Development of an Enhanced Mobile Banking Security: Multi-Factor Authentication Approach

[1]Ndunagu, J.N., [2]Nwoduh U.J
[1]National Open University of Nigeria
[2]Federal Polytechnic, Nekede, Owerri

[1]jndunagu@Noun.Edu.Ng
[2]udofifa2@Yahoo.Com

Abstract
Technology has played a significant role on how we work, play and interact. The future of finance is not left out in the emerging technological wave rapidly disrupting conventional modes of operation. Banking transactions can now be done via the web and mobile applications. With these new and innovative self banking applications, there has been an increase in cases of identity theft. This paper focuses on the development of a highly secure mobile banking platform to check mobile device identity authentication vulnerabilities. The study presents a framework to overcome the limitations of authentication models for mobile banking applications. This means banks will need to handle fraud detection using a more secure multi-factor approach. Banks that provide a secure and frictionless mobile banking experience will be rewarded with happier customers. The methodology adopted is structured system analysis and design. The software development tools used include Android Integrated Studio 2.2, XML, Java JDK and SQ lite. The new application of multifactor authentication built on smart biometrics can bridge the gap between usability and security to create a frictionless mobile banking experience.

Keywords: Mobile banking, security, multifactor, authentication

1.0 Introduction

Banking transaction is changing; technology and a major push for innovation are bringing new and exciting ways to perform financial transactions. Mobile banking is an aspect of financial technology that enable customers have virtual access to banking halls from any location at any time. This is made possible through the use of the internet. Almost all financial institutions (if not all) now offer banking services via the web. Some institutions have taken a step further to develop mobile banking applications as well. Financial institutions seeking to remain competitive and keep customer satisfaction high must offer mobile access to their customer base as it provides banks with avenues and opportunities to reach geographically remote or rural markets, to focus on new markets and overcome infrastructure limitations and improve efficiency, to access payment system or simply to retain market share. However, with these new opportunities come challenges. Top of the list is checking fraud and identity theft or simply put, how can banks verify genuine mobile banking application users?

The focus of this paper is developing a mobile application that reduces incidents of identity theft.

Mobile banking is defined as the execution of banking services and transactions using a mobile device, such as telephone or tablet [1]. It also defined as a facility which provides banking services such as balance enquiry, funds transfer, bill payment, and transaction history via a user's mobile phone [2]. Unlike some other bank transactions, mobile banking is done without the need for a human teller or cashier. It provides access to the most popular banking services such as viewing account balances, paying bills, transferring funds and checking rates. Other major services provided through mobile banking are inquiries like account statement, checking status transaction, recharging of telephone lines.

Access to mobile banking is dependent on telecommunication networks especially the Global System of Mobile communication (GSM). Mobile banking is clearly a leading new channel in the space of banking and payments in today's world. This system of banking is fast becoming popular among many bank users most probably because of its ubiquity (seeming

presence everywhere), accessibility at all times and high number of mobile devices' users worldwide. Reports have it that the estimated number of mobile phone users globally as at 2014 is about 4.55 billion and the number is likely to reach 5.13 billion users by 2017 [3]. A Report by the Nigerian Communications Commission [4] shows that Nigeria has about 93 million users of mobile phone; representing 16% of the continent's total mobile subscriptions. The figure is increasing both in Nigeria and other countries as the year passes though at different pace depending on the country and the economy.

As users of mobile banking continues to increase across the globe, some factors prominent among them being technical and security standards has continued to be a major source of concern for many users. Almost all mobile banking services are open 24 hours a day with minimal security features for user authentication. Security concerns are cited by a large group of consumers as an inhibitor to the adoption of mobile banking services [1]. Currently, one of the most widely used authentication system obtainable in most Nigeria mobile banking cloud is the use of passwords or PIN (Personal Identification Number). However, these methods of authentication are often compromised as cases are bound where fraudsters transfer funds from individual accounts without the knowledge of the account users. Also cases has been recorded where account holders were deceived to giving out their password or PIN through phishing schemes. Moreover passwords and PIN can be guessed or stolen.

