https://dx.doi.org/10.4314/johasam.v6i3.11

Examining the Evolutionary Trends of Mobile Banking Platforms in Nigeria

Kelechi Onwe Udu (venkelud88@gmail.com, +2347034437823)
Department of Computer Science, Federal College of Education (Technical) Ekiadolor, Ekiadolor – Benin City, Nigeria.

John Otozi Ugah, *PhD* (ugahjohn@gmail.com, +2348037959012)
Department of Computer Science, Ebonyi State University, Abakaliki, Nigeria.

Loveth Uyinmwen Obaseki (iyohaloveth2251@gmail.com, +2348134245485)
Department of Computer Science, Federal College of Education (Technical) Ekiadolor, Ekiadolor – Benin City, Nigeria.

Abstract

This paper takes a critical review of the evolutionary trend of mobile banking platforms deployed by commercial banks in Nigeria, with the aim to recommend a more secure and robust one. It identifies the strengths and weaknesses of each and highlights the factors that led to the invention of the next succeeding one. The mobile banking platforms reviewed includes Short Messaging Service (SMS), Interactive Voice Response (IVR), Unstructured Supplementary Service Data (USSD), Wireless Application Protocol (WAP), SIM Application Toolkit (SAT), and Application (APP) based platforms. Many of these mobile banking platforms are still utilized by most commercial banks in Nigeria today. However, it is obvious that, although most commercial banks combine two or more of the mobile banking platforms in order to get better result, there are inherent security problems and other challenges in them, which need to be addressed. Having a mobile banking platform (APP-based) with inbuilt ability to confirm a user's authenticity before his transaction is completed, would bring a better security check and thereby bring enhancement to mobile banking transactions. The Application is made more flexible for users by allowing more than one user to use the application to transact once installed in a phone. It is as well equipped with more functionalities like including means for users to: enable/disable their SMS alerts, Change their SMS phone number, Edit their residential address, and Update their next of kin information, as their needs may arise.

Keywords: enhancement, evolutionary trend, mobile banking, platform, transaction.

I. INTRODUCTION

Mobile banking is a platform with which certain banking transactions can be performed from anywhere and at any time using mobile devices basically mobile phones or PDAs (Tiwari, Buse and Herstatt, 2006). The essence of introducing this technology into the banking sector is to make things easier for both banks' customers and staff (Gavin, 2007); such that one must not necessarily visit his bank's local branch before one can successfully perform any transaction. This achievement has gone a long way to increase the interest of several capitalists, industrialists, entrepreneurs, and in fact, all who have anything to do with a bank, to identify with banks that offer such services. They then explore the benefits of the technology since they most times have a lot to do with financial transactions of assorted types. This can be risky, cumbersome or time-wasting if they must have to visit their banks' local branch for all such transactions each time the need arise. Although, there are alternative banking platforms that can be used like Internet Banking (i-banking), ATM, POS, etc, mobile

banking have got numerous and outweighing advantages over all the above and their likes, which cannot in any way be overemphasized (Odumeru, 2013).

There is a daily increasing need for means of payment and financial transaction that would be both safer and more convenient. This can best be achieved by making payments and financial transactions without necessarily involving physical cash. Mobile banking among other platforms like ATM, POS, etc. give a good room for cashless transactions (Odumeru, 2013). Though, there may still be the need to move about with some physical cash, it would be in some rare cases. How be it, it may not need to be much amount of cash. Then, robbers and other criminals would not have wreaked much havoc by intercepting such a cash person. With it, the opportunities of criminals who would always seek chances to rob others of their cash will be reduced. This is because, it requires high level of security breach technologies like hacking, spoofing, Identity Theft to make an attempt (Agwu, 2015). The attempt so made still has tendency of failing, since several security techniques were deployed in the technology. Serious efforts are still being made to heighten and tighten up the security even the more.

