistence with the subjective human evaluation.

Due to the fact that there are many practical applications where the reference image is not available, a no-reference (blind) image quality assessment approach is desirable. Therefore, it is recommended that the future researcher in the field of image quality assessment also do further study on no-reference image quality assessment where an image signal is being assessed without any knowledge of the reference image.

## REFRENCES

Avcıbas A, Sankur B, and Sayood K, (2008), “Statistical evaluation of image quality measures,” Journal of Electronic Imaging, vol. 11, no. 2, pp. 206–223.

Bovik A.C, Wang Z and Lu L (2004),“Video quality assessment based on structural distortion measurement,” Signal Processing: Image Communication, special issue on video quality metrics, vol. 19, 1, 234-243.

Chaofeng li, Alan Bovik and Xiaojun Wu, 2011.’ Blind Image Quality Assessment Using a General Regression Neural Network’, IEEE Transactions on Neural Networks, 22, 5, 793-799.

Chen M. and Alan C. Bovik, 2010. ‘Fast Structural Similarity Index Algorithm’, ICASSP IEEE, 994-997.

Chen, M. J. and A.C. Bovik, “Fast structural similarity index algorithm, ”Journal of Real-Time Image Processing, Vol: 6 No: 4, Page(s): 281-287, December, 2011.

Damera-Venkata, N., T. D. Kite,W. S. Geisler, B. L. Evans, and A. C. Bovik, 2000. 'Image quality assessment based on a degradation model. IEEE Transactions on Image Processing, 9(4), 323-335.

Larson and Chandler, 2010. 'Most apparent distortion: full-reference image quality assessment and the role of strategy, Journal of Electronic Imaging 19(1), 011006-1-21.

Li, C., Alan Conrad Bovik, Xiaojun Wu, 2011. 'Blind Image Quality Assessment Using a General Regression Neural Network, IEEE Transactions on Neural Networks , 22, 5, 793-799.

Mittal, A. K. Moorthy and A. C., Bovik, 2012. "No-Reference Image Quality Assessment in the Spatial Domain,"IEEE Transactions on Image Processing, 254-261.

Mittal, A., R. Soundararajan and A. C. Bovik, 2013.'Making a Completely Blind Image Quality Analyzer, "IEEE Signal Processing Letters, 22,3,209-212.

Narwaria, M. and W. Lin, 2010. "Objective image quality assessment based on support vector regression," IEEE Trans. Neural Netw., vol. 21, no. 3, pp. 515–5190.

Okarma, K. 2009. 'Colour Image Quality Assessment Using Structural Similarity Index and Singular Value Decomposition', Lecture Notes in Computer Science Volume 5337, 2009, pp 55-65.

Pederson, M., Bonnier N., Hardeberg, J. and Albregtsen, F. (2010),' Attributes of image quality for color prints, Journal of electronic imaging, 19, 1, 011016-011016-13

Sakuldee, R. and Somkait Udomhunsakul, 2010. 'Objective Performance of Compressed Image Quality Assessments', World Academy of Science, Engineering and Technology 35, 154-163.

Sheikh, H. R., M. F. Sabir, and A. C. Bovik, 2006. "A statistical evaluation of recent full reference image quality assessment algorithms," IEEE Trans. Image Processing, vol. 15, no. 11, pp. 3440–3451

Simoncelli E. P, Wang Z, and Bovik A. C, 2003. 'Multiscale structural similarity for image quality assessment,' Proc. IEEE Asilomar Conf. Signals, Systems & Computers.

Soundararajan, R. and A. C. Bovik, 2012. "RRED Indices: Reduced Reference Entropic Differencing for Image Quality Assessment," IEEE Transactions on Image Processing, vol. 21, no. 2, pp. 517-526.

Vaysse1, P., G. Grenier, O. Lavialle, G. Henry, S. Khay-Ibbat, C. Germain and J.P. Da Costa, 2005. ' Image Processing as a tool for quality assessment of fruits in bulk shipping bins, Information and Technology for Sustainable Fruit and Vegetable Production, 381-388.

Wang, Z., Bovik A. C. Rao, P., 2004. 'Image quality assessment: From error visibility to structural similarity,' IEEE Trans. Image Processing, 13, 600–612.

Wang, Z. and A.C.Bovik, 2002. A Universal Image Quality Index, IEEE Signal processing Letters,Vol.9,pp. 81-84.

Full Paper

# SECURITY CHALLENGES AND VULNERABILITIES IN VANET AND THE PROPOSED COUNTERMEASURES

**A. A. Obiniyi**
Dept. of Mathematics,
Ahmadu Bello University, Zaria, Nigeria
aaobiniyi@gmail.com

**H. A. Sulaimon**
Dept. of Computer Science,
Federal College of Education, Zaria, Nigeria
sulaimha@yahoo.com

**ABSTRACT**

The networks that interconnect vehicles on road are called Vehicular Ad hoc Networks (VANETs). The main target of research in VANETs is the improvements of vehicle safety by means of inter vehicular communication (IVC). VANETs have several different aspects compared to mobile ad hoc networks (MANETs), in that the nodes move with high velocity because of which the topology changes rapidly. However, VANETs pose many challenges on technology, protocols and security which increase the need for research in this field. Vehicular Ad hoc Networks are prone to several vulnerabilities and attacks which cause severe problems in the network and also facade some potential security threats which can deteriorate their functioning. Therefore, the security of VANETs is indispensable. Hence, some constraints such as validating all VANETs entities simultaneously by all nodes and strict coordination amid entities are necessary for detection of a Sybil attack among others. This paper discusses some security challenges in vehicular ad hoc networks and proposes some measures that can overcome such vulnerabilities and security challenges.

**Keywords:** *Vulnerabilities, Security Challenges, Security Threats,*

## 1. INTRODUCTION

The main goal of Vehicular Ad Hoc Networks (VANETs) is to increase road safety for the drivers and provides comfort to the passengers by the use of wireless communications. In the near future, it can be expected that vehicles will be equipped with wireless communication devices, which will enable the formation of VANETs. Vehicle to Infrastructure provides solution to longer-range vehicular networks. It makes use of preexisting network infrastructure such as wireless access points (Road-Side Units, (RSUs)). Communications between vehicles and RSUs are supported by Vehicle-to-Infrastructure (V2I) protocol and Vehicle-to-Roadside (V2R) protocol. A VANET is a wireless network that does not rely on any central administration for providing communication among the On Board Units (OBUs) in nearby vehicles, and between OBUs and nearby fixed infrastructure usually named Road Side Unit (RSU)(Caballero-Gill, 2010). In this way, VANETs combine Vehicle TO Vehicle (V2V) also known as Inter-Vehicle Communication (IVC) with Vehicle TO Infrastructure/Roadside (V2I/V2R) and Infrastructure TO Vehicle (I2V) communications (Figure 1).

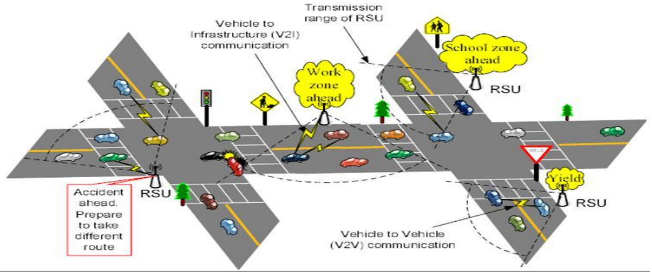

Vehicle to Infrastructure (V2I) communication
Transmission range of RSU
Work zone ahead
School zone ahead
RSU
Yield
RSU
Accident ahead. Prepare to take different route
RSU
Vehicle to Vehicle (V2V) communication

*Figure 1: V2V, V2I/V2R & I2V Communications.*

More so, OBUs in vehicles will broadcast periodic messages with the information about their position, time, direction and speed, and also warnings in case of emergency. RSUs on the roads will broadcast traffic related messages. Additional communications can be also useful depending on the specific application. Among all these messages, routine traffic-related will be one hop broadcast, while emergency warnings will be transmitted through a multi hop path where the receiver of each warning will continue broadcasting it to other vehicles. In this way, drivers are expected to get a better awareness of their driving environment so that in case of an abnormal situation they will be able to take early action in order to avoid any possible damage or to follow a better route. These applications include safety applications that will make driver safer, mobile commerce, roadside services that can intelligently inform drivers about congestion, businesses, and services in the vicinity of the vehicle" (Wong et al, 2006). "VANETs, especially compared to MANETs are characterized by several unique aspects.

Node moves with high velocity, resulting in high rates of topology changes (Leinmuller et al, 2006). For the reason of rapidly changing topology due to vehicle motion, the vehicular network closely resembles an ad hoc network however; the constraints and optimizations are remarkably different. VANETs have several different aspects compared to MANETs, in that the nodes move with high velocity because of which the topology changes rapidly (Wong et al, 2006).VANETs is also prone to several different attacks. Therefore, the security of VANETs is indispensable. VANETs pose many challenges on technology, protocols, security which increase the need for research in this field (Eichler et al, 2006). From the network perspective, security and scalability are two significant challenges (Wong et al, 2006). A formidable set of abuses and attacks become possible. Hence, security of vehicular network is indispensable (Raya et al, 2006). Meanwhile the growing importance of inter-vehicular communications (IVC) has been recognized by the government, corporations, and the academic community.

The CAR2CAR communication Consortium (C2C-CC), a non-profit organization initiated by European vehicle manufacturers with the objective of improving road traffic safety and efficiency published in 2007 a manifesto in which it proposes standards for V2V and V2I communications among other things. In 2008, The European Union deployed systems relying on V2V and V2I communications by reserving a radio frequency across the EU for vehicle applications aiming at enabling co-operative systems between carmakers.

This paper is organized in the following way, section 2 presents the security issues inherent in VANETs which gives an insight into the vulnerabilities of vehicular ad hoc networks. It also describes the false position information problem and also presents an overview of the Sybil attacks in VANETs. Section 3 discusses the proposed countermeasure to security problems in VANETs detection and how to prevent Sybil attacks in VANETs. It introduces the proposed solutions to false position information while section 4 concludes the paper.

## 2. SECURITY CHALLENGES AND VULNERABILITIES OF VANETS

The issues on VANET security become more challenging due to the unique features of the network, such as high-speed mobility of network entity or vehicle, and extremely large amount of network entities. Vehicular ad hoc networks are also prone to several vulnerabilities and attacks. These vulnerabilities can cause small to severe problems in the network and also poses some potential security threats which can deteriorate their functioning.