IBM Security Trusteer Research found that there is an increase in the number of mobile fraud toolkits offered for sale in underground forums which are able to steal customers' banking login credentials, inject fake messages, such as request for login credentials and credit card information, gain administrative privilege on the device, which effectively blocks attempts to remove the malware [5]. There are some other challenges and security risks faced by banks, solution providers and mobile operators in the implementation of mobile banking and payments. Some of identified key risks to the mobile banking and generally use of mobile devices according to Pegueros include: Malware, Malicious applications, Privacy violations relative to application collection and distribution of data, Wireless carrier infrastructure, Payments infrastructure /ecosystem, SMS vulnerabilities. Others are Hardware and Operating System vulnerabilities, Complex supply chain and new entrants into the mobile ecosystem and lack of maturity of fraud tools and controls [6]. Most of these risk factors like other computing devices depend largely on the mobile device, network service providers and application in use. The security risks associated with mobile devices are very similar to any other computing device with the few key exceptions:

i. Mobile devices have a smaller form factor and therefore are more susceptible to loss or theft.
ii. Mobile devices are more personal and there will be a tendency for users to use devices in a more personal and confidential way.
iii. Security controls and tools available have not matured to accommodate the constraints of limited processing power and limited battery life [6].

Mitigating most of these challenges require comprehensive approach that will ensure continued customer trust on mobile services. Efforts have been made by many researches to come up with solutions in this regard. Organisations delivering banking services on mobile devices currently face difficult choices over the right solution in terms of security standards considering business objectives, proliferation security vendors and their own capability [1].

This study presented a framework to help overcome some of the identified security challenges as it relates to user authentication through development of software that provides efficient and reliable identity authentication for mobile banking transactions at different levels using multi-factor authentication.

2.0 Literature Review

2.1 Concepts of Authentication

An authentication is a proof provided by an entity (claimant) to affirm to a monitor that he/she really corresponds to the identity he/she

provided. The monitor then matches the proof provided with existing identity of the user. Finally, the authorization is granted to the user if the credential matches the user identity [7].

Similarly authentication is defined as a security measure designed to verify or validate the identity of a user or station prior to granting access to resources. Authentication mechanisms include passwords and intelligent tokens [8].

In the context of computer systems, "authentication" is the process that ensures and confirms a user's identity. It begins when a user tries to access information. The user must first prove his access rights and identity. When logging into a computer, users normally enter usernames and passwords for authentication purposes. The login combination which must be assigned to each user authenticates access [9].

In other words, when an entity or a party tries to have access to information or perform some transaction, there is need to identify and ascertain that the user has a valid right to the information or transaction. The process of proving the identity and access right of the intended user is what is referred to as authentication.

2.1.1 Authentication Techniques

Rouse M, opines that the three most common categories of authentication factors are knowledge factors ("what the user knows") information that user must be able to provide in order to log in, such as a user names or IDs, passwords, PINs, secret questions etc; possession factors ("what the user has") anything a user must have in their possession in order to log in, such as SIM card, one-time password, security token etc and Inherent factors ("what the user is") any biological traits the user has that are confirmed for login, such as retina scans, fingerprint, facial recognition, voice, iris pattern etc) [10] [11].

Types of Authentication include:

(a) Single Factor Authentication

Single factor authentication is a process for securing access to given system, such as network or website that identifies the party requesting access through only one category of credentials [11]. Most single factor authentication uses what the user know such as password, secret questions, identifiable pictures etc. That doesn't mean there is only one thing to enter to prove one's identity. A good example of this is the secret questions where you may have 10 questions to answer; it's all just single factor authentication [10].

(b) Multi-factor Authentication

Multi-factor authentication is a method of user identification that combines a number of authentication factors. This type of authentication is often used for priority customer information and high risk financial transactions. [11]. This definition is corroborated another scholar who defined Multifactor authentication as a security system that requires more than one method of authentication from independent categories of credentials to verify the user's identity for a login or other transactions. [13]

Based on the above definitions, one can say that multi-factor authentication is an authentication technique in computer access control that a user has to present more than one category of authentication credentials to login or perform transaction. It can come in the form of two-factor authentication or three-factor authentication.

