IOSR Journal of Mobile Computing & Application (IOSR-JMCA)
e-ISSN: 2394-0050, P-ISSN: 2394-0042.Volume 3, Issue 5 (Sep. - Oct. 2016), PP 25-31
www.iosrjournals.org

Secured Models for Online Bank Vulnerabilities in Nigeria

Akinola Kayode E[1], Ehiwe, Dunsen Dominic[2], Somefun Olawale M[3]

[1]Computer Science Department, Abraham Adesanya Polytechnic, Ijebu-Igbo, Ogun State, Nigeria.
[1,2,3]Computer Science Department, Babcock University, Ilishan Remo, Ogun State Nigeria.

Abstract: *Security and confidentiality have always been a challenge to online transactions all over the world. As the number of customers using online banking system increases, the banking channel becomes a target for criminals to carry out their activities. Online banking include – the use of ATM, internet banking, mobile banking via phone /GSM networks etc. - which implement the use of fixed username and password or PIN for ATM cards to protect a customer's privacy or guard against fraud. In this paper, we review the current state of online banking security in Nigeria, its vulnerabilities and thus propose a multi-factor authentication mode of operation to reinforce the use of one time password, card-based authorization codes, transaction password and digital certificate that is commonly used as security measure in most banks in Nigeria.*

Keywords – *Security, Multi-Factor Authentication, Vulnerabilities, Online Banking, Fingerprint.*

I. Introduction

Online banking, also known as internet banking, e-banking or virtual banking, is an electronic payment system that enables customers of a bank or other financial institution to perform a range of financial transactions through the institution's website. The online banking system will typically connect to or be part of the core banking system operated by the bank and is in contrast to branch banking which was the traditional way customers accessed banking services.

Presently, all Banks in Nigeria have embraced Online or internet banking system. The development of Internet banking and its associated technologies has been driven by the ease of access the technology presents to its numerous users. The motivation of investment in electronic banking is largely the prospects of minimizing operating costs and maximizing operating revenue, Simpson J. (2002). Therefore, it implies that cost saving, convenience and speedy delivery have been a driving force in the quick adoption of this system. Bank branches have been shut down and subsequently, savings made from reduced staff remuneration and branch office maintenance budgets Nwogu Emeka Reginald (2012).

The massive implementation and deployment of the Internet banking system has been followed by increased vulnerability of attack. Abaenewe Zeph et al. (2013) write that the adoption of electronic banking (e-banking) has brought major challenges to the banking industry in terms of security. Although, issues related to security is one of the biggest challenges that the banking industry faces, banking online has contributed to this risk in multiple ways. The process involving online banking is such that it potentially keeps the isolated systems vulnerable to an environment which is open as well as risky. Most customers in Nigeria are still oblivious of the security challenges associated with this service; as a result, the vulnerability of these customers to banking online continues to grow. There have been cases of users asking unknown person(s) to assist in withdrawing money from ATM machine; in addition to incomplete sign out from a bank's website, which most of the time often lead to attacks resulting in heavy fund transfer or withdrawer from customers' account.

"Threats on the internet are multi-facet and much vulnerability exists with hackers continuing to exploit these security holes. In order to provide better quality of service to internet users, security flaws must be identified to provide effective defensive mechanism" Akinola & Odumosu (2015).Vulnerabilities on online transaction systems are continually searched for by these scrupulous attackers and when found, heavily exploited. This has resulted in heavy losses by end users, who often are victims of circumstance, as majority of the clients who have fallen victims of these advanced online related frauds have in most times not contributed to their woes.

According to Hole et al. (2012), the style of growth of Online Banking brings many security challenges and increasing cost of implementing higher security system for both Online Banking users and the banks. Hackers and Internet fraudsters are perpetually devising new means of breaking the security features entrenched in the Internet banking systems.

Consequently, there has been a renewed interest in a more robust system that would not only protect end user transactions from fraudulent attacks, but also prevent attacks like "Denial of Service" (DOS). At different times, most of the defenses on Internet banking attacks have been reactive Mathew Johnson (2008). Security systems developers tend more to develop defense against well-known attacks that probably have been over sung in the media and as such, less attention is given to research on current Internet banking system's vulnerabilities; which definitely need adaptive solutions. These days, attackers have become wiser, and are several steps ahead of security systems developers.