### 2.1. Vehicular Communications vulnerabilities of VANETs

The following section gives a general overview of Vehicular Communications vulnerabilities of VANET;

1. A. Jamming: The jammer deliberately generates interfering transmissions that prevent communication within their reception range. In the VANET scenario, an attacker can relatively easily partition the vehicular network, without compromising cryptographic mechanisms and with limited transmission power (Qian and Moayer, 2008).
2. B. Forgery: The correctness and timely receipt of application data is major vulnerability. The attacker forges and transmits false hazard warnings which are taken up by all vehicles.
3. C. Impersonation: Message fabrication, alteration, and replay can also be used towards impersonation. For example, an attacker can masquerade as an emergency vehicle to mislead other vehicles to slow down and yield. If a vehicle's owner deliberately steals another vehicle's identity and still claimed ownership, is also an act of impersonation.
4. D. Privacy: The inferences on driver's personal data could be made, and thus violating his or her privacy. Driver privacy is an important issue in vehicular communications. Drivers don't want their personal and private information to be accessible to others. Since the vehicle information such as location, speed, time and other car data are transmitted via wireless communication, it should not be made possible to infer the driver's identity from this information. Among this information, driver's location and tracing vehicle movements are more sensitive and must be taken into consideration carefully (Leinmüller et al, 2007).
5. E. In-transit Traffic Tampering: A node acting as a relay can disrupt communications of other nodes. It can drop or corrupt messages, or meaningfully modify messages. Attackers can also replay messages, for example, to illegitimately obtain services such as traversing a toll check point. Tampering with in-transit messages may be simpler and more powerful than forgery attacks (Qian and Moayer, 2008).
6. F. Authentication: Without authentication, illegitimate and malicious users can inject false messages into the network and confuse other vehicles by distributing false information. With authentication, vehicles can simply drop messages from unauthenticated users. Authentication and the inherent integrity property counter the in-transit traffic tampering and impersonation vulnerabilities

### 2.2. Sybil Attacks in VANETs

In this attack, a vehicle forges the identities of multiple vehicles. These identities can be used to play any type of attack in the system. These false identities also create an illusion that there are additional vehicles on the road. Consequence of this attack is that every type of attack can be played after spoofing the positions or identities of other nodes in the network. Since periodic safety messages (like beacon message) are single hop broadcasts, the focus has been mostly on securing the application layer. However, when the network operation is not secured, an attacker can potentially partition the network and make delivery of event-driven safety messages impossible.

#### *2.2.1. Global Positioning System (GPS) Spoofing*

The GPS satellite maintains a location table with the geographic location and identity of all vehicles on the network. An attacker can fool vehicles into thinking that they are in a different location by producing false readings in the GPS positioning system devices. This is possible through the use of a GPS satellite simulator to generate signals that are stronger than those generated by the genuine satellite.

*2.2.2. Position Faking*

Authentic and accurate reporting of vehicle position information must be ensured. Vehicles are solely responsible for providing their location information and impersonation must be impossible. Unsecured communication can allow attackers to modify or falsify their own position information to other vehicles, create additional vehicle identifiers (also known as Sybil Attack) or block vehicles from receiving vital safety messages.

*2.2.3. Tamper-proof device*

The use of secret information such as private keys incurs the need for a Tamper-Proof Device (TPD) in each vehicle (Raya and Hubaux, 2007). In addition to storing the secret information, this device will be also responsible for signing outgoing messages. To reduce the risk of its compromise by attackers, the device should have its own battery, which can be recharged from the vehicle, and clock, which can be securely resynchronized, when passing by a trusted roadside base station. The access to this device should be restricted to authorized people. For example, cryptographic keys can be renewed at the periodic technical checkup of the vehicle. As its name implies, the TPD contains a set of sensors that can detect hardware tampering and erase all the stored keys to prevent them from being compromised. The availability of this feature makes the TPD on one hand too sensitive for VANET conditions (for example, the device can be subject to light shocks because of road imperfections; TPDs also cannot tolerate extreme temperatures that may not be unusual for vehicles) and on the other hand too expensive for non-business consumers. In fact, current commercial products such as the IBM 4758 card which contains cryptographic coprocessors is oriented towards financial applications and cost several thousands of dollars.

### 2.6. Cryptographic Techniques

Cryptography is the study of the design of techniques for ensuring the secrecy and/or authentication of information. The following cryptographic techniques are examined;

a) Symmetric key algorithms,
b) Asymmetric key algorithms.

*2.6.1. Symmetric Key Algorithms:*

In symmetric key cryptography, the entities that communicate securely have access to a secret data known as a key. This key is used to encrypt the data at the source and the same key is used to decrypt the data at the receiver of the message. The exchange of messages takes place using 2 functions E(•, •) and D(•, •) to encrypt and decrypt the message, having the property EM = E(K,M) and M = D(K,EM), where K is the key used to secure the message M. EM is the message that is transmitted by the source and received by the intended and unintended recipients of the message.

*2.6.2 Asymmetric Key Algorithms:*

In asymmetric key cryptography, each principal that is a source of a message has a pair of keys: Private Key, Public Key. The private key is known only to the principal, whereas the public key can be shared with all the entities in the system without jeopardizing the security of the private key. The keys can be visualized as a pair of functions Pr(•) and Pu(•) representing the private and public keys respectively, having the property M = Pr(Pu(M)) and M = Pu(Pr(M)), where M is the message that is to be secured using the keys

## 3. PROPOSED COUNTERMEASURE APPROACHES

In literature, different techniques are proposed for detection of Sybil attack in VANETs. Sybil attacks are always possible in the absence of any logical centralized authority. As there is no centralized entity in VANETs, detection of Sybil attacks is very difficult. Some constraints such as validating all entities simultaneously by all nodes and strict coordination among entities are necessary for detection of a Sybil attack. The following approach of verifying nodes position is taken from (Xio et al, 2006) in which Sybil attacks are considered to be one of the biggest threats to VANETs security. These attacks are believed to impair VANET safety applications thereby creating an illusion of traffic congestion. To overcome the above security threat a scheme called basic signal strength based position verification has been proposed to verify position claims based on signal strength of beacons. This technique takes full advantage of inherent properties of VANETS such as mobility, traffic pattern and also road side base stations. Position verification relies on monitoring the signal strength of periodical beacons. The following roles are played by each node according to (Ertaul and Mullapudi, 2007) each node periodically broadcasts a beacon message at beacon intervals, for the purpose of neighbor discovery.

The beacon message can be in the following format:

{ NodeID, B#, Pos, NList, Sigt }

Where NodeID is the claimer's identity, B# is a beacon sequence number, Pos is the sender claimed position, and Nlist is the neighbour list. Then neighbour list contains the following information.

NList: {NodeIDi, B#i, RSSi}

NList is the sender's most recent neighbor list containing signal strength measurements. Sigt is the digital signature for the whole packet.

In each item of NList, RSSi is the Received Signal Strength of beacon Bi, recently received from neighboring node NodeIDi.

The neighboring nodes residing within the signal range of the claimer, receives the previous beacon. The signal strength and corresponding neighbor information can be measured in their memory. It includes this neighbor information along with the signal strength when broadcasting a beacon message in another time. The node waits for a specific time interval tv after receiving a beacon message during which it collects signal strength measurements for the previous beacon from neighboring observers. Based on the collected measurements it can compute the position of the claimer. For example by performing Minimum Mean Square Error (MMSE)

To obtain the estimated position, the least square error (LSE) is first calculated, the least squares method minimizes the sum of squared residuals (also called the sum of squared errors, SSE). A residual is defined as the difference between the actual value of the dependent variable and the value predicted by the model (http://en.wikipedia.org/wiki/index.php?title= least-squares & Oldid=547861529).

$$LSE\ (P) = \sum_{i=0}^{n} (Zr(Ob\ ) - Zs(Ob,P))^2$$

Then the mean square error (p) will become

$$\mathrm{MSE}\ (\mathrm{p}) = \frac{\mathrm{LSE}\ (p)}{N}$$

$$MSE(P) = \sum_{i=0}^{n} \frac{(Zr(Ob\ ) - Zs(Ob,P))^2}{N}$$

Where p is the potential position of the claimer, N is the number of Observers. Zr is the received signal strength at Observers Ob. Zs is the calculated signal strength at Ob obtained from radio propagation model. By varying p, MSE can be minimized and finally get the optimized estimated position p. If the estimated position of claimer is far away from its claimed position, the node can be regarded as suspect node.

The security requirements of the vehicle authentication can be achieved by using digital signature. To implement digital signatures, asymmetric cryptography scheme is required, in which each vehicle has a certified public/private key pair. In asymmetric cryptography schemes, a vehicle uses its unique private key for generating a unique digital signature for every outgoing message. When a signed message is received, the recipient uses the public key of the sender to verify the digital signature of the sender on the message. Successful digital signature verification implies that the content of the message is not altered, and the sender is the only one who can generate this message, that is, achieving data authentication and non-repudiation. To achieve vehicle authentication, the public key of each vehicle must be authentic and all the vehicles in the network should be able to validate its authenticity. To adequately secure VANETs, each vehicle requires Public Key Infrastructure (PKI), where authentic certificate generated by a trusted Certification Authority (CA) is required. Figure 2 shows the fundamental elements in an authentic certificate cert$_i$ generated by a CA for a vehicle i, where ID$_i$ is the identity of vehicle i, PK$_i$ is the public key of vehicle i, T$_i$ is the validity period of the certificate cert$_i$, and sig$_{CA}$(ID$_i$|PK$_i$|T$_i$) is the signature of the CA, using the CA private key PK$_{CA}$, on the concatenation(ID$_i$|PK$_i$|T$_i$).

$$\mathbf{cert_i = (ID_i;\ PK_i;\ T_i;\ sig_{CA}(ID_i|PK_i|T_i))}$$

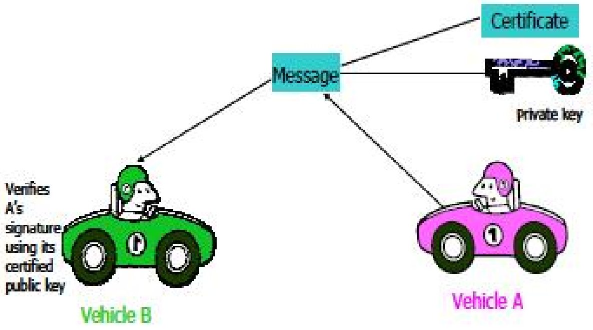


*Figure 2: Authentication*

Any vehicle can verify the certificate cert$_i$ by verifying the signature sig$_{CA}$(ID$_i$|PK$_i$|T$_i$) using the certified public key PK$_{CA}$ of the CA, which is known to all the vehicles in the network. The purpose of the certificates generated by the CA is to bind the identity of the certificate holder to its public key in an authentic way. A Vehicle I can send the following message

$$\mathbf{I \longrightarrow (ID_i;\ PK_i;\ T_i;\ sig_{CA}\ (ID_i|PK_i|T_i)),\ cert_i}$$

and by the time the other vehicle receives it, it has to extract and verify the public key of the vehicle I using the certificate and then verify I's signature using its certified public key. In doing this, the receiver should have the public key of CA.

Certificate Revocation: The most common way to revoke certificates is the distribution of Certificate Revocation Lists (CRLs) that contain the most recently revoked certificates; CRLs are provided when infrastructure is available. The certificates of a detected attacker or malfunctioning device have to be revoked.

But there are several drawbacks to this approach.

1. CRLs can be very long due to the large number of vehicles and their high mobility.
2. the short lifetime of certificates still creates a vulnerability window.
3. the availability of an infrastructure will not be pervasive, especially in the first years of deployment.