Two-factor authentication which is a sub category of Multi-factor authentication is an extra layer of security that requires not only a password and username but also something that only and only that user has (posses) on them. Using username and password with a piece of token that only the user has makes it harder for potential intruders to gain access and steal that person's personal data or identity [12]. Most two-factor authentication systems make use something the user has (possesses) in addition to what the user knows such as a swipe card.

Three-factor authentication on its own part combines of the three types of authentications mentioned earlier, i.e. what the user knows, what the user has and what the user is. In other words three factor authentication in addition to the previous two factors mostly used in two-factor authentication also uses 'what a user is' such as biometric characteristics. One major drawback

of multi-factor authentication is that new hardware token needs to be ordered and issued. This can take time and cause problems for a company's customers waiting to gain access to their own private data via this authentication procedure [12].

2.2 Security Issues in Mobile Banking

One of the most challenging security issues in mobile banking is user authentication. The technique of authentication currently used by mobile banking applications is perceived by customers as not being secure of enough to instil confidence as rising cases of identity theft and invasion of privacy in no way help to alleviate such negative perception. Some of the key issues that lead to security breaches have been identified. Previous studies suggest solutions like physical protection of mobile devices, security of applications from vulnerability threats, authentication of bank's customers and device, use of secure service providers, encryption of data for both transmission and storage.

Security checks are put in place to verify specific customer actions, and necessarily depend on the authentication, integrity and confidentiality of customer credentials and identity, as well as the content stored on the device itself. Other critical drivers affecting mobile security strategy and architecture are online and digital identity providers; payment providers and dis-intermediaries; banking and mobile platforms and services [1].

2.2.1 Mitigation of Security Issues in Mobile Banking

In an attempt to tackle the security issues, many research analysts have contributed their quota of ideas on how to solve these issues. According to Mobile Marketing Associate (2009), the following are ways of addressing some of the security issues associated with mobile banking:

1. **Data Transmission must be secured:** in this case, the term "secure" addresses mainly the concept of confidentiality and therefore requires encryption of the connection between the device and the bank.
2. **Application and Data Access must be controlled:** Before users can receive any sensitive information related to their bank accounts, a certain degree of verification must be completed. Ideally, the combination of several authentication factors and the possibility of challenging the user in case of a (potential) security breach should be part of the procedure.
3. **Data Integrity must be provided:** Any critical data stored on the mobile device must be protected against unauthorized modification. The issue of possible corruption and deletion error of sensitive information should also be addressed.
4. **Loss of Device must have limited impact:** the mobile banking service should be structured in a way that has little to no negative effect in the event of an unfortunate occurrence of the loss/theft of a customer's mobile banking device. For example the feature embedded in the software client that prevents a lost/stolen device from accessing customers account. Such features also contribute to creating a reliable banking experience and the assurance can lead to mobile banking users. [14].

Other methods used to mitigate security in mobile banking are as follows;

Usernames and Passwords

The idea here is that a mobile banking user possesses a unique identifier such as a customer ID. He also has a secret phrase that is paired with the identifier. When the user authenticates, he provides his unique identifier and provides his secret password. Using passwords for authentication is a simple idea. Assign a unique identifier to a user and instruct that user to supply a password to correlate to that identifier. Its administration is also pretty simple. Almost all computer systems have built-in applications to handle passwords. The user identifiers and passwords can be stored in a database allowing the entire process to be completed with the user as the only source of human input [15].

Passwords are the most common form of authentication used to control access to information ranging from credit cards to more

complex alphanumeric passwords that protect access to files, computers and network servers. They are widely used because they are simple, inexpensive and convenient mechanisms to use implement. [16]

The flaw in this type of authentication is that it can easily be compromised. Username and password combinations have a fundamental inadequacy stemming from human psychology. Passwords should be easy to remember and easy enough to provide swift authentication [15]. On the other hand, in terms of security the password should be difficult to guess, changed from time to time, and unique to a single account.