Research indicates that the top five banks in South Africa are exploring the adoption of biometric technology in preventing card fraud in the banks. According to Nick Perkins, Divisional Director of Identity Management at Bytes Systems Integration (Bytes SI), even though none of the banks have committed to a roll-out date yet, a particular bank already has over 1000 ATMs with biometric capabilities lined up for use.

"The benefit of using biometrics as an additional user authentication mechanism is two-fold:

- It's an authentication method that can't be copied as a user's fingerprint cannot be successfully cloned without being detected by the machine sensors.

The South African Centre for Information Security says biometric technology has great potential in the African market where the rate of card fraud is high; the adoption of a more secure banking method is long overdue. "The vulnerability of passwords is not going to go away and new alternatives are needed to help people keep their money and accounts secure," agrees Greg Sarrail, Vice President for Solutions Business Development at Lumidigm. Consequently, Nigerian banks must be in sync at extending this technology to the banking populace in the country.

Banking and security professionals expect to have an increasing demand for biometric security systems if governments and corporate institutions in the country and across the continent step up efforts in fighting corruption and crime. In addition, likely applications for the technology adoption will see it being used for border posts identification, ticketing at venues etc.

II. Features of Online Banking

Online banking facilities typically have many features and capabilities in common, but also have some that are application specific.

2.1 The common features fall broadly into several categories:

1. A bank customer can perform non-transactional tasks through online banking, including:

- Viewing account balances
- Viewing recent transactions
- Downloading bank statements, for example in PDF format
- Viewing images of paid cheques
- Ordering cheque books
- Download periodic account statements
- Downloading applications for M-banking, E-banking etc.

2. Bank customers can transact banking tasks through online banking, including :–

- Funds transfers between the customer's linked accounts
- Paying third parties, including bill payments (see, e.g., BPAY) and third party fund transfers (e.g., PayPal, FAST)
- Investment purchase or sale
- Loan applications and transactions, such as repayments of enrollments
- Credit card applications
- Register utility billers and make bill payments
- Financial institution administration
- Management of multiple users having varying levels of authority
- Transaction approval process

2.2 Advantages Of Internet Banking

There are some advantages on using e-banking both for banks and customers:-

- Convenience – Banks that offer internet banking are open for business transactions anywhere a client might be as long as there is internet connection. Apart from periods of website maintenance, services are available 24 hours a day and 365 days round the year. In a scenario where internet connection is unavailable, customer services are provided round the clock via telephone.
- At the touch of a button, actual time account balances and information are availed. This hastens the banking processes hence increasing their efficiency and effectiveness.
- Online banking allows for easier updating and maintaining of direct accounts. The time for changing mailing address is greatly reduced, ordering of additional checks is availed and provision of actual time interest rates.
- Friendlier rates – Lack of substantial support and overhead costs results to direct banks offering higher interest rates on savings and charge lower rates on mortgages and loans.

- Some banks offer high yield certificate of deposits and don't penalize withdrawals on certificate of deposits, opening of accounts without minimum deposits and no minimum balance.
- Transfer services – Online banking allows automatic funding of accounts from long established bank accounts via electronic funds transfers.
- Ease of monitoring – A client can monitor his/her spending via a virtual wallet through certain banks and applications and enable payments.
- Ease of transaction – the speed of transaction is faster relative to use of ATM's or customary banking.

2.3 Disadvantages of Internet Banking

- **Banking relationship** – Customary banking allows creation of a personal touch between a bank and its clients. A personal touch with a bank manager for example can enable the manager to change terms in your account since he/she has some discretion in case of any personal circumstantial change. It can include reversal of an undeserved service charge.
- **Security matters** – Direct banks are governed by laws and regulations similar to those of customary banks. Accounts are protected by Federal Deposit Insurance Corporation (FDIC).
- **Complex encryption** software is used to protect account information. However, there are no perfect systems. Accounts are prone to hacking attacks, phishing, malware and illegal activities.
- **Learning** – Banks with complicated sites can be cumbersome to navigate and may require one to read through tutorials to navigate them.
- **Transaction problems** – face to face meeting is better in handling complex transactions and problems. Customary banks may call for meetings and seek expert advice to solve issues.