To avoid the shortcomings in 1 to 3, there is a need for a set of efficient revocation protocols, namely Revocation Protocol of the Tamper-Proof Device (RTPD), Revocation protocol using Compressed Certificate Revocation Lists (RCCRL), and Distributed Revocation Protocol (DRP). In RTPD, once the CA has decided to revoke all the keys of a given vehicle T, it sends to it a revocation message encrypted with the vehicle's public key. After the message is received and decrypted by the TPD of the vehicle, the TPD erases all the keys and stops signing safety messages. Then it sends an acknowledgement (ACK) to the CA. All the communications between the CA and the vehicle take place in this case via base stations. In fact, the CA has to know the vehicle's location in order to select the base station through which it will send the revocation message. If it does not know the exact location, it retrieves the most recent location of the vehicle from a location database and defines a paging area with base stations covering these locations. Then it multicasts the revocation message to all these base stations. In the case when there are no recent location entries or the ACK is not received after a timeout, the CA broadcasts the revocation message, for example, via the low-speed FM radio on a nationwide scale or via satellite.

## 4. CONCLUSION

In this paper, some of the security threats to vehicular ad hoc networks focusing on the vulnerabilities such as false position information, Sybil attack problems and some of the proposed solutions to overcome these security threats are also presented. A set of revocation protocol are used to revoke the certificates of a detected attacker or malicious node. The Basic Signal Strength Based Position Verification approach significantly detects the Sybil nodes in the network. Based on the security issues discussed in this paper it is clear that the field of inter vehicular communications requires the design of robust and secured architecture in order to prevent the security problems.

## REFERENCES

Caballero-Gill P. 2010. Security Issues in Vehicular Ad hoc Networks. Retrieved on 25thDecember, 2012 from http;/www.Cdn .intechweb.org/pdfs/12879.pdf

Eichler S., Schroth C. and Eberspacher J. 2006. "Car-to-Car Communication," Institute of Media and Communication Management,SAP Research CEC, University of St. Gallen , Switzerland, p8

Ertaul L. and Mullapudi S. 2007. The Security Problems of Vehicular Ad Hoc Networks (VANETs) and Proposed Solutions in Securing their OperationsRetrieved on 25thDecember, 2012 from http;/www.mcs.csueastbay.edu/lertaul /VANETSCamReady.pdf

http://en.wikipedia.org/wiki/index.php?title= least-squares & Oldid=54786152. Retrieved on 10th June, 2013

Leinmuller T., Schoch E. and Kargl F. 2006. "Position Verfication Approaches for Vehicular Ad hoc Networks," IEEE Wireless Communications, Vol 13, no 5, October , pp.16-20.

Leinmüller, T. Schoch, E. and Maihöfer, C. 2007. "Security requirements and solution concepts in vehicular ad hoc networks," in Proceedings of the 4th Annual Conference on Wireless on Demand Network Systems and Services, pp. 84–91

Qian Y. and Moayer N. 2008. Design Secure and Application-Oriented VANETs. May 11, Retrieved on 21st December, 2012 from http:/www.antd.nist.gov/pubs/Yi-paper7.pdf

Raya M., Papadimitratos P. and Hubaux J.P.2006. EPFI, "Securing Vehicular Communications," IEEE Wireless Communications, Vol 13, no5, October, pp.8-13

Raya M. and Hubaux J.P.(2007).Securing vehicular ad hoc networks. Journal of Computer Security.Vol. 15 No 1, 39–68

Xio B., Yu B. and Gao C. 2006. "Detection and Localization of sybil nodes in VANETs," Proc.Wksp. Dependability issues in wirelessAd hoc Networks and Sensor Networks, pp. 1-8.

Wong K. D., Tepe K.E, Chen,W. and Gerla M. 2006. "Inter Vehicular Communications,"

IEEE Wireless Communications, Vol 13, no 5, October, pp.6.

Full Paper

# SMARESIM: AN IMPROVED MODEL OF E-VOTING SYSTEM BASED ON BIOMETRIC ENCRYPTION

**M. C. Ndinechi**
Electronics Development Institute, Awka.
National Agency for Science and Engineering Infrastructure
mikez4god@yahoo.com

**V. C. Ossai**
Electronics Development Institute, Awka.
National Agency for Science and Engineering Infrastructure
arissyncline@yahoo.com

**K. C. Okafor***
Electronics Development Institute, Awka.
National Agency for Science and Engineering Infrastructure
vikossai2@yahoo.com

**C.C Udeze**
Electronics Development Institute, Awka.
National Agency for Science and Engineering Infrastructure

**H. C. Inyama**
Nnamdi Azikiwe University, Awka,

## ABSTRACT

The adoption of e-governance strategy in electioneering processes (using Nigeria context- 36 states) will effectively reduce cost as well as enhance election activities. What makes an e-voting model acceptable is its ability to properly authenticate voters and provide a secure means through which a voter can express his/her franchise. This paper therefore, proposes Self-Monitoring Analysis and Reporting E-Voting Simulation Model (SMARESiM), a design model of an e-voting system leveraging on Biometric Encryption (BE) viz Biometric key Binding (BKB) which is a secured strategy that entails fusing of biometrics with cryptographic schemes.The main objective of this research is to improve on the already existing E-voting models by fusing and adopting bio-cryptographic techniques as well as using a secure transmission channel for confidential datasets of a voting process.This work develops a simulation model of an E-voting system which adopts relevant algorithms and mathematical equations with emphasis on biometric security schemes. The simulation of a prototype model of the electronic voting system is developed using Proteus 7.6 application software.

The prototype model would consist of electronic kiosk polling booths (two e-booths) that are all networked to the state electoral collection center and two state collection centers (in this model) are networked to the national electoral collection center via a VPN backbone. The proposed SMARESiM uses a Virtual Private Network (VPN) as the means of communication between the various polling booths and collection points. The results of validation show that the proposed model facilitates the adoption of E-governance in the developing countries.

**KEYWORDS:** *Biometric Encryption, Cryptography, E-voting Booths, Privacy, Security.*

## 1. INTRODUCTION

Election is a process by which members of an organization or a society select people to hold offices of authorities (Shane, P., 2004).

The term "e-voting" encompasses all voting techniques involving electronic voting equipment including voting over the internet, using booths in polling stations (e-booths) and sometimes even from remote sites (e.g. via SMS). According to (Cramer R.et al, 2006) e-voting is any voting method where the voter's intention is expressed or collected by electronic means. The following e-voting approaches have being identified by this literature viz;

- Kiosk voting (e-booths)
- Remote electronic voting
- Internet voting (I-voting)

Basically, this work uses the term e-voting with the specific reference to kiosk voting (e-booth) over the internet (through a secure public infrastructure). This is discussed in the SMARESiM design model developed in this work. An Electronic Voting System has asits main components (Cramer R.et al, 2006):

i. The Electronic Voters Register.
ii. Authentication- which is done prior to balloting.
iii. Voting, Collation and Transmission.

Owing to the fact that there are a lot of vulnerabilities in the current voting scheme used in Nigeria, there is a need to develop a secure and reliable means of voting so as to reduce the vulnerabilities associated with voting, increase flexibility and security as well as reducing the cost of elections.

In this work, the use of some of Direct Recording Balloting Machines connected over a VPN (secure internet facility) is characterized. This will completely eliminate the cost associated with the printing of several million ballot papers.

The use of biometric encryption techniques and secured communication channels to transmit voting results which is being adopted in this simulation model would reduce to the barest minimum the fraud and irregularities associated with elections. Worthy of note is that BKB has not yet been adopted in E-voting systems.

## 2. LITERATURE REVIEW

### 2.1. Related Works

The work in (Oleg Murk, 2000) presented e-voting Schemes and explained that e-voting is a promising application of cryptography, which can have positive impact on democratic process. The work discussed cryptographic aspects of constructing e-voting schemes and tried to generate a preliminary framework on the notion of choice. The author added that on the internet, implementing cryptographic protocols like digital encryption and signature has been widely accepted.

The authors in (Ivan Damgard et al, 2002) described the theory behind a practical voting scheme based on homomorphic encryption and gave an example of an ElGamal-style encryption scheme, which can be used as the underlying cryptosystem. The work presented the most important goals for electronic voting schemes viz: Privacy, Robustness, Universal verifiability and freeness.

Fundamentally, different approaches to electronic voting are known in the literature such as the use of blind signatures and anonymous channels (A. Fujioka et al 1992), where the channels can be implemented using MIX nets (Ohkubo and Abe, 2000),(Abe,1998) for instance or be based on some physical assumption (Ivan Damgard et al, 2002). The idea in such a scheme is that a voter prepares a ballot in clear text, i.e., a message stating for whom he votes (Ivan Damgard et al, 2002). He then interacts with an authority that can verify that he is eligible to vote and has not already voted. If this is the case, the authority issues a blind signature on the ballot. Informally, this means that the voter obtains the authority's digital signature on the ballot, without the authority learning any information about the contents of the ballot. On the other hand, a voter cannot obtain such a signature without interacting with the authority, and is therefore prevented from voting several times (Ivan Damgard et al, 2002).

The work in (IEEE Security & Privacy, 2008) presents an evaluation of e-Voting systems equipped with voter-Verified Paper Records. The work stated that owing to the need to increase public confidence, various states are increasingly considering electronic voting systems that provide voter verified paper records. In the work, an analysis and evaluation of New Jersey’s criteria against several different e-voting machine types revealed potential threats and possible solutions on privacy, security, and performance issues. The authors in(IndrajitRay et al, 2001) propose a secure electronic voting protocol that is suitable for large scale voting over the Internet. In their work, the protocol allows a voter to cast his or her ballot anonymously by exchanging untraceable yet authentic messages. The protocol ensures that (i) only eligible voters are able to cast votes, (ii) a voter is able to cast only one vote, (iii) a voter is able to verify that his or her vote is counted in the final tally, (iv) nobody, other than the voter, is able to link a cast vote with a voter, and (v) if a voter decides not to cast a vote, nobody is able to cast a fraudulent vote in place of the voter. The following assumptions were made in the context of this protocol viz (Indrajit Ray et al, 2001):

i. Hard-to-invert permutations
ii. Blind Signature on messages
iii. Secure Transit

In their final analysis, the work concludes that the protocol is suitable for large scale voting over the Internet and that satisfies the core properties of secure voting systems – namely accuracy, democracy, privacy and verifiability.