Below are some obvious weaknesses of password authentication:

- Password may be easy to guess.
- Some passwords could be written and placed in a highly visible area which could have negative impact.
- Discovering passwords by eavesdropping or even social engineering. [17].

2.2.2 One-Time Password

A one-time password list makes use of lists of passwords which are sequentially used by the person wanting to access a system. The values are generated so that it is very hard to calculate the next value from the previously presented values [17]. This is a bit similar to the basic username and password combination except that the password never travels through the public network. The system uses a client side generator and a server. Basically, the generator accepts a secret password from the user and concatenates it with information sent from the server in control of the authentication. Various computations and hashes are performed on the user's secret password which can be verified by computations by each end of the communication [15]. It is important to keep in mind that Password systems only authenticate the connecting party. It does not provide the connecting party with any method of authenticating the system they are accessing, so it is vulnerable to spoofing or a man-in-middle attack [17]

2.2.3 Personal Identification Number (PIN)

PIN is a multi-digit number that is used by somebody to gain access to an account at an ATM, a computer, or a telephone system. It is numerical in format and like a password should be kept secret [18]. The most common use of the PIN is for Automated Teller Machines (ATM) [15]. Benefits of use of PIN includes provision of access to multiple types of network systems and websites; facilitating information privacy management, while preventing unauthorized access due to loss of credit/debit cards or usernames/password [9].

Most financial PINs are 4-digit numbers in the range 0000-9999 resulting in 10,000 possible numbers. This means that an attacker would need to guess an average of 5000 times to get the correct PIN. However, it may take a matter of seconds for computer to work out. That is why most systems implementing PIN authentication has predetermined number of times a user can attempt to login [19].

3.0 Methodology

System design presents a conceptual design of the new system including processes, data models, identified requirements and expectations of the system users.

3.1 Analysis of the Existing System

The analysis was mainly based on the existing system as obtainable in Diamond Bank Nigeria Plc which was used as case study, however, similar systems obtainable in other commercial banks in Nigeria were also studied to have a comprehensive analysis and proffer a good design for the new system.

Based on the data collected and reviewed, below is a summary of how the current system operates. The focal point of this description is on operations or activities that relate to security of the system, user identification and authentication.

3.1.1 Services Offered Through Mobile Banking

Services offered through mobile banking vary among banks and the type of account one

operates. As a minimum most mobile banking platform enables users to check account balance, view SMS based transaction statement and transfer funds to accounts within the same bank. However some platforms offers more services like transfer of funds across banks, payment of bills (such as utility bills and taxes), information services (like checking rates and share prices), and purchase of airtime, movie tickets and flight tickets.

Depending on the bank, banking services are offered through java based application, mobile web browsers and native platforms like Andriod, Windows, and BlackBerry. Most mobile apps can be downloaded from any of the major app stores such as Google play, Apple store, Windows app store. However, some banks offer mobile banking services through mobile web browsers. In the case of the mobile web browsers, the user will need to type in the bank's web address into the address bar and submit in order to log on. When this is done, the device will automatically be directed to a mobile version of the site if the mobile device is compatible.

3.1.2 Requirements for registering and using mobile banking

The requirements for registering and using mobile banking may vary among different banks. However some requirements are basic to all banks. An intending user need to have an account with the bank, online user ID (Internet Banking ID), a payment card (such as Credit, ATM/Debit card) from the bank, and Registration code which is sent to a user's registered phone number after the first authentication stage.

3.1.3 Steps for registering or activating mobile banking

1. Input online user ID (Internet Banking User ID) and bank account numbers then select submit. A registration code will be generated and sent to your registered phone number as an SMS.
2. Enter the registration code sent to your phone number
3. Choose a password (not less than six characters) which you will use to access this service at anytime, reconfirm the password.
4. Choose a four digit pin for transactions, reconfirm the pin
5. Select confirm

Alternatively

1. Enter 16 digit Debit card number and account number then select submit. An online user ID and registration code will be generated and sent to users registered phone number as an SMS.
2. Input the online User ID and registration code.
3. Choose a password (not less than six characters) which will be used to access this service at anytime, reconfirm password;
4. choose a 4digit pin for transactions, reconfirm pin and select confirm

3.1.4 How to login and use mobile banking channel

1. Open the mobile App in your mobile device
2. Click on Sign In.
3. Input your online user ID and password then submit.
4. You will have access to the various services available on the channel.