III. The Security Threat Associated with Online Banking

- **Security threats which come from malicious insider**–there is too much reliance on external consultants for the maintenance of the system (especially software and networking) in Nigeria banks. The examples of this kind of security breaches are fraudulent activities, stealing of financial information which can be sensitive for the customer etc.
- **Security threats from casual hackers and armed robbers -** This kind of security breach involves defacement of websites or 'denial of service' – which crashes a site etc. in the case of armed robbers. Furst et al (2005) observed that there are several and distinct ATM robbery technique, each of which presents unique challenges in responding.

The most common technique is for the armed robber to rob the ATM user immediately after the victim makes a withdrawal.

Other techniques include the following:

- The armed robber forces the victim to go to an ATM to withdraw cash and collect the money immediately.
- The armed robber forces the victim to reveal the PIN, and then uses the card to make withdrawal
- The armed robber follows someone who has just withdrawn cash from an ATM and robs him or her outside the ATM premises.

These ATM robbery techniques can be curtailed, if CCTV cameras can be installed around banks and ATM machine premises. In addition Nigerian government should provide CCTV cameras on Nigeria highways in major cities and towns Akinola & Ogunobi (2015).

- **Security threats which stem from internal flaws** that exist in the design of the systems or set up of the security measures. Examples of this kind of breach of security can be instances where genuine users who do not have any criminal intention can see and transact from other customers' accounts.

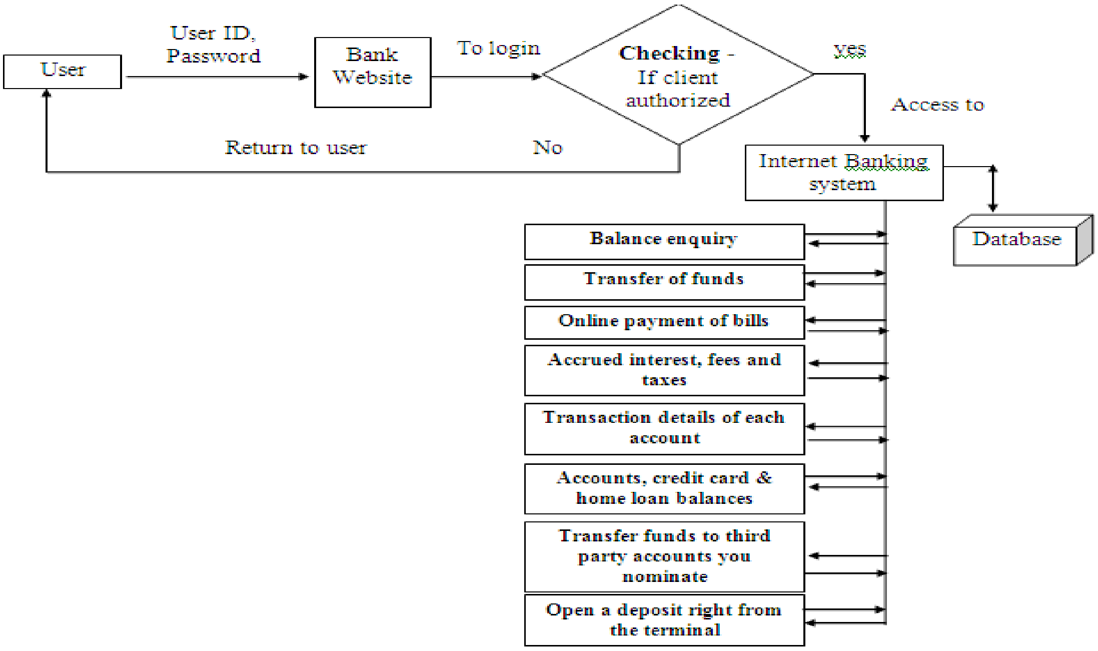
IV. Existing Method of Authentication Used in Most Banks

Authentication mechanisms are of three kinds, these include

1. **Single Factor Authentication -** An authentication mechanism that utilizes any one of the factors is called single factor authentication - this is the basic authentication method. (For example, a User ID and Password comes under this category).
2. **Two Factor Authentication-** An authentication mechanism that utilizes a

combination of two factors i.e. (User Knows, User Possesses). This method is used by various banks for authentication on their banking platform or application E.g. User using a password as the first factor (User Knows) and a One-Time Password (OTP) as the second factor (User possesses) to perform say, a funds transfer transaction.