The authors in (Adem and Metin, 2011), observed that the traditional methods of electioneering is characterized by long period of preparation, fake voting, faulty voting, mistakes made in counting the votes, long period of counting and high cost of voting process, in order to avoid these limitations; the system applied biometric fingerprint authentication. In the work, a biometric based e-voting system is designed for providing a secure election on electronic environment for the electors. Technologies such as XSL language which is compatible with Asp.Net, Framework 2.0, Java Script, Xml is used but can be deployed in Microsoft Windows operating system (Adem andMetin, 2011). Again, the, biometric based software libraries are also used for integrating the fingerprint control to the system. In this regard, the elector identification system is programmed with C# language and equipped with an optical fingerprint scanner SDK (SupremaInc®) to accept a scan, recognize the elector, and open the correct elector record in the database and verify system (Suprema, 2010). This module uses a dynamic link library (DLL) that can be displayed in a web application. Attacks are indispensible in biometric based systems, hence besides privacy issues, the major identified limitations of the works discussed above is presented. Applying texture-based feature extraction techniques to fingerprint authentication is very vulnerable. In this case, its security properties considering biometric integration is very vulnerable as attackers, Trojan horses, etc. Biometric technologies may add a new level of authentication and identification to applications, but are not, however, without their risks and challenges. There are important technological challenges such as accuracy, reliability, data security, user acceptance, cost, and interoperability, as well as challenges associated with ensuring effective privacy protections. Some common security vulnerabilities of biometric systems include: spoofing; replay attacks; substitution attacks; tampering; masquerade attacks, trojan horse attacks and overriding Yes/No response(J.L, Wayman, 2001).All feature extraction e-voting models are weak. A traditional biometric system will store the original templates in a database, for use in authentication/identification comparisons. If an attacker can gain access to the database (despite its security measures) then all template data (X) can be compromised (J.L, Wayman,2001).

## 3. DESIGN METHODOLOGY

In this research, an acceptability Index score was obtained from primary data sources (INEC offices in Anambra, Abuja and Enugu). At the time of this research in June 2012, limited hardware facilities lacked the functionalities required for optimizing our BE algorithms in the country. Consequently PROTEUS ISIS version 7.6 was used to develop a real life simulation that characterizes the voting scenario using program description language which later was coded with Assembly language. The implementation was characterized with various components to realize the expected simulation behaviour. Also, the control program of the chips was encrypted. The algorithm was captured in the codes and simulated modules/classes include: the Fingerprints Processing Unit (FPU), the Remote Polling Booths (RPB), State Collection Centers (SCC) and the National Collection Center (NCC), all linked via a VPN communication link. The methodology used here has embedded in it a certain degree of gate level oriented design and programmable VLSI (Very Large Scale Integration) in the sense that gate level components are logically connected together and used to characterize various components in this system. Also programmable microcontroller chips were embedded in this design to serve as the CPUs of the various blocks in the model, hence conceptualized as HYBRID MODELING AND SIMULATION METHODOLOGY. All the logical components characterized or modeled to describe the real life scenarios. After the configurations, the model was run in a simulation environment depicting a contextual voting scenario.

### 3.1. Multi-Protocol Label Switch -Open Virtual Private Network (MPLS-OVPN)

This work identified MPLS-VPN as an important solution to security threats surrounding the use of public networks.It offers a secure network connection between a sender and a receiver over a public non- secure network. A VPN transforms the characteristics of a public network into those of a private secure network and provides the means to securely transmit data between two networked devices over an insecure transport medium (Cranor L, 2007). A VPN creates a secure virtual links between their co-operate headquarters and remote sites via the internet.

In the characterization of the proposed SMARESiM, the polling booths at the various wards would be characterized as the remote INEC offices, the state INEC collection centers would be characterized as the branch offices while the INEC headquarters in Abuja is characterized as the co-operate office. But when compared to other solutions e.g. leased lines, VPNs are relatively inexpensive.

VPN makes use of many security mechanisms e.g. encryption, the use of digital signature to ensure that data cannot be modified without detection. It uses tunneling process to transport the encrypted data over the internet. Tunneling is mechanism for encapsulating one protocol in another protocol (Cranor L, 2007). The VPN architecture consists of the VPN client, Network Access Server (NAS), A Tunnel terminating device (VPN sever), and a VPN protocol.

#### *3.1.1. Open VPN Solution*

OpenVPN is a VPN solution adopted in proposed SMARESiMmodel. This work characterizes tunneling, encapsulation and transfer of data. It uses VNI (Virtual Network Interface) for capturing in coming traffic before encryption and sending outgoing traffic after decryption. The VNI appears as the actual network interface to all applications and users.

Essentially, an OpenVPN performs the following viz:

1. Receives packets of data (votes) from the polling booths using after receiving the packets, it compresses the packets.
2. After compression, it encrypts the packets.
3. It tunnels the packet to the receiving end.
4. On receiving the encrypted traffic, the OpenVPN performs the reverse of cryptographic operations to verify its integrity and authenticity.
5. It then decompresses the packets.
6. The decompressed data is passed by the VNI to the user interface.

Fig 1 shows the flow diagram of information between the various polling booths in different wards, the state and national collection centers as characterized by the SMARESiM.

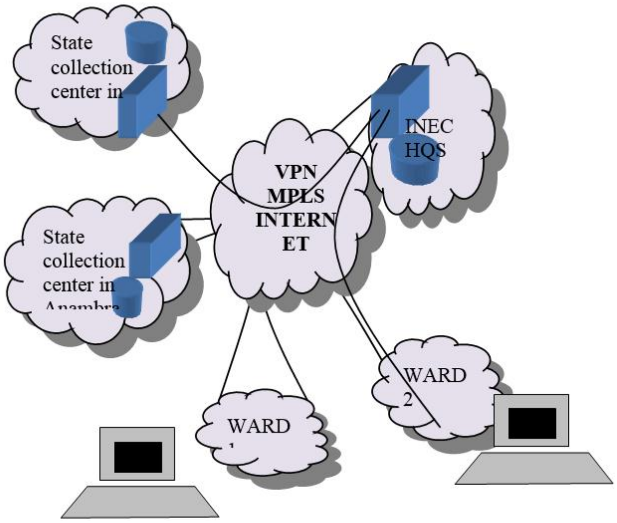


*Figure 1: The Flow diagram of MPLS -VPN backbone for the proposed SMARESiM*

### 3.2. Biometric Encryption (BE) Proposal Adopted in SMARESiM

The concept of Biometric Encryption (BE) was first introduced in the mid-'90s by (G.J. Tomko et al, 1996) and is adopted in SMARESiMproposed model. BE is a process that securely binds a key to, or extracts a key from, a biometric, such that neither the key nor the biometric can be retrieved from the "helper data" (also called a "private template") created by this process and stored by the application, except upon presentation of the correct live biometric sample for verification. In essence, the key is "encrypted" with the biometric — a 'fuzzy' process due to the natural variability of biometric samples. It securely binds a digital key to a biometric or generates a digital key from the biometric, so that no biometric image or template is stored. What is stored is the BE template otherwise known as a "bio-metrically encrypted key" or "helper data". Neither the digital key nor the biometric can be retrieved from the stored BE template which stored. Helper data is obtained by binding a chosen key to a biometric template. As a result of the binding process, a fusion of the secret key and the biometric template is stored as helper data. Applying an appropriate key retrieval algorithm, keys are obtained from the helper data at authentication (Uludag .U et al, 2004). Since cryptographic keys are independent of biometric features, these are revocable while an update of the key usually requires reenrollment in order to generate new helper data. They extract an array of phase values from the fingerprint image using a Fourier transform and apply majority coding to reduce the feature variation. Instead of generating a key directly from biometrics, they introduce a method of biometric locking: a pre-defined random key is "locked" with a biometric sample by forming a phase-phase product (i.e., the dot product of the extracted phrase array and a random-value array). This product can be unlocked by another genuine biometric sample. A sophisticated approach to biometric key-binding based on fingerprints was proposed by (C. Soutar et al, 1998), (C. Soutar, 1999). With BE, the digital key is recreated only if the correct biometric sample is presented on verification.

The output of BE verification is either a digital key or a failure message. This "encryption/decryption" process is fuzzy because of the natural variability of biometric samples.

### *3.2.1. Adopted BEOperational Models*

The Operational mode is depicted in figure 4; at enrollment a filter function, $H(u)$, is derived from $f_o(x)$, which is a two dimensional image array (0 indicates the first measurement). Subsequently, a correlation function c(x) between $f_o(x)$ and any other biometric input $f_1(x)$ obtained during verification is defined by

$$c(x) = FT^{-1}\{F_1(u)F*_0(u)\} \ldots\ldots\ldots\ldots\ldots\ldots(1)$$

which is the inverse Fourier transform of the product of the Fourier transform of a biometric input, denoted by $F_1(u)$, and $F*_0(u)$, where $F*_0(u)$ is represented by $H(u)$. The output $c(x)$ is an array of scalar values describing the degree of similarity (Soutar et al, 1998).

To provide distortion tolerance, the filter function is calculated using a set of T training images $\{f_0^1(x), f_0^2(x) \ldots, f_0^T(x)\}$.

The output pattern of $f_0^T(x)$ is denoted by $c_0^T(x)$ with its Fourier transform $F_0^T(u)H(u)$ . The complex conjugate of the phase component of $H(u)$,$e^{i\phi}(H(u)$, is multiplied with a random phase-only array of the same size to create a secure filter, $H_{stored}(u)$, which is stored as part of the template while the magnitude of $H(u)$ is discarded. The output pattern $c_o(x)$ is then linked with an N-bit cryptographic key $k_o$ using a linking Algorithm I.

I: Linking $k_o$ with $c_o(x)$

*Begin ()*

If (the n-th bit of $k_o$ = 0) then L locations of the selected part of $c_o(x)$ which are 0 are chosen and the indices of the locations are written into the n-th column of a look-up table which is stored as part of the template, termed Bioscrypt.

During linking, redundancy is added by applying a repetitive code. Standard hashing algorithms is used to compute a hash of $k_o$, termed $id_o$ which is stored as part of the template, too.

During authentication, a set of biometric images is combined with $H_{stored}(u)$ to produce an output pattern $c_1(x)$. With the use of the look-up table, an appropriate retrieval algorithm calculates an N-bit key $k_1$ extracting the constituent bits of the binarized output pattern.

Finally, a hash $id_1$ is calculated and tested against $id_o$ to check the validity of $k_1$. The algorithm was summarized in (Soutar et al, 1998).

### *3.2.2. Proposed SMARESiM Model*

An innovative technique for securing a key using a biometrics i.e. biometric key binding is adopted in this work SMARESiM (Self-Monitoring and Reporting Electronic Voting Simulation Model). The digital key is linked with a biometric trait at a more fundamental level during enrollment, and is later retrieved using the same biometric trait during verification.

Furthermore, the key is completely independent of the biometric data, which means that, firstly, the use of the biometric is not forfeited if the key is ever compromised, and secondly, the key can be easily modified or updated at a later date.

We can refer to the biometrically encrypted template as a cancelable fingerprint.During enrollment,the Biometric Encryption process combines the biometric image with a digital key (which is randomly generated and not known even to the user)to create a secure block of data, known as a Bioscrypt.The digital key can be used as a cryptographic key.

The Bioscrypt is secure in that neither the fingerprint nor the key can be independently obtained from it.During the voter verification, the Biometric Encryption algorithm retrieves the cryptographic key by combining the biometric image with the Bioscrypt.

Thus, Biometric Encryption does not simply provide a yes/no response in user authentication to facilitate release of a key, but instead retrieves a key that can only be recreated by combining the biometric image with the Bioscrypt. It is this cryptographic key obtained that now allows the verified voter, access to the e-voting system.

After the voter cast his vote for the party of his choice, the votes is split into packets of data, which is encapsulated another packet with headers and then tunneled over a secured network facility (a VPN for this model). At the receiving end (collection centers), the encapsulated packets is de- encapsulated (the encapsulation and de-encapsulation is done via AES 128 encryption standards). The votes are now tallied at the respective collection centers and the final tally is done at the INEC national headquarters in Abuja.

