Journal of Science and Technology Research

Journal homepage: www.nipesjournals.org.ng

Improved Recognition System for Mobile Transactions in Banking Industries

[1*]**Adekunle M. Ibrahim, [1]Oyeyemi Oyebode**
[1]Department of ICT, Osun State University, Nigeria
Corresponding Authors Email: [*]kunle_ibrahim2001@yahoo.com, fempeg2013@gmail.com

Article Info

Abstract

In recent times, mobile banking has emerged as a winner among various banking services. Security has been the major concern since present authentication methods in most banking industries do not offer high level of security. There is always a risk of fraudulent attacks where criminals hack into people's private data and steal or damage their personal resources. Although conventional methods have helped to reduce the rate of fraud, but this is not enough since cyber criminals can bypass this approach by installing malware or another harmful virus on peoples' devices. In order to avoid this risk, reliable authentication procedures to improve authentication system to protect mobile devices and personal investments in banking industries must be adopted. In this research work, a robust interface that can be used to process most banking transactions through mobile devices has been designed with some improved security measures. Several algorithmic steps were involved in developing this system by studying the characteristic features of people's voice for easy detection and recognition. In order to authorize users into the system, a matching algorithm has been implemented to confirm account owners before any transaction can be made. The result recorded in this work confirms that mobile baking transactions with improved security measures that can make life difficult for criminals can be achieved. The developed interfaces are user friendly, fast, reliable and efficient. If banks can integrate this approach of mobile banking with the current wireless technology, it would go a long way in solving the challenges facing our banking industries today.

1.   Introduction

There are some unique challenges facing mobile banking. One of the problems is how fraud can be prevented in our society. Banks must ensure that transactions requests are made through authorized mobile users. Mobile Banking [1-3] plays a key role in our economy and has become an integral part of our lives. Currently, mobile users can also perform some basic banking transactions like checking balances, paying bills, and transferring money from anywhere anytime and of course you can also top up your mobile line via your mobile phones. The major concerns of existing papers on mobile and Internet banking are centred primarily on mobile banking and payment technologies as well as determinants of customer adoption of mobile banking service [4]. [4] points out that there has been no study on the relationship between mobile banking and payment services. According to our recent search, the only exceptions are in [5], comparing traditional and mobile payments, and [6], discussing economic and policy issues related to mobile payments based on various economic theories. Mobile banking has emerged as a winner among different banking services in today's

world. Its security is the major concern for banking transactions [7]. Since existing authentication techniques such as passwords do not provide a high degree of protection over our activities in banking. In [8], banking transactions by mobile devices such as phones or tablets are referred to as mobile banking. It is a safer digital alternative to Internet banking. The amount of passwords that people have to handle is becoming a serious problem as the world becomes increasingly more interactive. Reasonable biometric alternatives for authenticating mobile banking need to be explored by financial institutions. As a result, businesses and government consultants are increasingly devoted to creating more convenient and safe ways of accessing information, enabling people to digitally organise their lives without the fear of fraud [9]. In [10], the authors focus on developing mobile banking system and security where most technology options in mobile devices today can allow a variety of choices when implementing. Mobile banking is attractive because it is a convenient approach to perform remote banking, but there are security shortfalls in the present mobile banking implementations. Information technology (IT) has become an effective tool for economic and social growth in contemporary life [1].

In most banks today, long queuing has become the order of the day, customers would have to line up for hours to get things done. This creates a lot of problem for both customers as they waste their useful time in banking hall [11-13]. The management also wastes their time as they run around to find solution to those problems. Also it is observed that customers cannot withdraw money at the appropriate time since banks have their working hours. This is a big problem as needs can arise at any time and human beings will always like to have those needs solved. Also money deposited into accounts at times takes some hours to reflect in the account balance hence making banking operations slow and unhealthy for business growth. One of the biggest problems facing mobile banking today is the issue of trust and security. The vast majority of consumers are concerned about the safety of their credit card and personal details. People simply do not trust the Web, fearing that their transactions might not be safe. Apart from this, the prospect of online banking fraud has adverse effect on potential online shoppers. According to the literature, our traditional way of banking today has got one problem or the other in terms of getting loans, withdrawing money and other transactions. Most banks are struggling to achieve a better environment to eliminate these problems. This research work is all about how this can be improved. It is all about how a mobile phone can be used to perform most banking transactions without physically going through the banks. This can be processed in such a way that customers can access their bank accounts anywhere and have total control over their money. One does not need to have Internet connection; a mobile connection is all that is required. This study is aimed at enhancing accurate security in banking system to authenticate users using something more personal than other unwanted features. With the current technologies in our banking today, criminals can forge your username and password; he/she can access your account and get away with your money. However, it would be very difficult to gain access into somebody's account if a recognition system has been implemented with the user's voice. Apart from improving this security issue, this research work proposes to design and implement a robust recognition system that would drastically reduce the cost and time of visiting banks using machine learning techniques. In other words, some of the research questions that would be addressed in this project are: Can improved Recognition system be effectively used for mobile banking transaction? How can we use this system to solve the existing problems in our banking system?