In the existing internet banking model, a user needs to register with the bank for accessing internet banking by providing his or her account number, after which an authentication code will be sent via SMS to the phone number registered to the account. This is the first level of security that the new user is the account holder, once the user has entered the code, it provide a page for the user to enter his or her user ID, password and select an image as another means of security during registration on the bank's internet banking platform. Then, user can login through bank website if correct ID, password and image are entered, user can access to his bank account with internet banking. There is still an extra authentication process, i.e. to carry out any transaction on the internet banking, user must supply correct token (One Time Password).


User
User ID, Password
Bank Website
To login
Checking - If client authorized
yes
Access to
Return to user
No
Internet Banking system
Database
Balance enquiry
Transfer of funds
Online payment of bills
Accrued interest, fees and taxes
Transaction details of each account
Accounts, credit card & home loan balances
Transfer funds to third party accounts you nominate
Open a deposit right from the terminal

Existing Method of authentication for online Banking

4.1 Disadvantages of Existing Authentication Method

- Internet banking is done by using user ID and password of the user. In this system, anybody who knows the user ID, password, selected image and token can access the bank account and steal money from bank also.
- Complex encryption software is used to protect account information. However, there are no perfect systems. Accounts are prone to hacking attacks, phishing, malware and illegal activities.
- Learning – Banks with complicated sites can be cumbersome to navigate and may require one to read through tutorials to navigate them.
- Transaction problems – face to face meeting is better in handling complex transactions and problems. Customary banks may call for meetings and seek expert advice to solve issues.
- UserID and password can be captured using Trojan-horse programs.

4.2 Proposed Online Banking Security Model

Multi Factor Authentication - An authentication mechanism that involves the following stages:
Stage 1- The use of Login Password
Stage 2 - GSM Phone Numbers
Stage 3–Scanning of finger print or iris recognition

Multi Factor Authentication combines single factor authentication and two factor authentication with scanning of fingerprint or iris recognition. This is very necessary where a large value transaction authorized in a bank by using a combination of the person's user id, a smart card and his biometric authentication factor.

