American Journal of Engineering Research (AJER)
e-ISSN: 2320-0847 p-ISSN : 2320-0936
Volume-6, Issue-9, pp-226-231
www.ajer.org
Research Paper Open Access

Internet Banking In Nigeria: Authentication Methods, Weaknesses and Security Strength

[a,b]Akinola Kayode E., [b]Amanze Ruth C., [b]Somefun Olawale M., [b]Okonji Charles N., [b] Esomu Solomon E., [b]Nwala Kenneth T. and [b]Odunayo Yewande.
[a]*Computer Science Department, Abraham Adesanya Polytechnic, Ijebu-Igbo, Ogun State, Nigeria.*
[b]*Computer Science Department, Babcock University, Ilishan Remo, Ogun State Nigeria.*
Corresponding Author: Akinola Kayode E.

Abstract*: The growth in internet banking has resulted in a greater demand for fast and accurate user identification, authentication and authorization. Nowadays, numerous banking transaction, such as electronic payments, money transfer, deposits, or securities have become heavily dependable on internet technology. However in recent years there has been an increase in the abuse of internet usage, such as – phishing, malware injection, cyber stalking, identity theft and so on. As online transactions require new authentication methods, banks are trying to introduce new approaches in order to prevent attacks being successful and to increase security. The trend goes towards multiple-factor-authentication (mainly two-factor authentication). In fact most Nigeria banks employ two-factor authentication yet in different ways. Besides usual username or password approaches, additional tokens are applied for authentication in order to make online-banking more secure. This paper reviews the current state of internet banking in Nigeria, its authentication methods , weaknesses and security strength.*

Keywords*: Authentication Factor, Attacks, Weaknesses, Internet Banking, Security*

Date of Submission: 04-09-2017 Date of Acceptance: 20-09-2017

I. INTRODUCTION

Internet banking, also known as Online 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. Internet has been the platform on which most banks transactions and operations rides. According to the Nigerian Communications Commission (NCC), internet users in Nigeria have hit 91 million NCC (2017). Internet banking which include – the use of ATM, mobile banking via phone or GSM networks and so on, offers advantages such as speed of banking, improved efficiency, and convenience as well as less paper work. But since the Internet is a public network, it presents some privacy and security problems. In broad-spectrum internet banking poses significant risks both to the financial institution as well as the customers.

Malicious and criminal users have developed interest in exploiting business transaction opportunities available on the internet. Especially organized criminal attempts are on the rise. Consequently, more sophisticated attacks on internet banking have been on the increase. Most recent trends go towards complex phishing attacks. These types of attacks are not pure technical attacks; they exploit on one hand psychological and sociological properties of users and on the other hand technical flaws and weaknesses. To this end, high security standard needs to be put in place for authentication and authorization of transactions.

II. AUTHENTICATION

An authentication is a piece of information and process used to verify the identity of a person or other entity requesting access under security constraints CBN (2014). Authentication "requires users to prove that they really are who they say they are" before authorization can takes place, and it also governs what the user can access Roland (2004). There are different types of authentication method (One Factor, Two Factors and Three Factors).

Authentication methods that depend on more than one factor typically are more difficult to compromise than single factor systems. Accordingly, properly designed and implemented multi-factor authentication methods are more reliable indicators of authentication and stronger fraud deterrents in internet banking.

American Journal of Engineering Research (AJER)
e-ISSN: 2320-0847 p-ISSN : 2320-0936
Volume-6, Issue-9, pp-226-231
www.ajer.org
Research Paper Open Access

2.1 EXISTING AUTHENTICATION METHODS IN INTERNET BANKING

a) **One Factor Authentication –** This is an authentication mechanism that utilizes any one of the authentication factors like – Personal Identification Number (PIN), Password, smartcard and token. This is the basic and most common authentication method used in Nigerian banks.

b) **Two Factors Authentication-** An authentication mechanism that utilizes a combination of two factors - that is (User Knows and User Possesses). This method is used by various banks for authentication on their banking platform or application. For example, User using a password as the first factor (User Knows) and a One-Time Password (OTP - Token) as the second factor (User possesses) to perform say, a funds transfer transaction (figure 1). Such combinations result in at least two-factor authentication.