Fig 2which shows an analytical representation of the Biometric Key Binding (BKB) technique adopted and characterized in the proposed SMARESiM.

### 3.3 Modeling Assumptions

In this research, the SMARESiM is assumed to fit into the Nigerian environment which has 36 states as independent remote blocks. The BKB algorithm, we assume that multiple fingerprint samples Foare collected during the enrollment exercise and is encrypted. The fingerprint samples collected from the individuals during the enrollment or registration process are processed and the processed fingerprints are then are then bound with randomly generated strings of number Nk in a Biometric Key Binding (BKB) algorithm so that the randomly generated string Nkbe recovered on representation of the same fingerprint sample F1 of which F1 ≈ Fo'.

In this security and privacy based algorithm for the SMARESiM, the communication link used between the various polling modules {pm1, pm2,……., pmn} and collection points {cp1,cp2,…Σcp} in this model is the Open VPN backbone given as OVPNx where encrypted data (individual votes) En is tunneled via a secure and private network VPNx that is built on top of existing physical network in context of VPN Multi-Protocol Label Switching(MPLS).

It is assumed that VPNxmaintains data privacy through the use of a tunneling protocol, AES 128 encryption protocol and other security procedures.

This work assumes the use of two most common types of VPN setups; Remote access VPN and site-to-site VPN. The Remote Access VPN configuration is used to allow the individual polling booths located at remote sites to be able to communicate in a secure manner with the state collection centers while the site-to-site VPN allows for creation of dedicated, secure connections between the various INEC state collection centers and the national collection center across the open Internet or public connection.

Fig 3 gives a block diagram representation of the flow of information from the Remote Polling booth units (RPBU) to the INEC State Collection Centers (SCC) and the INEC National Collection Center (NCC) i.e. the end to end flow of information in the SMARESiM.

Each polling booth has these modules:

- Function keypad buttons
- Visual Display Unit

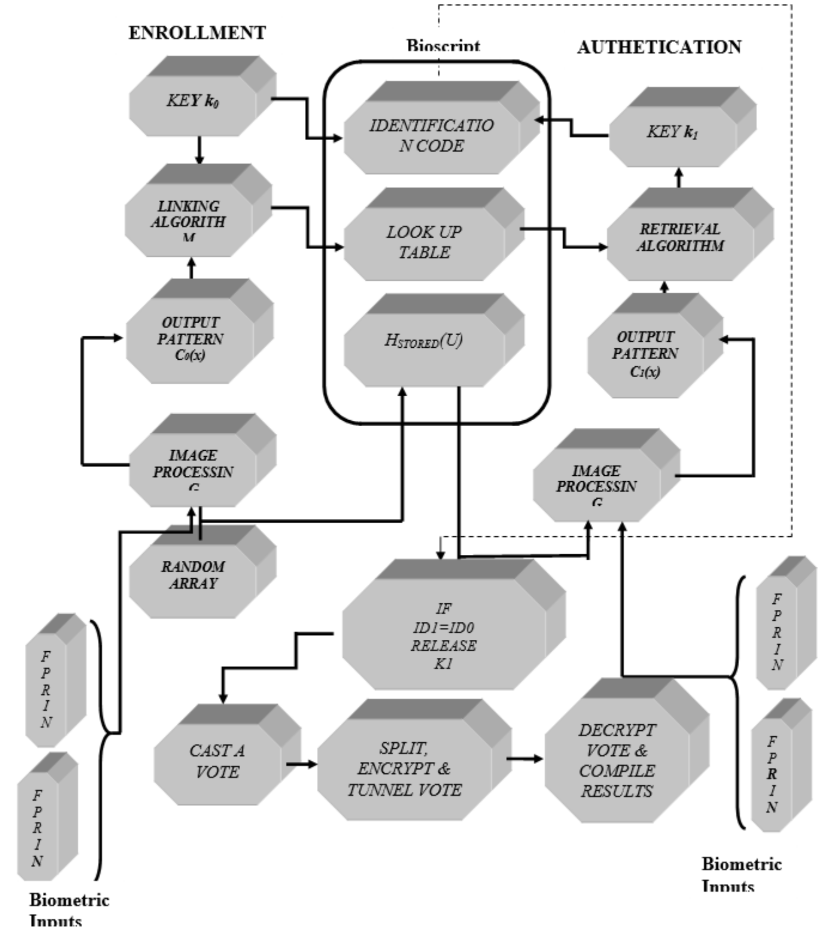


*Figure 2 an analytical model for enrollment and verificationin a biometrically encrypted E-voting system.*

- The Bioscrypt finger print module
- Secure Crypto-processor:
- Virtual Network Interface.

Each states collection centers and the national collection center will have the following:

- Control keypad:
- The Bioscrypt finger print module
- Secure Crypto-processor
- Virtual Network Interface

## 4. IMPLEMENTATION&EVALUATION

### 4.1. Simulation Design with Proteus 7.6

In the proposed the SMARESiM, Proteus 7.6 ISIS was used to characterize the individual E-polling booths and collection centers. It provides the platform through which the various voting processes were characterized. Typical applications of Proteus 7.6 ISIS include standard-based electronic and logical component feature characterization. The Proteus 7.6 ISIS environment is organized into; probe/simulation environment, component editor, sub circuit editor with a comprehensive collection of work tools that were used to characterize the SMARESiM. The Proteus 7.6 ISIS environment provides several modules for the simulation comprising a vast enterprise of digital and analog tools which with friendly graphical user interface that can be manipulated to achieve desired results.

### 4.2. Program Description Language (PDL) for the SMARESiM

A) Polling booths PDL

```
START
    Scan for Encrypted Finger Print
    IF Finger Print = 1 THEN
            DO UNTIL Keypad = 1
                    Display Chosen Party
                    Transmit Vote
            END DO
```

```
        ELSE
                Display "Voter not allowed"
        END IF
    END
```

```
    B) Collection Centers PDL
    START
        Scan for Encrypted Finger Print
        IF Finger Print = 1 THEN
                DO UNTIL Control Keypad = 1
                        Select Polling booth
                        Tally Votes
                END DO
        ELSE
                Do not grant access
        END IF
    END
```

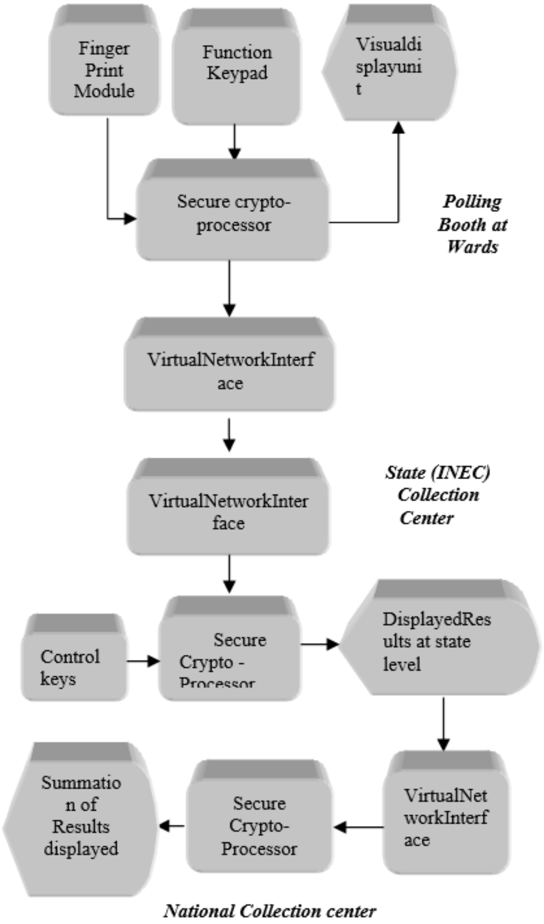
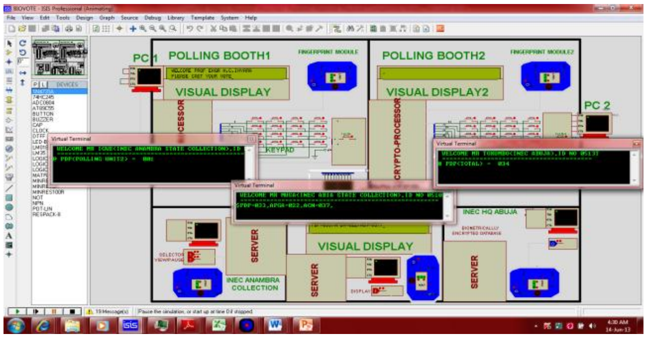


*Figure 3: Flow diagram for the SMARESiM Logical Interfaces End to End*

The PDL shown above is a summary of the lengthy code used in the characterization of the SMARESiM.



```
WELCOME PROF ENGR H.C.INYIAMA
PLEASE CAST YOUR VOTE_
```

```
WELCOME MR IGWE(INEC ANAMBRA STATE COLLECTION),ID
# PDP(POLLING UNIT2) = 001
```

```
WELCOME MR MUSA(INEC ABIA STATE COLLECTION),ID NO 0510
$PDP=033,APGA=022,ACN=037,
```

```
WELCOME MR TOKUMBO(INEC ABUJA),ID NO 05131
# PDP(TOTAL) = 034
```

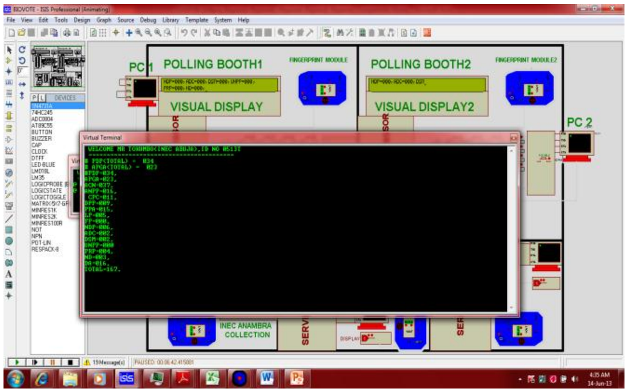
*Figure 4: Snapshots of the SMARESiM during Voting and Collection of total results*

Fig 11 presents a snapshot of SMARESiM with the administrators of the state and national collection centers having access to election results as the coming from the various polling booths. It also shows two voters at different polling booths. An MPLS-VPN backbone for the proposed SMARESiM was characterized based on the parameters in Table 1.