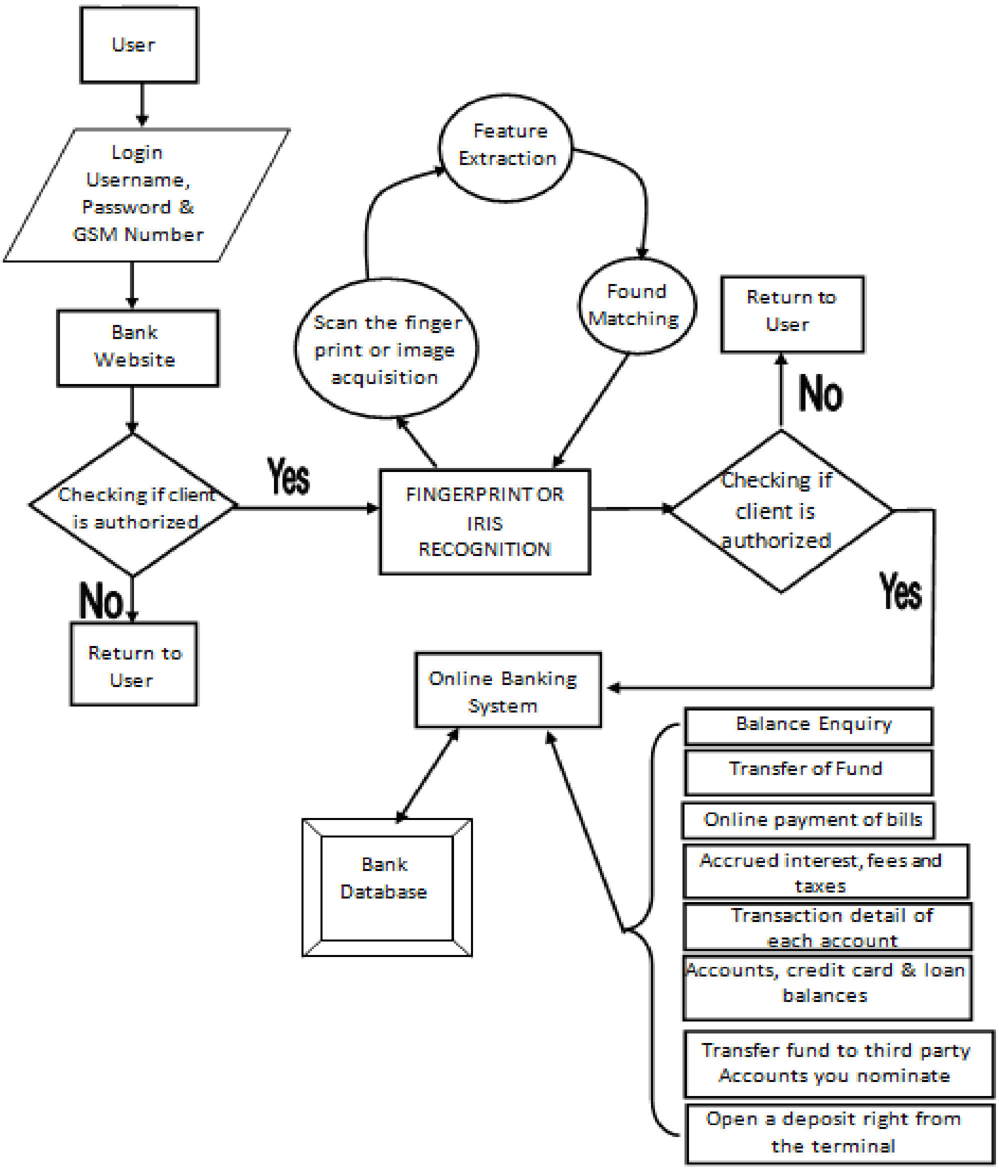

User
Login Username, Password & GSM Number
Bank Website
Checking if client is authorized
Yes
No
Return to User
Scan the finger print or image acquisition
Feature Extraction
Found Matching
FINGERPRINT OR IRIS RECOGNITION
Checking if client is authorized
No
Return to User
Yes
Online Banking System
Bank Database
Balance Enquiry
Transfer of Fund
Online payment of bills
Accrued interest, fees and taxes
Transaction detail of each account
Accounts, credit card & loan balances
Transfer fund to third party Accounts you nominate
Open a deposit right from the terminal