3.1.5 Findings and Drawbacks of Existing System

Findings from the analysis carried out on the current system of mobile banking as operated by Diamond Bank Nigeria Plc and most banks in Nigeria identified the following as the drawbacks associated with user identity and authentication:

(i) Passwords and PINs are the only line of Authentication Available

In the current system, the use of Passwords and PINs are the major line of authentication available to users. This type of authentication can be easily compromised using social engineering processes or guessed correctly by an unauthorized user to

gain access to one's bank account. Also authentic users can forget their passwords or PIN.

(ii) Slow Channels of Blocking Transactions by Customers

A lost or stolen mobile device with an installed mobile banking application does cause worry for the customer. Banks cannot tell when a mobile device has been compromised except when the genuine owner of the device and bank account notifies the bank. The owner would have to contact the bank's customer service centre (telephone line or email address. These channels may be laborious and sluggish for the customers as the unfortunate situation requires a swift resolution. Sometimes customer care lines are busy attending to other incoming calls.

(iii) Lack of multi-factor authentication

Presently, the only authentication mobile banking in Nigeria requires is the provision of username and password (Single factor). Multifactor Authentication is a better alternative as it is more secure. The current use of username and password could be compromised as some users tend to write their credential or save it where another person can access it.

As a result of these drawbacks, it is discovered that:

(i) A large number of people still prefer to have their money secured rather than having their time secured at the expenses of their money.

(ii) Most literates and persons below the age of 50 are hesitant to use Mobile banking applications as they do have reservations about the security of the application.

(iii) There is a lack of awareness and understanding of how to use these modern gadgets. This also contributes to the decline in mobile banking usage.

(iv) Multifactor authentication can cause a bit of delay as the part of the many reasons people use mobile banking in the first place is the speedy service delivery.

3.2 System Design

A viable alternative to the existing system as proposed by this study is the development of improved security application for mobile banking. The aim is to have an application that can provide efficient and reliable identity authentication for mobile banking transactions at different levels using a combination of many techniques. The proposed system will use multi-factor authentication system while the database will be secured using cryptography. Using the same resources available to the bank and the customers, the new system will handle suitably all identified problems in the existing system. Described below are the elements, features and specification of the new system.

3.2.1 Description of the new system

The new application is designed to support secured and time independent communication and collaboration between the bank and the customers. The aim is to have an application that can provide efficient and reliable identity authentication for mobile banking transactions at different levels using multi-factor authentication. The system will help both the bank and the customers solve most security issues relating to identity theft and user authentication. Specifically the system will do the following:

i) Create information account for the users.

ii) Generate login pin for users

iii) Allow users select authentication levels.

iv) Allow users perform transactions like fund transfer, bill payment, view balance statement and change pin with reliable authentication using one time pin and answer to secret question.

v) Generate and send transaction pins to users for each transaction which is sent to the alternate phone number other rather than line phone in which the App is installed is used for authenticating the transaction.

vi) Secure user information through encryption of records in the database.

It will be designed specifically for installation in mobile devices with android platform. The strength of the new system is its ability to allow

user chose levels of authentication factor and to generate and send one time transaction token to the user's alternate number for all sensitive transactions rather than the phone in which the App is installed. The transaction token can be pin, image or secret answer to secret question in a case of transaction exceeding a particular amount to be stated by the user at the point of registration or having more than three transactions in a day. This is to avoid situations where stolen or lost mobile devices can be used to perform sensitive transactions. Figure 1 below is a context diagram of the new system showing how the new system works and relationship that exist between the major components of the new system.