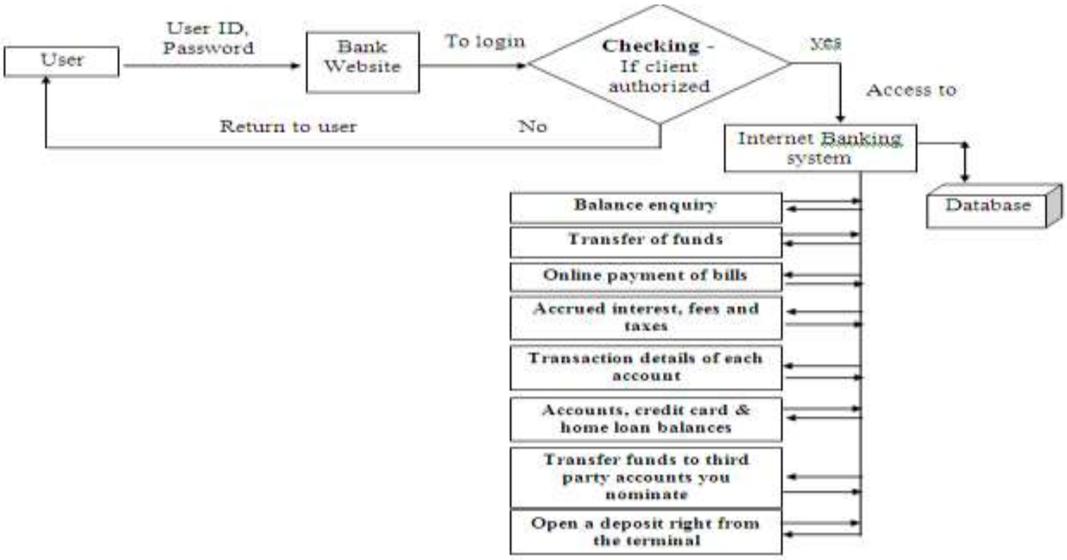
User
User ID,
Password
Bank
Website
To login
Checking -
If client
authorized
yes
Access to
Return to user
No
Internet Banking
system
Database
Balance enquiry
Transfer of funds
Online payment of bills
Accrued interest, fees and taxes
Transaction details of each account
Accounts, credit card & home loan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

Figure 1. Two Factor Authentication Model in Internet Banking using Password and Token
(Source: Akinola, Ehiwe and Somefun, 2016)

c) **Three-Factors Authentication** – This uses all three of the factors of authentication. For example, to access your bank account you might need to scan your fingerprint against a stored image (something you are), insert an access card or token numbers (something you have), and enter a four-digit code (something you know).

2.2 MULTI-FACTOR AUTHENTICATION

Multi-factor authentication can be two-factor or three-factor. Note that using two types of the same factor is not multi-factor authentication. For example, a password and personal information are both what you know, so using them together would still be single-factor authentication. The strength of authentication keys can vary even within a factor category. The name of your pet, a four-digit code and a random eight-character alphanumeric password are all examples of authentication keys based on what you know, but they each provide different protection against discovery attacks. Consequently, the strength of the authentication process is affected by the actual solution used. However, it is generally believed that multi-factor authentication improves security.