Figure2. Algorithm of Proposed Model for Internet Banking System

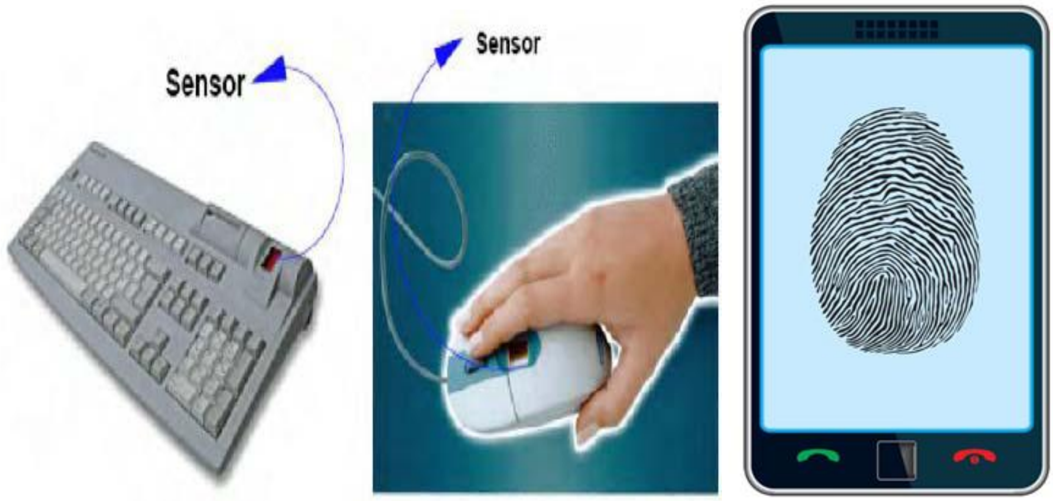
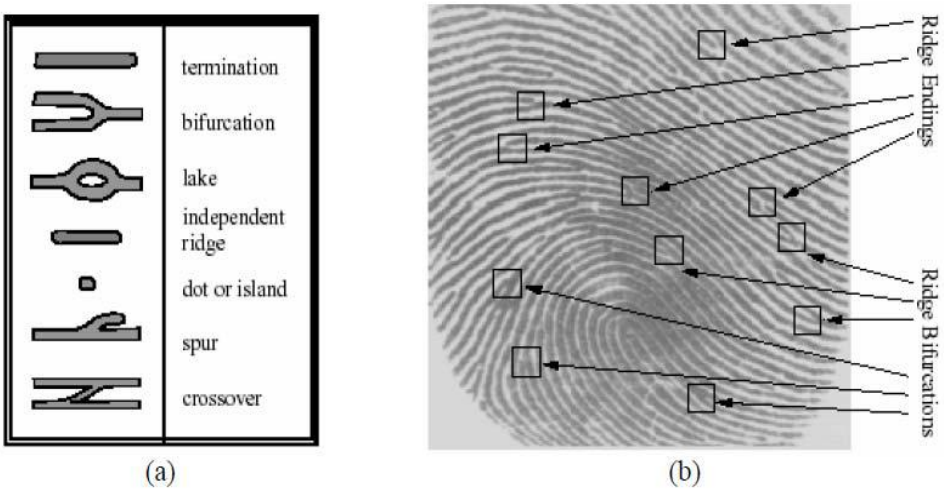


Figure3. Finger print recognition system

V. Finger Print Recognition System

Figure 3, shows the working of finger print recognition. In this process, first user scans his fingerprint through scanner and is sent to the database for validation of fingerprint. This validation is done through finger print recognition system in which image acquisition, edge detection, feature extractor and matching detection are done. If matching is found, the user is allowed to access the system. After the finger print image has been obtained, various methods of processing can be applied to the image to perform the many different vision tasks required today. However, if the image has not been acquired satisfactorily then the intended tasks may not be achievable, even with the aid of some form of image enhancement. Edge detection is a fundamental tool in image processing, machine vision and computer vision, particularly in the areas of feature detection and feature extraction, which aim at identifying points in a digital image at which the image brightness changes sharply or, more formally, has discontinuities. Feature extraction process can be viewed as similar. More complex pictures can be decomposed into a structure of simple shapes.

The arrangement for sensor can be made in-built in the existing computer accessories like mouse, keyboard mobile phone etc. easily. This makes the mode of identification very attractive and easier. Due to its unique identity and easy accessing, the finger print identification has been increased in civil and law enforcement applications.



(a)Different minutiae types, (b) Ridge ending and Bifurcation.

The diagram above shows the most of the existing automatic fingerprint verification systems based on minutiae features (ridge bifurcation and ending). Such systems first detect the minutiae in a fingerprint image and then match the input minutiae set with the stored template.

5.1 Advantages of Multi-Factor Authentication Technique

- In single authentication system, any intruders can hack user id and password and also they can access the internet banking. Mostly, user uses user id and password with name, date of birth, mobile number or family name etc. So hacker can easily trace the user id and password. So it is not secure authentication method.
- Double authentication system is better than single authentication system. In this method, banks provide security code to user mobile. User should use this code for login process. Computer fraud and theft can be hacked by insider or outsider. Insider is most responsible for the majority of fraud action. Since insider can easily hack username, password as well as user mobile SMS also. Mostly insider may be family members, colleague or nearby gang.
- In this proposed model, Finger print recognition has been used for uniqueness and anybody cannot change finger print of user. Fingerprints became an important identification of criminals through finger print recognition. So it is 100% secure model. Users fingerprint cannot be used anywhere without the knowledge of user.
- Finger print recognition is already used for recognizing and validating the frauds. But no internet banking system has used this method to avoid frauds to access the net banking system process.
- In this model, user should scan his fingerprint. But, all system has not scanning peripherals by default. So each system or laptop has to be made with scanning facilities inbuilt. For the machines already in use, user can use additional accessories for finger print scanning.
- Internet banking has user id, password or any other secure code. But there is no unique and secure data to login this system. Finger print is unique for all users.

