International Conference of Science, Engineering & Environmental Technology (ICONSEET), 3(3): 18-22, 2018
ISSN 0794-9650

www.repcomseet.com

Design and Implementation of Two – Way Mobile Authentication System for Banking Operations in Nigeria

Longe O. L[a]., Olatunji A.F[a], Ogunleye T.O[a].
[a]Department of Computer Science Federal Polytechnic, Ede Osun State, Nigeria
E mail: longelawrence@gmail.com

Abstract - This paper deals with software design and implementation of Two-way Mobile Authentication for banking operations in Nigeria (A case study of WAPOG Bank Plc, Osogbo). The system was designed and developed using WAMP stack, HTML, JAVA SCRIPT, PHP, CSS, and FTP. The system used dynamic password technology to obtain higher security guarantee than those used Static Password Technology. The system consists of several pages, among which are the introductory page, and home page. The home page was the gateway to the system operations. Iterative and user-centered design methodologies were adopted. The implementation of this system shows that customers can be authenticated strongly and free from cyber-attacks by generating a one-time password that any bank customer can use as a second factor authentication without any additional hardware called 'Token'. In view of this, it is advisable for the bank management to adopt this system to protect customers and themselves from increasingly sophisticated cyber-attacks.

Keywords: bank management, banking operations, dynamic Password, Cyber-attacks, second factor authentication, Token, Two-way Mobile authentication.

1.0 Introduction

Dynamic password (namely, One Time-Password) technology is a sequence password system and is the only password system proved non-decrypted in theory. Its basic idea is to add uncertain factor in authentication so that users need to provide different messages for authentication each time (Adeoye, 2012). By this way, the applications themselves can obtain higher security guarantee than those that use static password technology (Cryptomathic, 2012). The fact that there is continuous spread of online scams and the reality that people are increasingly wary of online banking channels, raise the stakes for banks to protect customers from increasingly sophisticated cyber attacks. This user friendly system will be able to generate a one-time password that any customer can use as a second factor authentication. This will ensure that users are authenticated strongly and free from cyber attacks (Alain et al., 2005).

1.1 Motivation for the Study

The issue of Cyber attacks in our contemporary banking operations is such that should be of concern to all. Nigerians are increasingly wary of online banking channels due to continuous spread of online scams and cyber attacks. Most of the online banking operations in Nigeria *use Static Password Technology.* There is need to ensure that users are authenticated strongly and free from cyber attacks in Nigeria. This leads to an idea of developing a flexible and users' friendly mobile application to generate dynamic password for online banking operations in Nigeria.

1.2 Aim and Objective

The aim of this research work is to develop a system that will allow users to make secured online transaction without any additional hardware called "Token". The objectives of this research work are:

(a) To develop a user interface that will allow user(s) to interact with the system

(b) To design a support database that will store data for retrieval when the need arises
(c) To develop a cost effective and user friendly authentication system
(d) To avoid the use of a simple username and password system that is not secure

2.0 Literature Review

2.1 Identity theft schemes

In the past years, customers of some world's largest banks have fallen victim to "man-in-the-middle" (MITM), identity theft schemes that have diminished the level of confidence that customers have in regards to online banking (David, 2015). This has affected the reputation of banks. As the term implies, the attackers stood in the middle of customers and banks and listen to all the communication between them, in order to steal account and other personal information (Jenifer, 2012). In one MITM scheme last year involving a large U.S. banking company, the thieves sent seemingly authentic e-mails asking customers to verify their account information. The e-mails directed customers to a spoofed bank website that seemed legitimate but actually redirected the customers to a fake website set up by a hacker in Russia. Due to this, customers who do not feel safe are increasingly steering clear of internet banking sites. The industry research firm, Gartner Inc. estimates that almost 9 million adults in the United States have stopped banking online. Another 23.7 million decline to start out of security concerns. The continual spread of online scams and the reality that people are increasingly wary of online banking channels, raise the stakes for banks to protect customers and themselves from increasingly sophisticated cyber attacks.

Authentication means using one or more mechanisms to prove that the person is who he claims to be. Once the identity of the human or machine is validated, the access can be guaranteed. Mobile authentication refers to wireless-based electronic payment for m-commerce to support point-of-sale/point-of-service (POS) payment transactions Mobile devices (Kuhmonen, 2017). In general, m-payment systems can be used by wireless-based merchants, content vendors and information and services providers to process and support payment transactions driven by wireless-based commerce applications.