OPNET modeler generates Trace files which are event scripts generated by the OPNET engine after a successful compilation. The OPNET modeler has object palettes with block sets that are configurable with real time or production values. It is these values fed into the OPNET engine that was used to characterize and configure the VPN communication link and it is on that basis that the graphs in fig 7 a-d where generated

### 4.3. Results and Analysis

The results obtained from the simulation model test bed are presented. The tallied election results are illustrated in pictorial form in the figure 16. The results were obtained from the SMARESiM. OPNET was used to evaluate the communication metrics; latency, throughput, stability margin and resource utilization.



```
NDP=000,ADC=000,DSM=000,UNPP=000,
PRP=000,ND=000,_
```

```
WELCOME MR TOKUMBO(INEC ABUJA),ID NO 05131
=========================================
# PDP(TOTAL) = 034
# APGA(TOTAL) = 023
$PDP=034,
APGA=023,
ACN=037,
ANPP=016,
 CPC=011,
DPP=009,
PPA=015,
LP=005,
PP=000,
NDP=006,
ADC=002,
DSM=002,
UNPP=000
PRP=004,
ND=003,
DA=016,
TOTAL=167,
```

*Figure 5 Snapshot capture of SMARESiM at the national collection center displaying total results on Proteus 7.6*

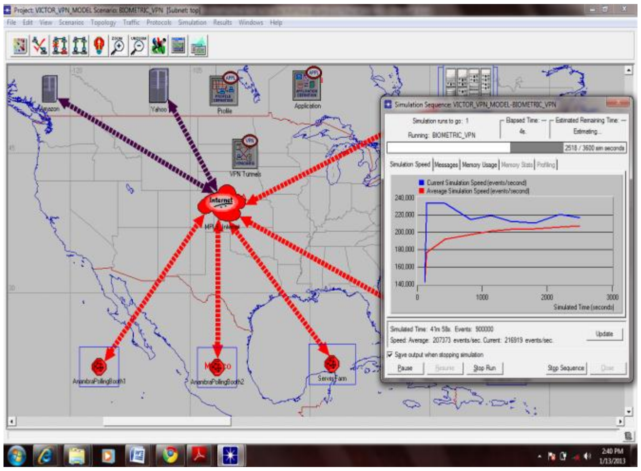
*Table 1: VPN-MPLS Parameters*

| LDP Configurations | Values |
|---|---|
| Status | Enabled |
| No. of Tunnel Sources with Names | [2]-Anambra Polling Booth 1&2 |
| No. of Destination centers with Name | [1]-Headquarter.Network Server |
| Encryption delay | 0.05sec |
| Decryption delay | 0.05sec |

| | |
|---|---|
| Advertisement Policy | No Delay |
| Signaling DSCP | CS6/NC1 |
| Reoptimization Timer(sec) | 3600 |
| Delay (sec) | 20 |
| Retry Timer (sec) | 120 |
| Propagation TTL | Enabled |
| Traffic Engineering | BGP |
| Fast Reroute Status | LSP Config |
| Revert Timer (Sec) | LSP Config |
| Label Space Allocation | Global GLA |
| CSPF Optimization Metric | TE Link Cost |
| Number of Shortest path | 5 |

### 4.4. Validation of Model's Communication Link

For the purpose of validation of the SMARESiM communication link, OPNET modeler was used to validate the traffic engineering in the system. OPNET was used to evaluate the end to end latency between the polling modules and the collection centers, its throughput, network stability and its network resource utilization. It is seen from the graphs that the VPNMPLS communication backbone for the SMARESiM would have low end to end latency, high throughput, high stability margin and efficient resource utilization considering the design layout for deployment of the SMARESiM.



Simulation runs to go: 1
Running: BIOMETRIC_VPN
Elapsed Time: 4s
Estimated Remaining Time: Estimating...
2518 / 3600 sim seconds
Simulated Time: 41m 58s Events: 500000
Speed: Average: 207373 events/sec. Current: 216919 events/sec.
☑ Save output when stopping simulation

*Figure 6: Snapshots capture of the OPNET modeler, showing how tunnels are created from end to end links in the MPLS VPN communication channel.*

### 4.5. Discussion of Results

OPNET was be used to evaluate the end to end latency between the polling modules and the collection centers, its throughput, network stability and its network resource utilization. This formed the basis for validation since biometric encryption has not been implemented in any E-voting model.

It is seen from the graphs in fig 7a, 7b, 7c, 7d; the MPLSVPN communication backbone for the SMARESiM had a low end to end latency, high throughput, high stability margin and efficient resource utilization considering the design layout for deployment of the SMARESiM.

## 5. CONCLUSIONS

A simulation model of an e-voting system leveraging on Biometric Encryption vizBiometric key Binding technique for the proposed SMARESiM has been adopted and characterized. An MPLS VPN backbone as its communication link has been successfully adopted and characterized. The communication link has also been validated using metrics like end to end latency, Throughput, Network Stability and Tunnel resource utilization. Worthy of mention is the fact that Biometric Key Binding (BKB) has not yet been adopted in any E-voting systems.

## REFERENCES

A. Fujioka, T. Okamoto & K. Otha: A practical secret voting scheme for large scale elections, Advances in Cryptology AusCrypt '92, pp.244-251.

Abe: Universally verifiable MIX net withverification work independent of the number of MIX centers; proceedings of EuroCrypt 98, Springer Verlag LNCS.

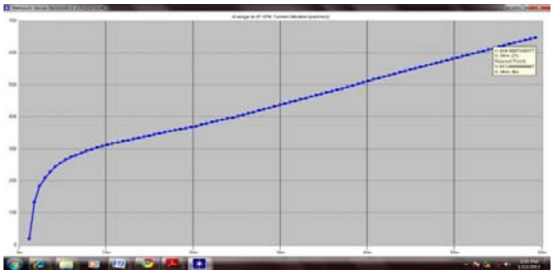


*Fig14a Average Resource Utilization*

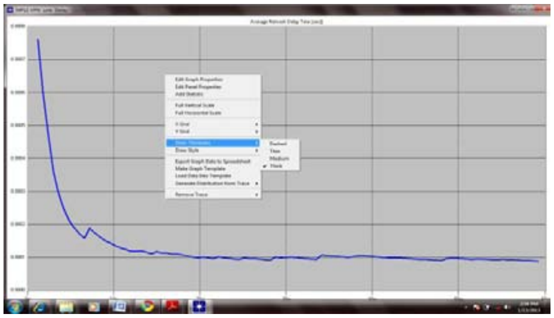


*Fig 14b AverageNetwork Delay Response*

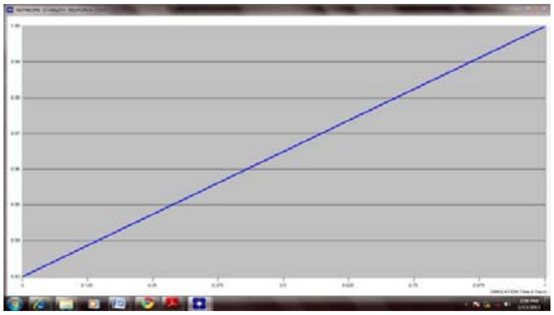


*Fig 14c Average Network Stability*

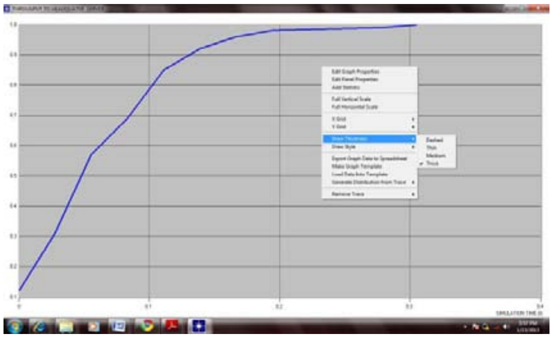


*Fig 14d Average Network Throughput Response*

AdemAlpaslan  andMetin BĐLGĐN: “ Web based secure e-voting system withfingerprint Authentication”  In ScientificResearch and Essays Vol. 6(12), pp. 2494-2500, 18 June, 2011.Available online at http://www.academicjournals.org/SRE.

C. Soutar. Biometric system security. Available at http://www.bioscrypt.com/assets/securitysoutar.pdf.

C. Soutar, D. Roberge, S. A. Stojanov, R. Gilroy, and B. V. K. VijayaKumar;. Biometric encryption using

image processing. In Proc. SPIE, Optical Security and Counterfeit Deterrence Techniques II, vol. 3314, pages 178-188, 1998.

Cramer, R. Franklin M. Schoenmakers B. and Yung M. (2006) Multi-authority secret ballot elections with linear work. In:Advances in Cryptology,EUROCRYPT'96, Lecture Notes inComputer Science, pp.72-83.

Cranor L. and Cytron R. (2007) Sensus: a security-conscious electronic polling system for the Internet. In: Proceedings of the Thirtieth Hawaii InternationalConference on System Sciences, Vol.3, pp.561-570.

G.J. Tomko, C. Soutar, and G.J. Schmidt.“Fingerprint controlled public key cryptographic system”. U.S.Patent5541994, July 30, 1996 (Priority date: Sept. 7, 1994).

IndrajitRay, Indrakshi Ray, NatarajanNarasimhamurthi: “An Anonymous Electronic Voting Protocol for Voting Over The Internet”.

Ivan Damgard, Jens Groth and Gorm Salomonsen, TheTheory and Implementation of an Electronic,Voting System, July 31, 2002.

J.L, Wayman, “fundamentals of biometric authentication technologies” Int. Image geaphics, vol.1, no.1, pp. 93-113, 2001.

Ohkubo and Abe: A Length-Invariant Hybrid Mix Proceedings of Asia Crypt 00, Springer Verlag LNCS.

Oleg Murk,Electronic Voting Schemes, M.Sc term paper,2000.

Shane, P. (2004) Democracy Online: The Prospects for Political Renewal through the Internet. New York: Routledge.

Uludag U, Pankanti S, Prabhakar S, Jain AK: Biometric cryptosystems: issues and challenges. Proc IEEE 2004, 92(6):948 960.

www.computer.org/security: Evaluating Electronic Voting Systems Equipped with Voter-Verified Paper Records.IEEE Security & Privacy, 2008.

Full Paper

# SOCIAL ENGINEERING ATTACK AWARENESS: CASE STUDY OF A PRIVATE UNIVERSITY IN NIGERIA

**C.AJAEGBU**
Computer Science Department Babcock University
chigozirim.ajaegbu@yahoo.com

**O. A. Adesegun**
Computer Science Department Babcock University
adeseguno@babcockuni.edu.ng

**Y. A. Adekunle**
Computer Science Department Babcock University
adekunleya@gmail.com

**O. Awodele**
Computer Science Department Babcock University
delealways@yahoo.com

**ABSTRACT**

Research has shown that social engineering attack is a form of attack that leverages on human mind or emotional desires in order to fortify their attacking strategy. Over the years, industries/organizations have devised several means of thwarting the technological based attacks but this form of partially non-technological base attack has been a challenge going by the security measures currently in place. The main aim of this work was to examine the level of social engineering attack awareness using a private university in Ogun state as case study. In order to cover the entire university community, the survey research design was adopted where the stratified random sampling technique was implemented across the university. In each of the stratum, a random sampling technique was applied and the result showed that the level of social engineering attack awareness was poor. In essence, the campaign of this form of non-technical attack should be given due attention in respect to an awareness program.

**Keywords:** *Phishing, Vishing and Social Engineering*

## 1. INTRODUCTION

Organizations over the years have devised several means of thwarting technological based attacks by attackers. Recently, attackers seem to abandon those technological based attacks for a more physiological and dangerous one known as social engineering attack. Social engineering attack has been defined by some scholars in so many ways such as: the act of manipulating people into performing actions or divulging confidential information (Robling and Muller, 2009). Maan and Sharma (2012) defined it as "an attack on human psychology by using some technical skills or technology". Also, Ashish (n.d) in his white paper defines social engineering as the collection of techniques used to manipulate people into performing actions or divulging confidential information. He further presented the reason behind social engineering as the total dependence of computer system on human operators.