TABLE 1. Categorization and Strength of Different Authentication Methods

Method	**Coded Pattern / technique**	**Location of means of Identification**	**Security Strength**
Something you know	Password	Numbers, Alphabets and Symbols on the keyboard	Low
	PIN	Numbers on the keyboard	Low
	Identifiable Picture	Stored Pictures in the database	Low

Something you have	Smart Card or Credit card	Encrypted card from the bank to the account owner	Medium
	USB Token which include One Time Password (OTP)	Encrypted Portable device that you can only buy or get from the bank where you own account	Medium
Something you possess	Fingerprint/Palm print	Fingerprint/Palmprint pattern	Medium
	Iris Features	Iris pattern	High
	Hand Geometry	Length and thickness	Medium
	Voice	Voice characteristics	Medium
	Signature	Shape of letters	Low
	Facial Recognition	Outline, shape and distribution of eyes and nose.	Medium

2.2.1 PASSWORDS

A password is a secret word or alphanumeric text that is shared by the verifier and the customer. It is usual for the verifier to keep the passwords protected on their system by storing them in encrypted or hashed form and in this form they may still be used in the authentication process. So the verifier usually has encoded copies of the passwords. Passwords are normally made up from the characters available on a standard keyboard. In Nigeria today, most banks conduct their transactions with the use of username-passwords, pass phrases or PIN numbers (figure 2).

The use of passwords for authentication is widely established as both implementers and customers accept them. However, password systems are susceptible to many attacks and attacks against passwords are less difficult to resist. Additional protections for the communication channel need to be added to protect the password, but this still does not prevent all attacks. Many security experts now regard passwords, by themselves, as insufficient for online authentication for anything other than low risk services.

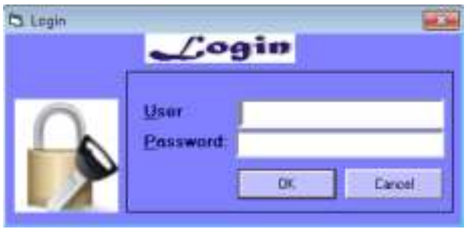

Figure 1. *Password interface*

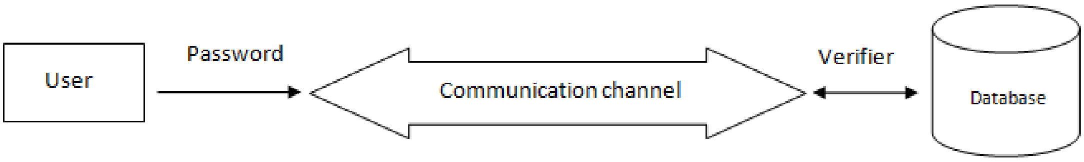

Figure 2. *Password Model*

Advantages of Password

1. Password based online authentication is easy to deploy, as special software does not need to be installed on the customer's computer.
2. Password systems are familiar to customers, systems administrators and managers. The security and management issues are well understood.
3. Passwords can (and should) be encrypted or hashed when stored on the verifier's system.

Disadvantages of Password

1. People have difficulty recalling strong passwords and often forget them, adding to management overheads.
2. An attacker may obtain a customer's password by using password sniffer without the customer being alerted. A password sniffer is a software application that scans and records passwords that are used or broadcasted on a computer or network interface. It listens to all incoming and outgoing network traffic and records any instance of a data packet that contains a password Janssen (2010). Crackers install them on networks used by systems that they especially want to penetrate, like telephone systems and network providers.
3. People will use the same or similar passwords across different systems without regard for the risks involved: the systems may use different levels of protection for the passwords.
4. People write down their passwords and leave the written copy in places that are accessible to others. People use passwords that are easy to remember, which often means they are also easy to guess (and so are weak passwords).
5. People share their passwords. The sharing of a password does not stop the password owners from continuing to use their password. Those

with whom the password is shared have access until the password is changed.

2.2.2 ONE-TIME PASSWORDS

One-time password systems rely on a series of passwords generated using special algorithms. Each password of the series is called a one-time password as it is distinct from the others generated and can only be used once. A wide variety of one-time password systems exist that provide varying protection against attacks. Common advantages of one-time passwords systems are:

(i) They are easy for customers to use

(ii) They have relatively low implementation costs and complexity, when compared to hardware tokens.