2.2 Authentication Factors

There are three universally recognized factors for authentication today (Josang and Sanderud, 2009):
(a) What you know (e.g. password's, pin's)
(b) What you have (e.g. smart cards or tokens)
(c) What you are (e.g. finger prints, face recognition, biometrics, etc)

Two-factor authentication is a mechanism which implements two of the three factors and is therefore considered stronger and more secure than the traditionally implemented one – factor authentication system (Pawar, 2013). Recent work has been done on trying alternative factors such as a fourth factor, e.g. somebody you know, which is based on the notion of vouching. Only recently, two-factor authentication systems based on mobile devices have started to gather some interest within the research community. Authentication mechanism is presented which requires both a Web and a GPRS connection (Saurabh, 2011). The end user enters user id/password details using a web based interface and gets an OTP via short message service on the mobile phone, which must be typed in to grant access to the system (Thigpen, 2005).

2.3 Mobile ID

The Mobile id offers a strong two –way authentication by authenticating the user to the service and service to the user. The mobile Id works in such a way that the user is required to send the code generated by the application after which the Mobile Id generates a code to identify the user with the service (Josang and Sanderud, 2009). Vulnerabilities of mobile devices include: Untrustworthy Interface, Theft or loss of the device, Man-in-the-middle-attacks, etc.

3.0 Methodology

This study has been derived from the implementation of internet. It is mostly used to share and distribute information all over for more efficient operation and reliable results. The design, coding and testing were done in an iterative manner (Roger, 2006).

3.1 Data Collection Technique

The methods adopted in getting all needed information are as follows:

(a) Reading through documents and bank's procedures

(b) Personal interview with relevant players like the users of internet banking and some members of staff of banks operating internet banking

(c) Consulting textbooks, e-books, review of related past research work

(d) Information is also gathered from the internet, from various web-sites.

4.0 Results and Discussion

The major components for the system are Input Design, Output Design, Process Design and Program Design. The tools that are used for this research work are: Hyper Text Markup (HTML), Macromedia Dreamweaver, PHP-WAMP server, My SQL, Macromedia Flash, Macromedia Fireworks and Adobe Photoshop.

4.1 The Model of the System

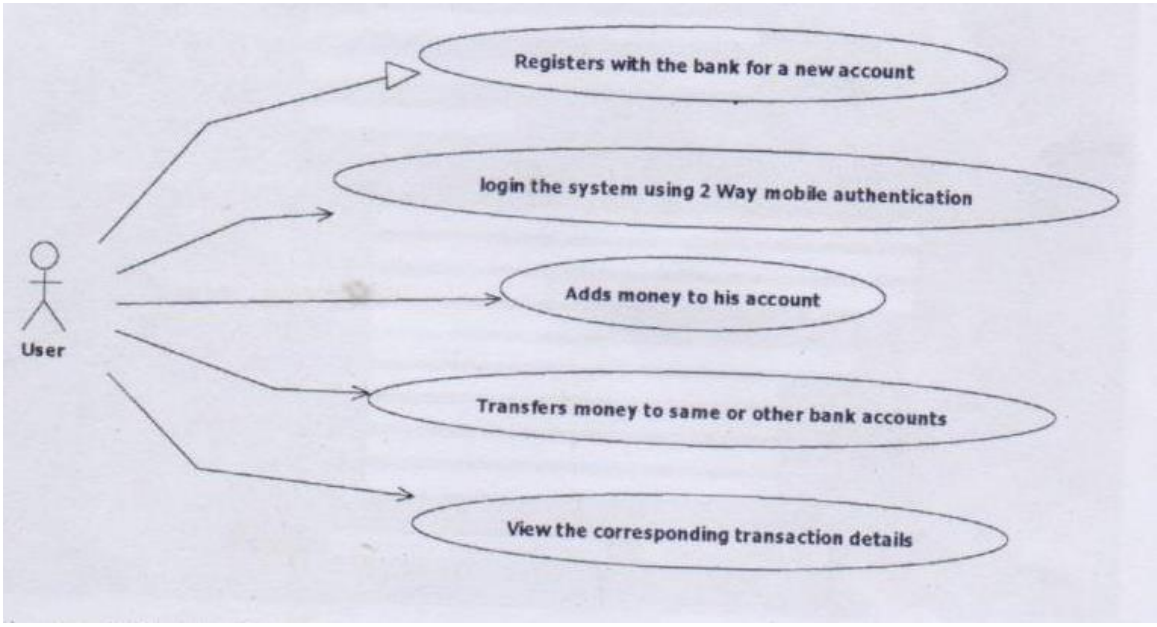

Fig.1: UML Diagram

The first screen is the main page or home page, which points to all other pages on the system. The next page is the input screen for the new user. Others are Transfer processing screen, client information screen and so on. Figures 2 and 3 show the screen shots from the system:

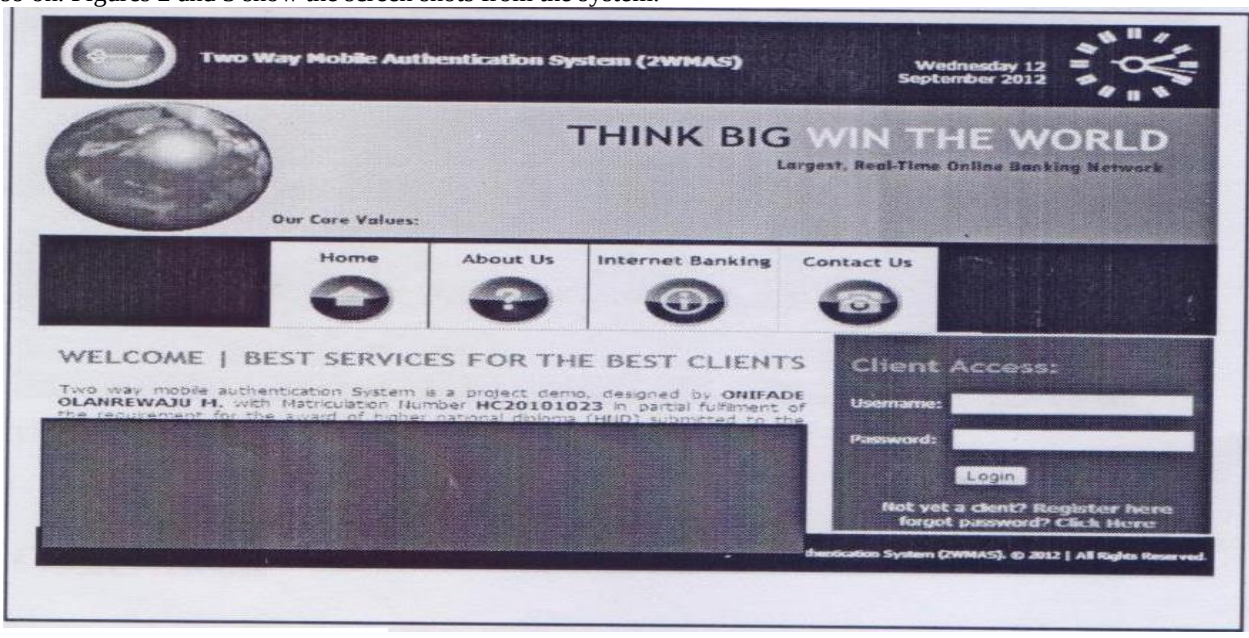

Fig. 2: Screen shot of Main Page

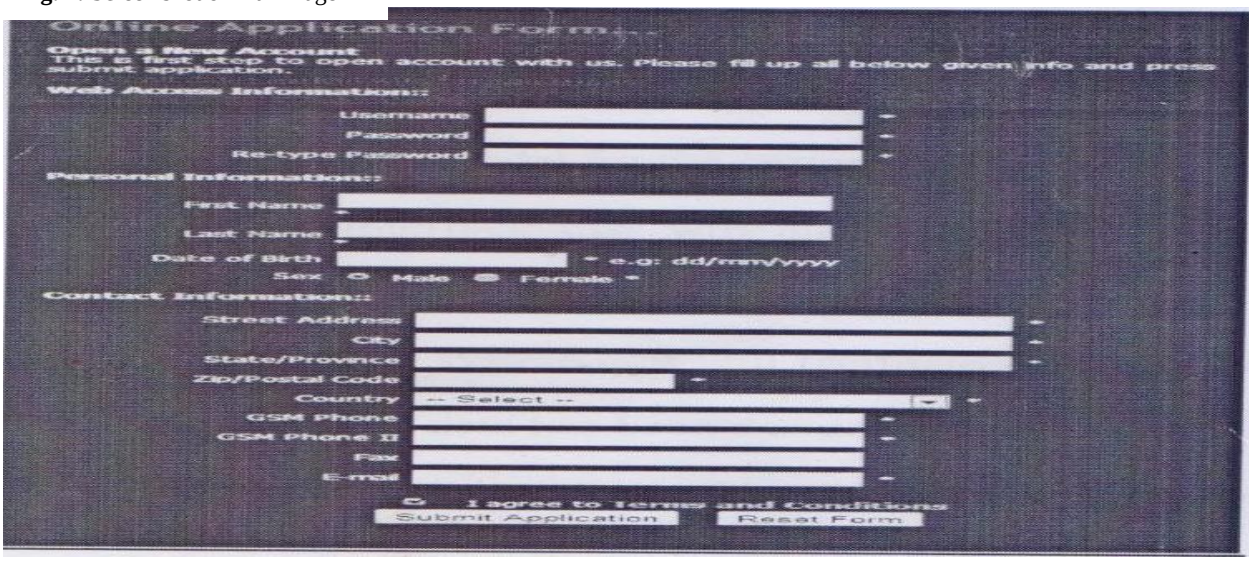

Fig.3: Screen shot of New User Screen

5.0 Conclusion and Recommendations

The study has examined the implementation of Two-Way Mobile Authentication system (2WMAS), for banking operations in Nigeria. In a challenging economy, financial institutions are backbone of industrialization and economic development and they require a secured customer's relationship and financial transactions to achieve their objectives.

To achieve highly secured and reliable online banking transactions in Nigeria, the following recommendations are made:

(a) The management of each of the banking institutions should motivate their IT Unit to review their online banking websites with the view to improve its security procedures.
(b) The banking institutions in Nigeria should adopt dynamic password authentication, like the one implemented in this research work for all their online banking transactions.

References

[1] Adeoye O. S. (2012). Evaluating The Performance Of Two-Factor Authentication Solution In The Banking Sector. [Online]. Available: https://core.ac.uk/download/pdf/25836460.pdf. (Accessed on September, 2017).

[2] Alain H., Thorsten K.,Thomas W. (2005) Secure Internet Banking Authentication. [Online]. Available: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.606.6659&rep=rep1&type=pdf. (Accessed on 1st January, 2018).

[3] Cryptomathic (2012). Two- Factor Authentication for Banking. [Online]. Available: https://cdn2.hubspot.net/hubfs/531679/Documents/White_Papers/Cryptomathic_White_P aper_-_2fa_For_Banking.pdf. (Accessed on 2nd June, 2018).