Twitchell (2006) looked at it as the practice of using deception or persuasion to fraudulently obtain goods or information and the term is often used in relation to computer systems or information they contain.

Social engineering is a sort of attack that leverages on human weakness or emotional desires to gain access to unauthorized information and should involve the general awareness of the entire public in this 21st century.

Research has shown that social engineering attacks are likely to increase even more going with the high level of the technical security solution which has made it difficult for attackers to execute their attacks effectively.

According to Twitchell (2006) phishing a form of social engineering attack has increased from 2,560 unique phishing attacks as of January 2004 to 15,244 unique phishing attacks in December 2005. He also noted that, the delivery of malware Trojans as part of phishing attacks increased from 5 to 180 unique attacks from January 2004 to December 2005.

Maan and Sharma (2012) classified social engineering attack into two major categories such as Human-Based social engineering attack and Computer-Based social engineering attack.

In human-based social engineering attack, the attacker focuses mainly on the psychological instinct of the victim. This is often achieved through establishment of relationship with the victim, encompassing fear and trust. In this form of attack, the victim releases the information within his/her jurisdiction. This form of attack was further classified into Piggybacking, Tailgating and Telephone Cheat.

In computer-Based social engineering attack, the attacker employs the use of technology by using computer system or its main mode of operation is through technological techniques such as phishing, fake mail and PoP-Up window attack. Thapar (n. d) in his article also pointed out another computer-based social engineering attack known as vishing. Vishing is seen to be the combination of voice and phishing, a practice leveraging voice over internet protocol (VoIP).

## 2. RELATED WORKS

Guido and Muller (2009) highlighted on the unawareness of social engineering and its use to lure people into disclosing confidential information. The aim of their paper was to examine the use of social engineering to access critical/confidential data within a firm. Their work was accomplished through the use of phone calls, where the phone number was suppressed. The caller carried out the operation both as a fictitious and actual member of the firm respectively. Also, Xing and Facebook were used to get the network that the targeted person was connected to and to provide additional information respectively. From their work, they observed that people can easily be deceived through social engineering.

Mann and Manish (2012) in their paper looked at the ill-classification of social attack as a non-technical attack. The main aim of their paper was to show that social attack cannot yield meaningful result to the attacker without technical involvement. Thus their specific objectives were to classify social engineering into two basic types and to establish that social engineering is a partial technical attack. The researcher gave a description of the possible means of achieving social engineering attack through sub-division of the two broad classifications of the attacks. From the descriptive study of the different forms of attack, and its operation, the researchers were able to establish that social engineering cannot be completed without technical involvement. Thus, it can be regarded as a partial technical attack.

Kvedar, Nettis and Fulton (2010) noted the overlap among various authors in the direction of awareness training among employees in an organization. The main aim of their study was to show the effectiveness of social engineering as a network attack and the importance of an awareness program as the major mitigation technique. Thus their specific objective was to use social engineering to obtain information from each group participating in the computer and network vulnerability assessment simulation program. Their paper adopted the four step process of social engineering such as – information gathering, relationship development, execution and exploitation. For information gathering, the public resources were used to find out more about the program; In relationship development, the attacker focuses on the participants by welcoming them on arrival; for execution and exploitation, the attackers disguise themselves as official facilitating the execution of CANVAS, and was able to use that to acquire the necessary information from the focus target. From the analysis pertaining to the vulnerability of social engineering, it was observed that understanding of the value of information as well as proper usage of information is as important as an awareness of social engineering efforts.

Twitchell (2006) opined that with the increased rate of technical attack mitigation, it has become difficult for attackers. This has led to the increased use of social engineering attack to gain unauthorized access to information and it is a potentially dangerous threat to information security. Thus, there is a need to incorporate social engineering in information assurance curricula. The main aim of his paper was to show whether and if the current IA curricula address social engineering. Thus the specific objectives are; to look at the various mitigation techniques for social engineering and to find out the extent to which social engineering and defenses against it appear in current curricula. To achieve that, a review of different proposed mitigation techniques of social engineering from different authors was conducted along with an in depth study of a number of prominent information curricula. From the study, he observed that none of the curricula specifically address some of the important mitigation techniques like education, training, awareness and auditing as related to social engineering though almost all dealt with the general counter measures.

Ashish (n. d) pointed out the need for social engineering awareness stating that the primary reason behind less discussion of enormous social engineering attack is shame (i.e. most humans seeing it as shame having played with their intelligence). The main objective of the paper was to explore possible ways by which social engineering attack could be reduced. Thus its specific objectives were; to predict the possible means of manipulating the user intelligence by the attacker and to suggest counter measures to such attack. In order to achieve this, analyses of the possible social attacks were embarked upon by the researcher and also the classification of the attacks into computer and human based attacks. The outcome of his study was to suggest various means of controlling social engineering attack in an organization. This encompasses the measurement such as information security policy, insurance protection, incident management, audits and compliance, awareness and education and operating procedure.

Though, Twitchell (2006) considered the need for social engineering in academic curricula, its work likewise that of other researchers failed to carry out an awareness test in an academic environment. This researcher work took a closer look at social engineering attack awareness in a university environment.

Gregory, Gordon, Michael and Paul (2004), opined that "cryptography is the only piece of the computer security puzzle that becomes increasingly complex as time & technology advance". But such process is not flexible enough to mitigate the challenges posed by social engineering in computer security paradigm. Their work also noted the importance of implementing a security measure that can counter the two aspects of social engineering which are the physical and psychological aspects. The main aim of their work was to devise proper means to control both the physical and psychological attacks of social engineers. Thus their specific objectives were: to investigate the effect of using the physical and psychological aspect of social engineering in the company; to proffer solution to mitigate such attacks. The work adopted a survey research method where a combination of interview in form of interaction in order to gain trust within the employees of the company was used together with a small draft of questionnaire. The outcome of their work showed that human traits can be ill-used even in a company where security is a concern, if proper preventative measures are not taken.

Lively Jr. (2003) argued that the psychological social engineering based attack, which appears to be more dangerous, seems to be given less attention. The main aim of the work was to investigate the different dimensions of this form of attack. Thus the specific objectives were: to examine the mindset behind social engineering; to classify the psychological based attack into different groups and also take an in-depth look on each. The work adopted a descriptive method, where the author classified the psychological based attack into four major categories and gave the description of each together with the sub-divisions and the possible ways by which the attacker can use them. The outcome of the work showed that there is need for a written security policy in every organization coupled with awareness program among employees.

It was observed that most of the research work that has been conducted in this area has not put into consideration the need to have an awareness program within a university community. Thus the university community forming the pillar for the success of any society, there is a need for an awareness program.

## 3. METHODOLOGY

This research adopted the survey design where a proportionate stratified random sampling technique was used across the various departments/divisions of the University. A population of 160 was considered with 97 as the sample size. For every division considered regardless of the population, a sampling fraction of 3/5 was used for the distribution of the research instrument (copies of questionnaire) and this adopted a random sampling technique among the staff in each department/division.

## 4. ANALYSIS

A total number of 97 copies of questionnaire were distributed and out of the 97 copies, 83 were returned while 14 were not. The result is presented below using bar chart representation.

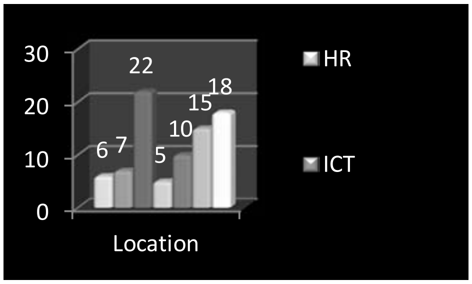


*Fig 1: Department/Division of respodents*

chart showing the various departments/divisions considered together with the sample size of each (i.e sampling fraction of 3/5) in the course of this research work.

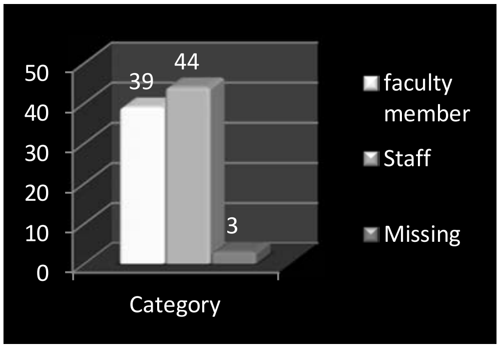


*Fig 2: Institutional placement*

Chart showing placement of respondents. In the university, an employee is either a faculty or a staff. This chart shows the number of faculty and staff members that responded to the questionnaire.

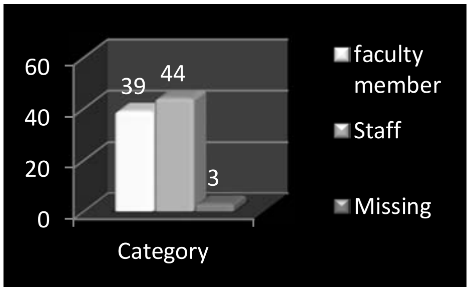


*Fig 3: Gender*

This shows that the total number of respondents (random distribution) in terms of gender were 52 males and 30 females.

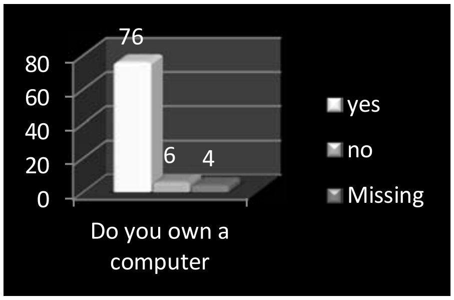


*Fig 4: Respondents that own computers*

The number of computer owners are of greater percentage. This implies that the university community encourages and admires the computer age of 21st century.

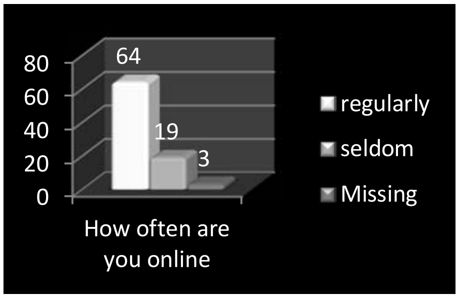


*Fig 5: Rate at which internet is used*

The response shows that there is constant internet access across the entire university community.

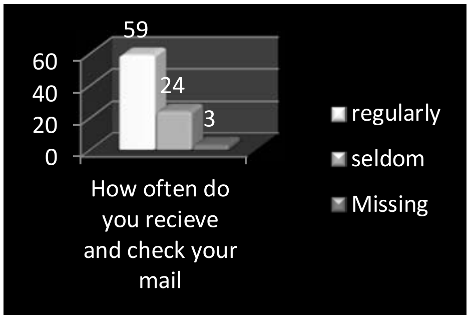


*Fig 6: Rate at which respondents receiving and check mails*

This shows that approximately the whole staff/faculty members understand the need for an E-mail and majority said they check it regularly.