(iii) Some of the attacks used against traditional passwords are mitigated with one time passwords. For example, with discovery attacks (attacks that recover passwords such as phishing attacks):

(iv) Any (one-time) password obtained may be used only once

(v) With some systems, the (one-time) password obtained can be used only within a very limited time frame.

(vi) Authentication of the verifier is not usually supported, which can be exploited in attacks.

Figure 3. One time password on the internet
Source: https://images.search.yahoo.com

2.2.3 HARDWARE TOKENS

Tokens is a form of one-time passwords. It is a specialized device that protect secrets (normally cryptographic keys) and perform cryptographic operations. The cryptographic operations support authentication of both parties and the protection of the communication channel used for the authentication exchange.

Drawbacks of hardware tokens, compared to other authentication keys, include:

- Increased cost, implementation and deployment complexity
- Reduced ease of use for customers.
- It can be lost

***Figure 4**. Hardware token*
Source: https://images.search.yahoo.com

Table 2. Comparative Studies of Existing Authentication Methods

Authentication Model	Either User PIN or Password to Login	Smart Card	Iris Recognition	Security Rating
One Factor Authentication Model	Can be Hacked			Not Secured
Two Factor Authentication Model	Can be Hacked	Can be Hacked		Half Secured
Three Factor Authentication Model	Can be Hacked	Can be Hacked	Cannot be Hacked	Fully Secured

Table 3. Summary of past related studies on different authentication models

AUTHORS	TECHNIQUE ADOPTED	CONTRIBUTION	LIMITATIONS
Jimoh and Babatunde (2014).	Short Message Service (SMS) verification.	Developed an algorithm for enhancing ATM authentication system using Short Message Service (SMS) verification. 2.Conducted a usability testing of the proposed system	The developed algorithm only considered a minimum withdrawal amount.
Das and Debbarma (2011)	Finger print biometrics	Developed a system for the withdrawal interface of the ATM while incorporating the finger print biometric in the authentication process	A nominee or third party's finger print was incorporated in the design.
Santhi and Ram (2012)	Finger print biometric and GSM technology	Proposed an algorithm that provides two phases of security using both biometric and GSM technology as alternatives.	The proposed system was not built as an improvement on the existing system
Prithika and Rajalakshmi (2013)	Iris Recognition and Palm Vein (IRPV) recognition technology	Proposed using the Iris Recognition and Palm Vein (IRPV) recognition technology to prevent card duplication and crimes via the ATM	The proposed system was not built as an improvement on the existing system
Okereke and Okpara (2013)	Facial recognition technology	A system which incorporates facial recognition technology into the identity verification process used in ATMs was proposed	The study relied on open-source facial recognition program and did not discuss the local features that will be analyzed for the facial verification process.
Ibidapo, Omogbadegun, and Oyelami, (2010)	Fingerprint biometrics	A fingerprint mechanism as a biometric measure to enhance the security features of the ATM was developed	
Selvaraju and Sekar (2010)	Advanced Encryption Standard (AES) algorithm	The Advanced Encryption Standard (AES) algorithm was adopted to improve the security level of ATM Banking Systems.	
Oko and Oruh (2012)	Finger print biometric and token.	Developed an ATM based fingerprint verification and simulated it for ATM operations by incorporating the fingerprints of users into the bank‟s database.	1. The system developed was inefficient because there was no finger print matching algorithm. 2. The system developed was not built as an enhancement of the existing system.
Ravikumar, Vaidyanathan, Thamotharan and Ramakrishan (2013	Finger print recognition in digital image processing using both primary and reference fingerprint to authenticate users instead of the traditional pin number	A new business model which would enhance ATM security was proposed.	Another reference fingerprint belonging to a nominee or a close family member was adopted which could also lead to a security breech,thus compromising the security of the account owner. The proposed system was not built on the existing system.
Padmapriyaand Prakasam (2013)	A combination of fingerprint biometric, token and GSM technology	Proposed a system architecture that incorporates both the finger print and GSM technology into the existing PIN-based authentication process.	A nominee or third party's finger print was incorporated in the architecture. There is a discord between the main user and the nominee user in the proposed system architecture

(Source: Muhammad, Alhassan & Ganiyu, 2015)

III. CONCLUSION AND RECOMMENDATION

The paper provides the detailed study on internet banking in Nigeria. It also reviewed authentication methods, weaknesses and security strength in the banking system. Finally, robust authentication scheme needs to be put in place to mitigate series of successful attacks occurring in Nigeria banking system. Therefore in resolving the issues, a new security and authentication model is proposed for implementation in near future.