[4] David L. (2015). Improving Customer Authentication. [Online]. Available: https://www.frbatlanta.org/-/media/documents/rprf/rprf_pubs/improving-customer-authentication.pdf. (Accessed on 7th February, 2017).

[5] Jenifer S.R. (2012). A Five-Ways Fuzzy Authentication for Secured Banking. [Online]. Available: http://www.ijera.com/papers/Vol2_issue4/BG24375379.pdf. (Accessed on 3rd February, 2018).

[6] Josang, A., Sanderud, G., (2009). Securitry in Mobile Communications: Challenge and Oppurtunities. Proceedings of the Australasian information security wokshop conference on ACSW frontiers, 2003.

[7] Kuhmonen S. (2017). One-Time Password Implementation for Two-Factor Authentication. [Online]. Available: http://www.theseus.fi/bitstream/handle/10024/123782/One-Time+Password+Implementation+for+Two- Factor+Authentication.pdf. (Accessed on 14th Decenber, 2017).

[8] Pawar P., Acharya S., Polawar A., Baldawa P., Junghare S. (2013). Internet Banking Two Facto Authentication Using Smartphone. [Online]. Available: https://www.ijser.org/researchpaper/Internet-Banking-Two-Factor- Authentication-Using-Smartphone.pdf. (Accessed on 17th December, 20017).

[9] Saurabh P. (2011). Towards End-to-End Security in Branchless Banking. [Online]. Available:https://www.microsoft.com/en-us/research/wp-content/uploads/2011/05/mbanking-hotmobile-cameraready.pdf. (Accessed on 13th January, 2017).

[10] Thigpen S. (2005). Authentication Methods Used for Banking. [Online]. Availability: http://www.infosecwriters.com/text_resources/pdf/Authentication_Methods_For_Banking.pdf. (Accessed on 4th January, 2017).

[11] Roger, S.P. (2006). Software Engineering: A practitioner's Approach. New York: McGraw Hill, 2005.