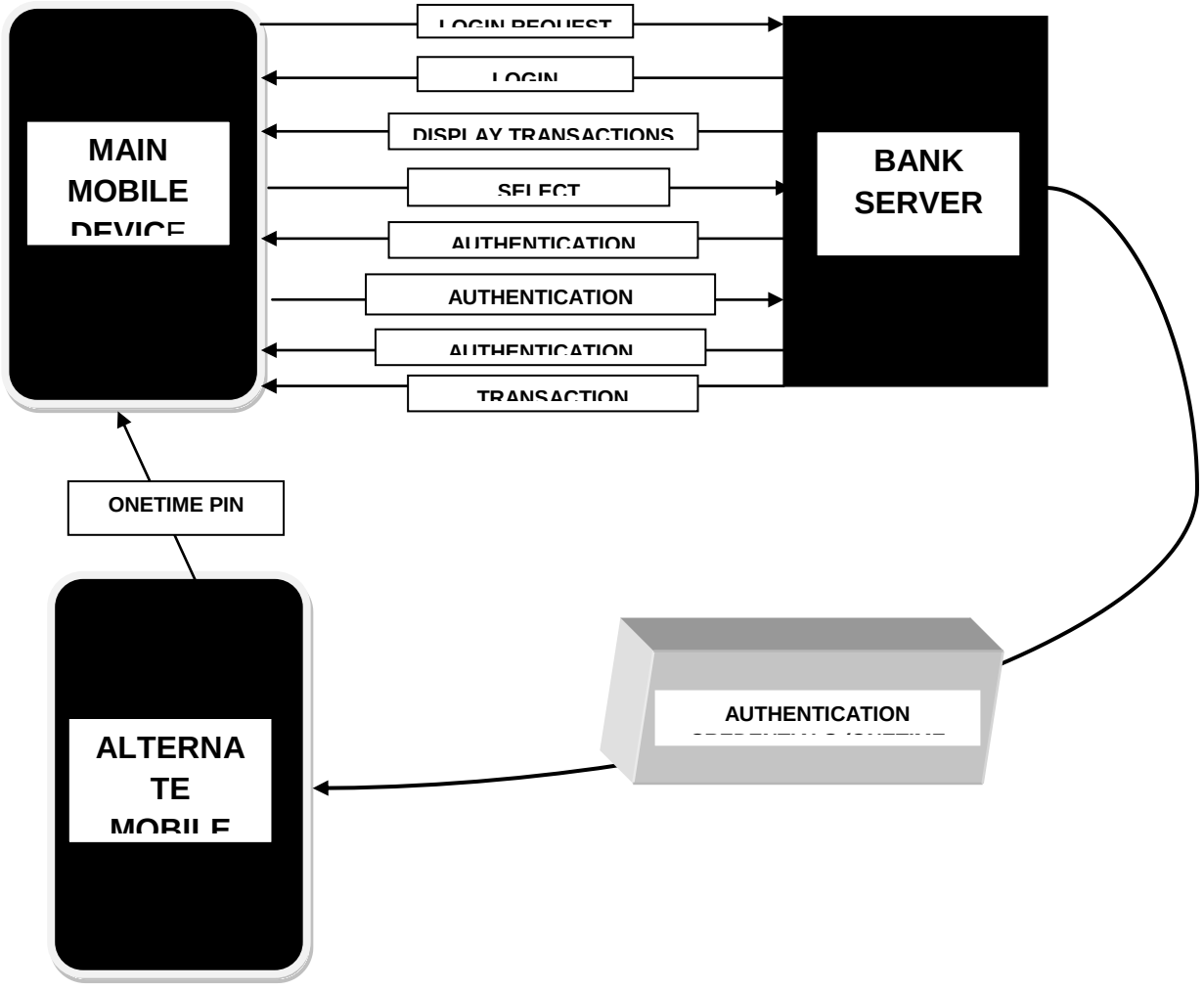

Figure 1: Context diagram for the new system

Software Modules Modularity is the ability of a system to be broken into identifiable sub-tasks. Each identifiable sub-task forms a module which can be coded differently and later linked to the main system. This approach helps to limit the task of debugging and maintenance to each module rather than looking at the whole system. Hence the new system is divided into the following modules:

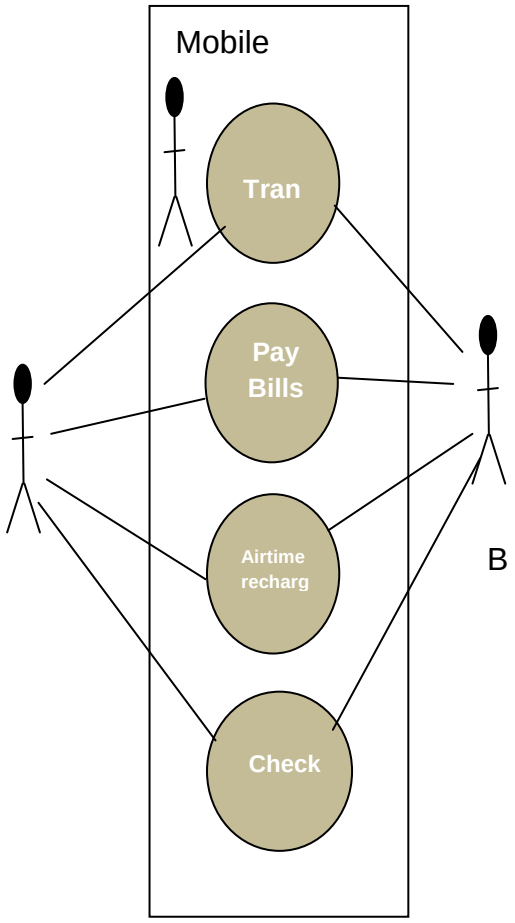

Figure 2: Use Case Diagram of the new system

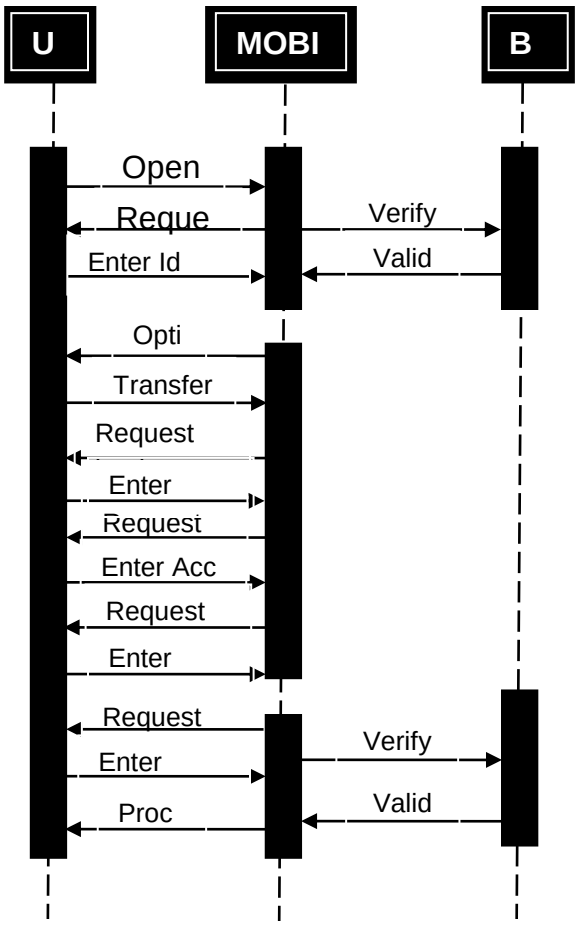

Figure 3: Sequence diagram for transfer of funds

4.0 Discussion of Result

The discussion here centers on the key implementation factors and the security features of the new software. In the new application, the key security features are the multi-factor authentication provided through the use of onetime pin and the two mobile devices used for transactions. Each of the security features are discussed in details as:

4.1 Multi-Factor Authentication

The new software application combines knowledge and possession authentication techniques together which makes it multi-factor. The knowledge authentication (that is "what the user knows") used in this software is username and password while the possession authentication which is "what the user posses" is

the one time PIN generated for each transaction. Each of these techniques individually provides good security however the combination of the two techniques provides an even better security against guessing, man in the middle attack and other forms of social engineering attack while still maintaining the simplicity and affordability of implementation (which is the main reason for use of single factor authentication)