Historically, fraudsters have targeted the various payment vehicles (ISACA, 2011), for which mobile banking is not an exception. There have been some reported cases of bank customers incurring some enormous financial losses as a result of some security breaches on their bank account via mobile banking platforms. This is one of the bottlenecks that have watered down the interest of some victims of such frauds and those close and/or dear to them from making use of the mobile banking technology. Of course, it would have eased the banks' staff workload as the banking halls each day get overcrowded with customers seeking one financial transaction or the other physically. It would have as well, brought about convenience and safety on the side of the banks' customers. This paper recommends ways to improve the security of the mobile banking technology by confirming a transaction before it is finally completed. Also by bringing in some new features/functionalities such as means to Enable/disable SMS alerts, Change SMS phone number, Edit residential address, and Update next of kin information.

Confirmation a user's authenticity before completing his transaction is involved here. For instance, at a certain stage in the course of performing a transaction, the system deploys One Time PIN/Password (OTP) technology. This OTP technology is also a good avenue of making the rightful owner of the bank account to know that his account is under attack. He can then contact the bank's customer care unit to help out by taking some immediate security actions. The user may as well decide to immediately change his mobile banking PIN. Mobile Banking has got several platform, which are SMS, IVR, USSD, WAP, SAT and APP-based platforms. Each is to be treated in detail hereunder.

II. EVOLUTIONARY PROGRESSION OF MOBILE BANKING PLATFORM

In this section, the researcher describes the history of mobile banking. It begins with Short Messaging Service (SMS) as a mobile banking platform.

1. Short Messaging Service (SMS) Based Option: This is the first and oldest mobile banking service offered to bank customers since 1997, which banks use to send bank account details to their customers (Tomi and Joe, 2002). Generally, SMS allows users to send/receive text messages on a mobile phone using the numbered keypad on the mobile handset to input characters. SMS mobile banking requires a registered customer to initiate a transaction by sending a Structured Short Messaging Service (SSMS) message to the bank's service provider. For instance, '*bank_balance_PIN*' for balance enquiry; or

'*bank_transfer_current_savings_amount_PIN*' for transfer of a specified amount of money from a user's current account to his savings account.

In each of these examples, the SSMS would be sent using a SMS short address or code (a short phone number) through the GSM Network to the Mobile Network Operators SMS Centre, which stores and forwards the SSMS message to the mobile banking service provider via the SMS gateway allocated to the short address/code. The service provider uses the user's mobile number, forwarded by the SMS Centre with the SSMS message, to identify the user and respond to his request. Initially, SMS option was unidirectional; but much later, the bidirectional SMS-based option was invented.

a. Strengths of SMS Based Mobile Banking Option

i. Simplicity: SMS based mobile banking is the simplest form of mobile banking platform.
ii. Compatibility: It is compatible with all phones (Gavin, 2007).
iii. Download: It requires no download, updating nor pre-configuration for a customer.
iv. Internet Connection: Internet connection is not required for one to use SMS based option.
v. Memory Consumption: It does not take much storage space in the phone memory.

b. Weaknesses of SMS Based Mobile Banking Option

i. Syntax Memorizing: This option has the difficulty of memorizing transactions syntaxes.
ii. Transaction Limits: It is the narrowest in transaction limit per day (Omeye, 2018).
iii. Access to Scammers: It can be manipulated just with a user's PIN (Omeye, 2018).
iv. Limited Functionalities: It has the limitation of enabling just a few functionalities.
v. Transaction Charges: The user is charged both by his bank and his network provider.
vi. Status Check Delays: A transaction's success/failure confirmation may at times delay.
vii. Network Problem: Limited/no mobile network coverage (not internet) hinders its use.

These are the bottlenecks of SMS-based option that led to the invention of the next – IVR.

2. Interactive Voice Response (IVR) Based Option: In telephony, IVR is a phone technology that allows a phone caller to select options from a voice menu and interact with the phone system, just like the initial process of calling in order to speak with a mobile network representative, say MTN (Gavin, 2007). A pre-recorded voice prompt is played and the caller presses a number on a phone keypad to select an option. Speech recognition can also interpret the caller's simple spoken answer such as '*Yes*' or '*No*'; more complex words, sentences and business names, or even a number as a valid response to the voice prompt. IVR requires a registered user to dial a published phone number and be answered by a pre-recorded voice that presents menu options to the user, who in turn, responds. It is session-based and not 'store-and-forward' based as it is in SMS option. In IVR, one is either immediately responded to, within the same session he called, or he is not responded to at all, and that session goes. In such case, the user starts afresh when he wishes to continue with/complete the transaction.