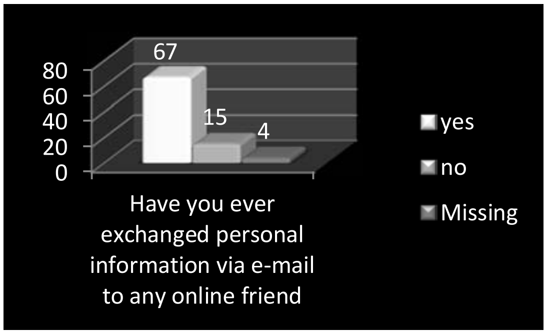


*Fig 7: Exchange of personal information via e-mail*

This chart shows that the level at which staff/faculty members disclose information deemed personal/private to online friends met through say facebook, twitter et cetera is high.

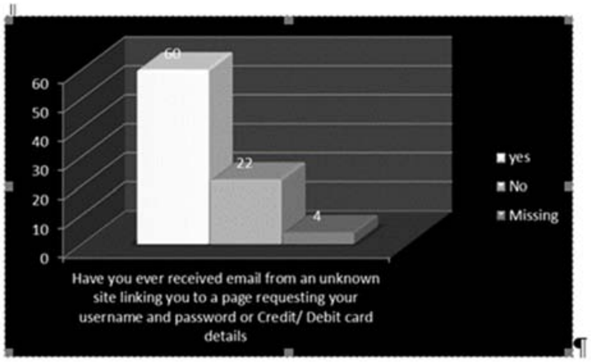


*Fig 8: Respondents response about receiving e-mail from an unknown site*

This chart shows that greater percentage of the respondents have received mails requesting for their user name and password in form of a link.

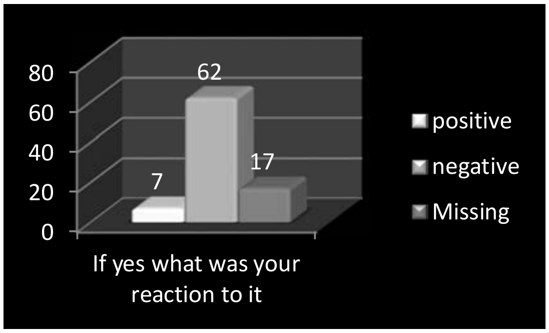


*Fig 9: nature of response in regards to fig 8*

This is a follow-up to the previous question where respondents who answered in the affirmative that they have received mails from an unknown site showed their reaction to the message received. While 7 respondents said their reaction was positive, 62 said their reaction was negative. This shows that the individual conciousness about strange sites is of high percentage in the university community though they might not be fully aware of the purpose of the link.

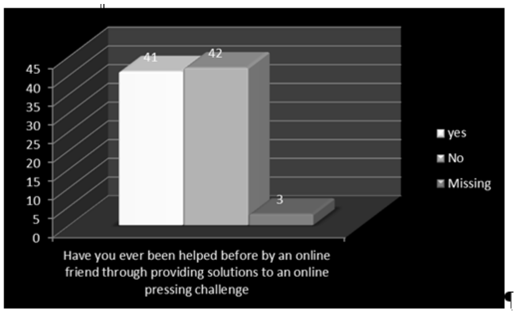


*Fig 10: Seeking for online assistance through an online friend*

This chart shows that some of the respondents (41) have at one time or the other been helped by an online friend at their own will while others (42) have not been helped may be because they lack the knowledge on how to go about it or the attitude of dislike.

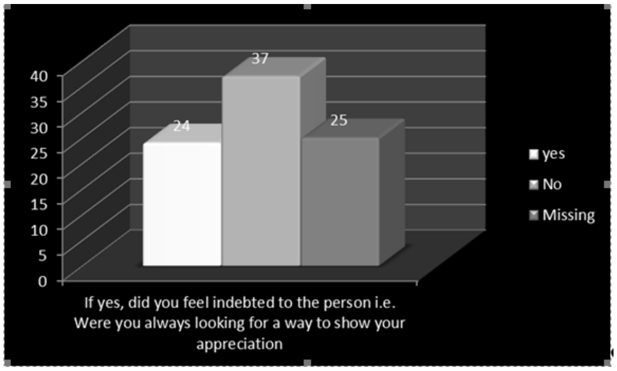


*Fig 11: Reaction to the help rendered*

This chart shows that 24 respondents were indebted to the online friend that helped them, 37 said they were not and 25 dis not give any answer whether they were indebted or not. This shows that the chances at which their intelligence can be manipulated is high.

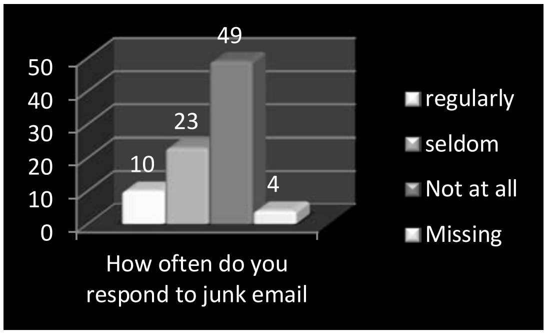


*Fig 12: Respondents response to junk e-mail*

This shows that 10 respondents responded to junk emails regularly, 23 seldomly responded while 49 respondents sadi they do not respond to junk emails at all.

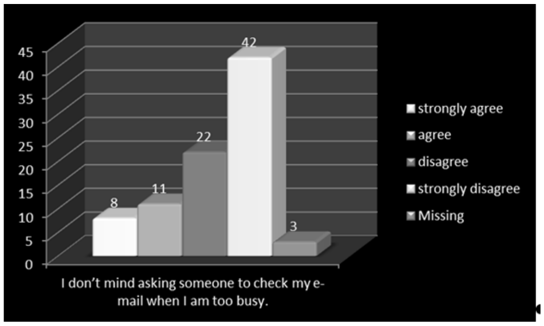


Fig 13: Respondents giving access to another person to check their e-mail

This chart shows the extent to which respondents give access to people to check their personal email when they are too busy to do it. 8 respondents strongly agree that they can allow someone check their mail for them, 11 agree, 22 disagree while 42 strongly disagree that they can allow somebody check their email when they are too busy to do it.

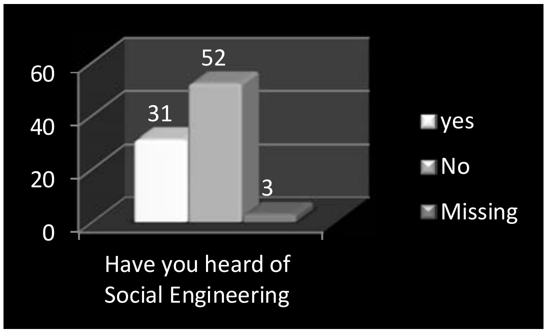


*Fig 14: Respondents knowledge of Social engineering*

This shows that the awareness of the social engineering attack in the university community is very poor.

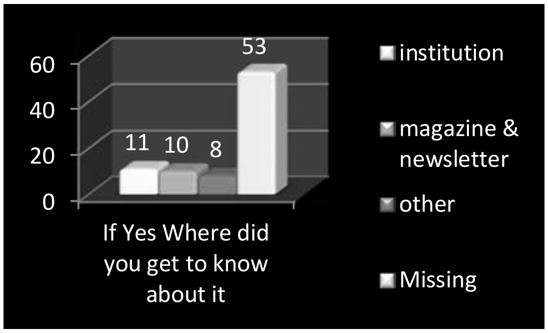


*Fig 15: Rate at which respondents leave PC(s) with other people unattended to*

This chart shows that 7 respondents often leave their PC with friends without supervision, 42 seldom do that, while 33 respondents said they do not leave their PC with friends without supervision. This shows that some respondents believe that having undue access into their PC can leave them vulnerable to attack.

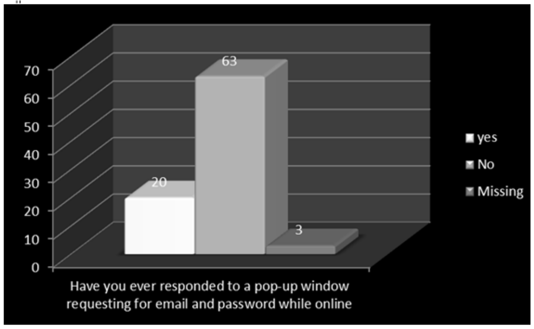


*Fig 16: Response to online pop-up window*

The chart shows that the number of respondents that do not respond to pop-up window is high. This could be as a result of so many things which may include fear of viral attacks among others.

## 5. DISCUSSION OF RESULTS

During the course of this research, the following observations provided answers to the research questions

1. There is a need for every member of staff/falcuty in of the university into consideration, to be aware of basic security measures as regards to the use of internet. For by so doing, the individual and the administration will be freed from any sudden attack that might cause demages to the system in place.
2. It was also observed that the level of social engineering attack awareness among staff/falcuty members is quite poor going with the survey result where the awareness is centering only towards the IT and Computer Science division/department respectively.

## 6. CONCLUSION

The result and analysis shows that there is need to always involve the entire university community in seminars related to computer security issues. This will go a long way not only to create individual or general awareness but will also help to add more value to vital administrative information.

## REFERENCES

Kvedar D, Nettis M and Fulton S P (2010). The use of formal social engineering techniques to identify weakness during vulnerability competition. Journal of Computing Sciences in Colleges.80-87.

Twitchell D P (2006). Social engineering in information assurance curricula. In Proceedings of the 3rd annual conference on Information security curriculum development (InfoSecCD '06), New York. Retrieved from http://dl.acm.org/results.cfm?h=1&cfid=300388271&cftoken=71308834

Maaleji W and Ali R (2011). The 4th International Workshop on Social Software Engineering (SSE'11). Proceeding of the 19th ACM SIGSOFT symposium and the 13th European Conference on Foundation of Software engineering, New York. Retrieved From http://dl.acm.org/citation.cfm?id=2025211.

RoBling G and Muller M (2009). Social Engineering: A Serious Underestimated Problem. Proceedings of the 14th annual ACM SGCSE in Computer Science Education, New York. Retrieved from http://dl.acm.org/results.cfm?h=1&cfid=300388271&cftoken=71308834.

Maan P S and Sharma M (2012). Social Engineering: A Partial Technical Attack. IJCSI International Journal of Computing Science Issue. 9(3), 557-559.

Ashish T (n.d). Social Engineering – An Attack Vector most intricate to tackle. Retrieved on 10/03/2013 from http://www.infosecwriters.com/text_resources/pdf/Social_Engineering_AThapar.pdf

Lively Jr. C. E. (2003) Psychological based social engineering. http://www.giac.org/certified_professionals/practicals/gsec/3547.php

Gregory L. Orgill, Gordon W. Romney, Michael G. Bailey, and Paul M. Orgill. (2004). The urgency for effective user privacy-education to counter social engineering attacks on secure computer systems. Proceedings of the 5th conference on Information technology education (CITC5 '04). ACM, New York, NY, USA, 177-181. Retrieved from http://doi.acm.org/10.1145/1029533.1029577