4.2 Two Mobile Phones/Devices

The two mobile phones required in this new scheme for authentication ensures secured authentication in event of loss or theft. This is because the onetime PIN required to complete a transaction will not be sent to the same stolen or lost phone. This technique ensures that only an authorized user initiates and completes a transaction. The advantage here is that it is secured and yet inexpensive to implement when compared to most multi-factor authentication techniques that requires hardware for processing of biometric data or use cards. Moreover most mobile devices used in this part of the world do not have the necessary resources to process biometric data.

5.0 References

[1] KPMG. (2015). *Mobile Banking 2015: Global Trends and theirImpacts on Bank.* Retrieved from www.kpmg.com/UK/en/IssuesAndInsights/ArticlesPublication/Documents/PDF/Marketsector/financialServices/kpmg-global-mobile-banking-report-july-2015.pdf

[2] Quick, C. (2009). *With Smartphone adoption on the rise, opportunity for marketers is calling, nielsenwire*. Retrieved December 12, 2011, from http://blog.nielsen.com/nielsenwire/online_mobile/with-smatphone-adoption-on-the-rise-opportunity-for-marketers-is-calling/

[3] Anshul, S. (2014). *2 Billion Smartphone users by 2015: 83% of Interent usage from mobiles.* Retrieved November 19, 2015, from https://dazeinfo.com/2014/01/23/smartphone-users-growth-mobile-internet-2014-2017

[4] NCC (Nigerian Telecommunication Commission). (2013, March 29). *Industry Data.* Retrieved from www.ncc.gov.ng

[5] Bach, D. (2001). BITS Sets New Guidelines to help wireless banking. American Banker.

[6] Pegueros, V. (2012). Security of mobile banking and payments. Sans Institute Reading Room.

[7] Syed, Z. S., Estelle, C., Rosenberger, C., & Schwartzmann, J.-J. (2013). A review on Authentication Methods. Australian Journal of Basic and Applied Sciences.

[8] Webster's New World Telecom Dictionary Online. (2010). Retrieved 11 26, 2015, from www.yourdictionary.com/authentication.html

[9] Technopedia. (2015). *Multi-factor-authentication*. Retrieved from www.technopedia.com/13657/multi-factor-authentication-mfa

[10] Myers, L. (2012). *What is Multi-factor authentication and how will it change in future*. Retrieved 11 25, 2015, from www.intego.com/mac-security-blog/topic/multi-factor-authentication

[11] Kim, J., & Hong, S. (2011). *A Method of Risk Assessment for Multi-Factor Authentication.Journal of Information Processing Systems* (Vol. 7).

[12] Securenvoy. (2014). *An extra layer of security that is known as multifactor authentication*. Retrieved from www.securenvoy.com./two-factor-authentication/what-is2fa.shtm

[13] Securenvoy. (2014). *An extra layer of security that is known as multifactor authentication*. Retrieved from www.securenvoy.com./two-factor-authentication/what-is2fa.shtm

[14] Mobile Marketing Association. (2009). *Mobile Banking Overview.* Retrieved from www.mmaglobal.com/files/mbankingoverview.pdf

[15] Thigpen, S. (2012). *Authentication methods used for Banking.* Carolina: East Carolina University USA.

[16] Kessler, G. (1996). *Passwords-Strenghts and Weaknesses*. Retrieved from https://www.researchgate.net/publication/266038051_PASSWORDS_-_Strengths_and_Weaknesses

[17] Duncan, R. (2001). *An Overview of Different Authentication Methods and Protocols.* SANS Institute of InfoSec Reading Room.

[18] Microsoft Encarta Dictionary. (2009). Personal Identification Number. Redmond, WA, USA: Microsoft Corporation.

[19] Cayan Insights. (2010, December 10). Retrieved November 26, 2015, from https://cayan.com/glossary/personal-identification-number