The IVR system takes instructions from the user by recording the tones of the number selected on the keypad or spoken commands, and creates an instruction that is forwarded to the service provider, which uses the user's forwarded phone number to identify him as factor of authentication and to get back to him. IVR based option is one of the old options, now rarely used.

a. Strengths of IVR Based Mobile Banking Option

i. User-friendliness: It is user-friendly, as the user hears and responds to the pre-recorded voice prompts played, especially those who finds it difficult to read (Gavin, 2007).
ii. Compatibility: It is also highly compatible with almost all mobile phones (Omeye, 2018).
iii. Memory Space: No much memory is needed as no application is housed (Omeye, 2018).
iv. No Syntax Memorizing: The voice prompts take care of it (Gavin, 2007).
v. Status Check: The transaction success/failure is instantly known as it is session-based.

b. Weaknesses of IVR Based Mobile Banking Option

i. Cost Intensive: The user spends much money placing the calls. At times, his airtime gets exhausted along the line, making him to loose even the one he has spent fruitlessly (Gavin, 2007).
ii. Vulnerable to Interceptions: It is vulnerable to hackers' interception with the voice call.
iii. Limited Functionalities: It supports only few of the expected mobile banking functionalities.
iv. Complexity: Its complexity emanates from language barrier, unclear voices, etc.
v. Network Problem: Network unavailability or shortage completely encumbers its use.

The above are weaknesses that led to the quest for and invention of the next option – USSD.

3. Unstructured Supplementary Service Data (USSD) Based Option: This is simply a menu-driven form of SMS option, where after initiating his transaction, a customer receives a text menu as opposed to a string of words (Gavin, 2007). A registered bank customer initiates his transaction by dialing the banks published number usually containing asterisks (*) and harsh (#) signs, that is, a bank's published USSD string/code.

Like SMS, it transports small messages between the mobile handset and the network; but unlike SMS' 'store-and-forward', USSD is session-based. USSD is of two forms – USSD1 and USSD2. USSD1 only allows one way communication, but USSD2 allows two ways communication – Duplex Mode, full one, as it can be full or half (Mbam, 2002). With USSD2, the interaction between the user and the service provider would be held in the same session. USSD is available in an estimated 95% of all mobile handsets in the market today according to Gavin (Gavin, 2007). For instance, an Access Bank registered user can dial her published USSD code (*426# or *901#) (Diamond, 2018). The reply can come as shown in Figure 1 below (not in voice form).

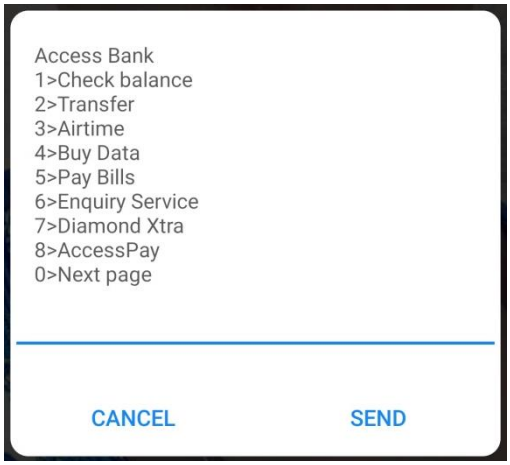

Figure 1: Access Bank USSD Code Initial Response Interface

A user, to whom this interface is presented, is expected to look closely, see the number associated with the transaction of his interest, and type it back into the interface using the provided space. With that, his request is conveyed to the bank's service provider, who in turn, processes the request and gets back to him accordingly. The interface guides the user till completion of his task. More so, the user can still decide to dial the number that will deliver an SMS message for his intended transaction directly to the bank's service provider.

a. Strengths of USSD Based Mobile Banking Option

i. Simplicity: Like SMS option, USSD is a simple option too considering its general nature.
ii. Compatibility: From Gavin (2007), it is compatible with estimated 95% of phones.
iii. No Download: No Download or update, as it is already built into most GSM networks.
iv. Pre-configuration: No pre-configuration is required for a registered bank customer/user.
v. Internet Connection: This is not required. Network provider's service is just enough.
vi. Memory Consumption: It takes only negligible storage space in the phone memory.
vii. Cost Effectiveness: USSD option incurs little/no cost (depending on the bank), as opposed to the first two – SMS and IVR.
viii. Security: The data being transmitted via the USSD channel are encrypted, and so, safe.