Method/Model	**User id & password to login**	**SMS Security code**	**Finger print / Iris recognition**	**Security**
Single Authentication system	Can be Hacked			Not Secured
Double authentication system	Can be Hacked	Insider only can hack		Half secured
Proposed model for Internet Banking System with finger print recognition	Can be Hacked		No one can hack	Fully secured

VI. Security Precautions for Banks, Government and Online Banking Users

1. There should be less reliance by banks on external consultants in the maintenance of their computer software and networking.
2. Banks should install CCTV cameras inside and outside of their premises.
3. Banks should update their antivirus software's regularly to safe guard the data of their customers from viruses, worms, Trojans, spyware etc.
4. Banks should adjust to Biometric systems usage i.e. Fingerprint and Iris recognition techniques to identify genuine clients and prevent fraud.
5. Nigeria government should install Closed Circuit Television (CCTV) cameras on public highways and in shopping malls and arcades where ATM machines are installed.
6. Online banking users should not login to their account details from unauthorized computers because some software memorize password.
7. Banks should enable automatic logout of customer on their website after three to five minutes of idleness on their website

Future Work

Future researchers can work on how to do away completely with PIN-Card authorization by the introduction of Bimodal biometrics like Palm and Finger vein, fingerprint and face recognition authentication which is very fast, accurate and difficult to contravened. Furthermore, mobile phones can be found in almost every part of the world in both urban and rural areas, therefore a better authentication with biometric can be developed using smart-phones.

References

[1]. **Abaenewe Zeph, Ogbulu Onyemachi and Ndugbu Michael (2013).** Electronic banking and Bank Performance in Nigeria West African Journal of Industrial & Academic Research. Vol. 6, No. 1.

[2]. **Akinola, K. E., Odumosu, A. A.(2015).** Threat Handling and Security Issue in Cloud Computing.**International Journal of Scientific & Engineering Research (IJSER).** ISSN 2229-5518 (Online). 2015; 6(11): 1371-1377. November 2015. **www.ijser.org**

[3]. **Akinola, K. E. & Ogunobi S. G.(2015).** Availability and Utilization of Information Communication Technology Facilities, in Early Detection and Prevention of Crime in Ogun State, Nigeria. **American Journal of Computer Science and Information Engineering.** ISSN 2375-3846. 2015; 2(2): 23-27.(http://www.aascit.org/journal/ajcsie).

[4]. **Emeka Nwogu and McChester Odoh (2015).** Security

[5]. Issues Analysis on Online Banking Implementations in Nigeria. International Journal of Computer Science and Telecommunications. Volume 6, Issue 1, January 2015.

[6]. **Furst, K, .Lang, W. and Nolle, E. D. (2002) ,** Internet

[7]. Banking Development and Prospects: Working Paper, Center for Information Policy Research, Harvard University

[8]. http://www.financedigest.com/the-rise-of-biometric-technology-in-banking.html

[9]. http://www.bytes.co.za/content/secure-identity-management-key

[10]. **Hole, Moen and Tjostheim (2013**). An Analysis of the

[11]. online banking Security Issues. Department of Computer Science, University of Auckland.

[12]. **Matthew Johnson and Simon Moore (2007).** A New

[13]. Approach to E-banking . In U'Ifar Erlingson and Andrei Sabelfeld, editors, Proc. 12th Nordic Workshop on Secure IT Systems (NORDSEC 2007), pages 127-138. Retrieved . May 14, 2012,

[14]. http:www.matthew.ath.cx/publications/2007-Johnsonebanking.pdf.