REFERENCES

[1] Akinola, K. E., Ehiwe, D. D., and Somefun, O. M. (2015): Secured Models for Online Bank Vulnerabilities in Nigeria.IOSR Journal of Mobile Computing & Application (IOSR-JMCA). 3(5). 25-31.

[2] Central Bank of Nigeria: Guidelines on Electronic Banking in Nigeria, August, 2003

[3] Das, S.S. & Debbarma, S.J. (2011). Designing a biometric strategy (fingerprint) measure for enhancing ATM security in Indian e-banking system. International Journal of Information and Communication Technology Research. 1(5). 197-203.

[4] Ibidapo, O. A., Omogbadegun, Z. O, & Oyelami, O.M. (2010). Towards Designing a Biometric Measure for Enhancing ATM Security in Nigeria E-Banking System. International Journal of Electrical & Computer Sciences IJECS-IJENS. 10 (6). 63-68

[5] Janssen, C. (2010). Password Sniffer. Retrieved from Techopedia: http://www.techopedia.com/definition/8798/password-sniffer

[6] Jimoh, R.G. and Babatunde, A. N. (2014). Enhanced Automated Teller Machine using Short Message Service authentication verification. World Academy of Science, Engineering and Technology. International Journal of Computer, Information Science and Engineering. 8(1).14-17.

[7] Muhammad, B.L., Alhassan M.E. &Ganiyu, S.O. (2015). An Enhanced ATM Security System using Second-Level Authentication. International Journal of Computer Applications. 111(5). 8-15.

[8] Nigeria Communication Commission (2017, July 15). Vanguard Newspaper, p. 21. Retrieved from

[9] http://www.vanguardngr.com/2017/07/internet-users-nigeria-now-91m-says-ncc/)

[10] Okereke, E. Ihekweaba, G. & Okpara, F.K. (2013). Facial verification technology for use in ATM transactions. American Journal of Engineering Research (AJER). 2(5). 188-193.

[11] Oko, S. and Oruh, J. (2012): Enhanced ATM security system using biometrics. IJCSI International Journal of Computer Science Issues. 9(5). 352-357.

[12] Padmapriya, V. & Prakasam, S. (2013). Enhancing ATM security using fingerprint and GSM technology. International Journal of Computer Applications. 80(16). 43-46.

[13] Prithika, M. & Rajalakshmi, P. (2013). Card duplication and crime prevention using biometrics. IOSR Journal of Computer Engineering (IOSR-JCE). 10(1). 1-7.

[14] Ravikumar, S., Vaidyanathan, S., Thamotharan, S. & Ramakrishan, S. (2013). A new business model for ATM transaction security using fingerprint recognition. International Journal of Engineering and Technology (IJET). 5(3). 2041-2047.

[15] Roland, J. (2004). CCSP Self-study: Securing Cisco IOS networks (SECUR). Indianapolis, IN: Cisco Press.

[16] Santhi, B. & Ram Kumar, K. (2012). Novel hybrid technology in ATM security using biometrics. Journal of Theoretical and Applied Information Technology. 37(2). 217-223.

[17] Selvaraju, N. & Sekar, G. (2010). A method to improve the security level of ATM banking systems using AES algorithm, International Journal of Computer Applications. 3(6).

BAkinola Kayode E. “Internet Banking In Nigeria: Authentication Methods, Weaknesses and Security Strength.” American Journal of Engineering Research (AJER), vol. 6, no. 9, 2017, pp. 226–231.