b. Weaknesses of USSD Based Mobile Banking Option

i. Transaction Limits: This is faced with limited transactions per day (Diamond, 2018).
ii. Criminals' Chances: It can easily be manipulated if only a criminal access a user's PIN, as there is no other factor of authentication except the PIN (Omeye, 2018).
iii. Functionalities' Limitation: It enables just a few functionalities (Diamond, 2018).
iv. Lack of Completeness: USSD option mostly would still need SMS for its final response (example in account balance inquiry), and so, it lacks completeness on its own.
v. Network Problem: Network unavailability or shortage can bar the use of USSD option.

These are the issues with USSD option that led to the quest for and invention of WAP option.

4. Wireless Application Protocol (WAP) Based Option: WAP is an open international standard for applications that use wireless communication (Gavin, 2007). It is to enable access to the Internet via mobile phones. WAP is now the protocol used for the majority of the world's mobile internet sites, known as WAP sites. WAP sites are websites written in, or dynamically converted to Wireless Mark-up Language (WML) and accessed through the WAP browser via mobile phones. WAP offers the user a similar experience to that of internet banking but utilizes phone instead of computer. The mobile phone and General Packet Radio Service (GPRS) is used to display or transmit the data between the user and the bank.

a. Strengths of WAP Based Mobile Banking Option

i. Syntax Memorization: No Syntax memorizing is associated with this (Gavin, 2007).
ii. Transaction Limit: This option has loose transaction limit per day (Omeye, 2018).
iii. More Functionalities: WAP based option has wider range of transactions it supports.
iv. Cost Effectiveness: Only the multipurpose data for internet connection is required.
v. Ready Balance/Brief Statement: On login, user's balance/brief statement displays.
vi. Security: This option is secure provided the user guards his login details jealously.

b. Weaknesses of WAP Based Mobile Banking Option

i. Internet Connection: There must be internet connection for this to be used (Gavin, 2007).
ii. Pre-configuration: The phone must be properly configured as provided by the MNO.
iii. Downloads: It requires download and updates of the WAP browser.
iv. Memory/Graphic Ability: Needs enough memory/graphic ability to store/display browser.
v. Complexity: It is complex to operate, as less educated fellows may find it difficult to use.
vi. Scammers Chances: Much loss can be incurred if a scammer accesses the user's login details, as the transaction limit per day is loose (Omeye, 2018; Onozure, 2018).
vii. Compatibility: It is incompatible with so many phones, as many of them in the market today cannot take care of the bottlenecks pointed out from numbers (i) to (iv) above here.

These are the limitations that led to the quest for and invention of the next option – SAT.

5. SIM Application Toolkit (SAT) Based Option: SIM Application Toolkit (SAT) also referred to as SIM-Based Application allows for the service provider or bank to house the user's mobile banking menu within the SIM card (Gavin, 2007). SAT consists of a set of commands programmed into the SIM card that defines how the SIM interacts directly with the outside world and initiate commands independent of the handset and the network. This enables the SIM to build up an interactive exchange between a network application and the end user, and control access to the network. The SIM also gives commands to the handset, such as 'display menu' and 'ask for user input'.

If the SIM card already exists in the market, the service provider can either send the application/its updates Over the Air (OTA), which entails the delivery of several encrypted text messages that self-configure the application on the SIM card; or provision new SIM cards with the updated application already embedded in it. Once the application is on the SIM, instructions from the customer can be entered, encrypted, and transported by SMS to the bank or her service provider.

a. Strengths of SAT Based Mobile Banking Option

i. Syntax Memorizing: All platforms using application take care of this, as they display the list of all the possible transactions it can offer in a menu form (Gavin, 2007).
ii. Transaction Limit: It is also loose in terms of transaction limit per day (Omeye, 2018).
iii. Limited Functionalities: It supports wide range of functionalities/transactions.
iv. Security: SAT is secure enough, as the transmitted data are encrypted (Gavin, 2007).
v. Compatibility: It is compatible with all phones, once it can accept and read SIM cards.

b. Weaknesses of SAT Based Mobile Banking Option

i. Updating: It is difficult to update the application, since the SIM cards bearing them are already far away from the service providers. It will cost both parties much (Gavin, 2007).
ii. Memory Space: The application takes a considerable space in the SIM card's memory.
iii. Fixed Storage: The application must be in the SIM card occupying the supposed contacts' space, whereas the device memory or SD card may be spacious enough (Gavin, 2007).
iv. Cost: This option makes user spend a lot in the course of his transactions (Gavin, 2007).
v. Network Problem: Network unavailability or shortage can hinder its use totally.

The above are its weaknesses that led to the quest for and invention of APP-based.

6. Application (APP) Based Option: This is the latest mobile banking platform. It requires a phone that supports the GPRS download of the application and subsequent updating from time to time (Gavin, 2007). The phone also needs to have enough memory/graphic ability to house/display the application when launched – all obtainable in all android phones. Once installed, the application uses GPRS (USSD or SMS for ordinary phones) to carry the user data from the device to the service provider encrypted (Gavin, 2007).

The user browses and finds the application, launches it, and follows the application stepwise directions to complete his transaction. This application can be pushed to the mobile phone by a service provider Over the Air (OTA) or the user can download it by accessing the service provider's/bank's WAP-site or even from the Google Play Store.

According to Gianni and Pier (2015), the services for off-branch banking offered by several banks, show that mobile applications have surpassed the mobile web channel in completeness of the offer, due to the fact that additional capabilities of mobile devices make possible advanced features and applications; serious works are still being done to add more.

a. Strengths of APP Based Mobile Banking Option

i. Syntax Memorization: Not applicable, the application displays all needed (Gavin, 2007).
ii. Transaction Limit: It is the loosest in terms of daily transaction limit (Omeye, 2018).
iii. Limited Functionalities: It has the widest range of functionalities, as it supports all supposed transactions as far as mobile technologies and solutions are concerned.
iv. Security: It is 95% secure as transmitted data are encrypted. It also utilizes many factors of authentication like i-banking ID, PIN, etc (David, 2006; DiamondMobile, 2018).
v. Compatibility: It is compatible with all android phones (bearing in mind that this paper is focusing on enhancement of android application mobile banking option precisely).
vi. Application Updating: It is easy to update the application, just like any other application.
vii. Memory Space: This is not an issue as android phones have enough device/SD memory.
viii. Unfixed Storage Location: The application can reside anywhere accessible to the phone.
ix. Scammers' Chances: Scammers have little or no chance once a user's details are guarded.
x. Cost Effectiveness: This takes care of the cost problems of the earlier options; charges are only at the back end (bank), from the front end, only the multipurpose data is required.

b. Weaknesses of (the Existing) APP Based Mobile Banking Option

i. Network Problem: This is a general issue to all options; APP-based is not an exception.
ii. Internet Connection: This is fully required in Application based mobile banking option.
iii. Complexity: It is really complex, requiring some level of education to operate/use it.
iv. Downloads: It requires downloading, installing and updating the application.
v. Pre-configuration: It requires internet configuration settings; and that for the activation of the application itself, which requires the bank's staff directives (DiamondMobile, 2018).
vi. Security Issue: No alert for the rightful user in case of unauthorized access/login before completing most transactions. Also, the loss will be enormous if a scammer accesses the user's details, as it has the loosest transaction limit per day (Omeye, 2018).
vii. Inflexibility: It is not flexible, as only a user can make use of it (DiamondMobile, 2018).
viii. No means to Enable/Disable SMS Alert: A user cannot enable/disable SMS alert.
ix. No means to Change SMS Alert Phone Number: A related case with No. (viii) above.
x. No means to Update Next of Kin Details: The existing system has no means of this (DiamondMobile, 2018).

The above-shortcomings, especially from numbers (vi) to (x) are the lapses of the existing APP-based option that led to the main objectives of this paper, which seeks to recommend ways of tackling the lapses of the existing system.

III. CHALLENGES OF THE CURRENT SYSTEM

The APP-based mobile banking platform has some challenges associated with it, which are:

i. In case of unauthorized access, the rightful user has no way of being alerted of the inimical activity going on with his account prior to the completion of some transactions.
ii. The system is inflexible; as the installed application is restricted to one person/user.
iii. There is no means with which a user can to enable/disable his SMS alert at will.
iv. The system has no way of a user to change his SMS phone number if the need arises.
v. No means for a user to update his next of kin details without physically visiting his bank.

IV. SOLUTIONS TO THE CHALLENGES

These challenges can be checked using the following approaches:

i. Use of One Time PIN/Password (OTP). This was deployed to alert the rightful user in case a criminal gained access to his bank account prior to the completion of any of his transaction via the user's linked phone number or email (in case of loss of initial SIM card/phone number).
ii. The system was made flexible to allow more than one users use an installed application.
iii. Means of a user to enable/disable his SMS alert at will was included with OTP deployed.
iv. A module for 'Change SMS phone number' if need arises was provided, utilizing OTP.
v. Means of 'Update next of kin details' as need may arise was included, utilizing OTP.

V. CONCLUSION

The evolutionary trend of mobile banking platform, which chronologically includes SMS, IVR, USSD, WAP, SAT and APP based platforms, showed the strengths and weaknesses of each. With closer focus on the android APP based option, the existing system is faced with several challenges. There comes the need for enhancing the option, so as to forestall the outlined weaknesses. The new system has the relative advantages of making banking customers friendly. The services for off-branch banking offered by banks show that mobile applications have surpassed the mobile web channel, due to additional capabilities of mobile devices made possible (Gianni and Pier, 2015). GPRS can be used to improve the security and capabilities of fraud detection according to ISACA (ISACA, 2011).

REFERENCES

Agwu C. O. (2015). The consequences of mobile spam in Nigeria emerging and evolving mobile communication sector of the economy. *International Journal of Advanced Research in Computer Science and Software Engineering*, 5(5), p.119.

David P. (2006). *The Enabling Environment for Mobile Banking in Africa.* Report Commissioned by Department for International Development (DFID) through Bankable Frontier Associates. www.bankablefrontier.com.

Diamond (2018). *Category: *426# USSD – What are the short codes I can use for this service?* http://www.diamondbank.com/bwl-advanced-faq-category/426-ussd/

DiamondMobile (2018). *Diamond Mobile Banking Application for Smartphones – Processes of getting started with the application after downloading.* Customer Care Services Centre – Line: 0700-300-0000.

Gavin T. K. (2007). *Mobile Banking Technology Options: An Overview of the Different Mobile Banking Technology Options, and their Impact on the Mobile Banking Market.*http://www.gsma.com/mobileforedevelopment/wp-content/uploads/2012/06/finmark_mbt_aug_07.pdf.

Gianni, F. & Pier, L. P. (2015). *An Analysis of Features and Tendencies in Mobile Banking Apps.* The 12th International Conference on Mobile Systems and Pervasive Computing (MobiSPC 2015). p.26.

ISACA (2011). *Mobile Payments: Risk, Security and Assurance Issues.* An ISACA Emerging Technology White Paper, www.isaca.org.

Mbam, B. C. E. (2002). *Information technology and management information system: technical, practical and skilled approaches.* Our Saviour

Odumeru, J. A. (2013). Going cashless: Adoption of mobile banking in Nigeria. *Arabian Journal of Business and Management Review (Nigerian Chapter)* 1(2), 9 -12.

Omeye, K. (2018). *A detailed review of all the mobile banking platforms from the oldest to the latest pointing out the shortcomings of each.* An Oral Interview with him, a Diamond Bank Plc Staff on Tuesday, April 10, 2018.

Onozure, D. (June 8, 2018). *28-yr-old man hacks into bank's app, steals N207m. Vanguard News*. https://www.vanguardngr.com/2018/06/28-yr-old-man-hacks-banks-app-steals-n207m/amp/.

Tiwari, R., Buse, S. & Herstatt, C. (2006). *Mobile banking as business strategy: Impact of mobile technologies on customer behaviour and its implications for banks*. Proceedings of PICMET '06 Published Technology Management for the Global Future. https://ieeexplore.ieee.org/document/4077590/

Tomi, A. & Joe, B. (2002). *Services for UMTS: Creating killer applications in 3g - history of mobile banking.* John Wiley. http://www.tomiahonem.com/s4u.html.