2. Methodology

This section explains the approach methodology and environment for building a voice recognition system. It focuses on the algorithms and flowcharts for building a recognition system that could be used to resolve security issues in banking. The procedures for achieving this goal involve several algorithmic steps as presented in Figure 1.
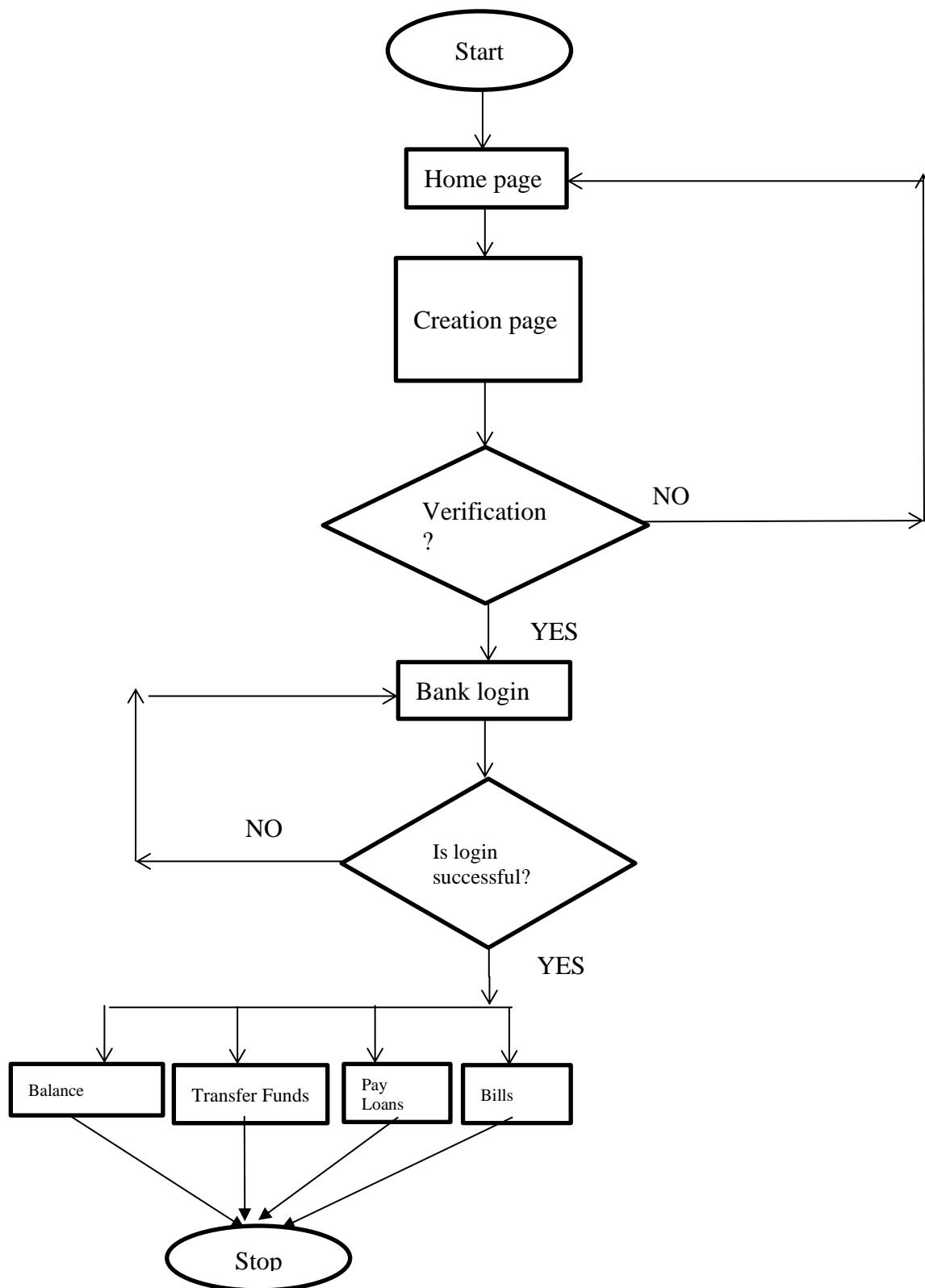
Figure 1: Overview of machine learning techniques

This diagrammatic representation illustrates steps or procedures for designing solutions to address some of the problems facing mobile banking. The flowchart system as presented in Figure 1 involves different modules of banking application where users can log into the application and input their details. Subsequently, the login details is verified and if the login details are correct it takes the user to the dashboard for further transactions but if the details are not correct it will decline it and takes the user back to login. If user has successfully login to the dashboard of the banking application, then the user can proceed to other transactions and user can log out when he/she is done. The following algorithms can be used for implementing each of the modules outlined in the flowchart presented in Figure 1.

A. Algorithm to Create Login Interface

Let voice recognition= v
Let new voice= j
   Let saved voice = k
   initialize v (v = 0)
   if j = k
       allow user to login
           proceed to mobile banking system
       enable banking transactions
   end
else: Do not allow login
initialize voice again
end

B. Algorithm to Perform Loan

Let voice recognition= v
Let new voice= j
Let saved voice =k
   initialize v (v = 0)
if j= k
allow user to login
proceed to mobile banking system
enable banking transactions
proceed to loan
initialize loan
enable amount of loan
finalize loan
end

C. Algorithm to Initiate Transfer

Let voice recognition= v

Let new voice= j

Let saved voice =k

initialize v (v = 0)

if j= k

allow user to login

proceed to mobile banking system

enable banking transactions

proceed to transfer

initiate transfer

enter transfer details

finalize transfer

end

D. Algorithm to Check Account Balance

Let voice recognition= v

Let new voice= j

Let saved voice =k

initialize v (v = 0)

if j= k

allow user to login

proceed to mobile banking system

enable banking transactions

proceed to account balance

click on account balance to view balance

end

3.   Results and Discussion

The implementation phase of this project was carried out using android studio IDE, java programming language was used as the programming language for developing the recognition system with a firebase server as the online database server for the project. Figure 2 shows the screen shot of the system splash screen that uses voice to welcome the user into the mobile application.

Voice Bank
A mobile voice banking application
Developed by Oyeyemi Oyebode
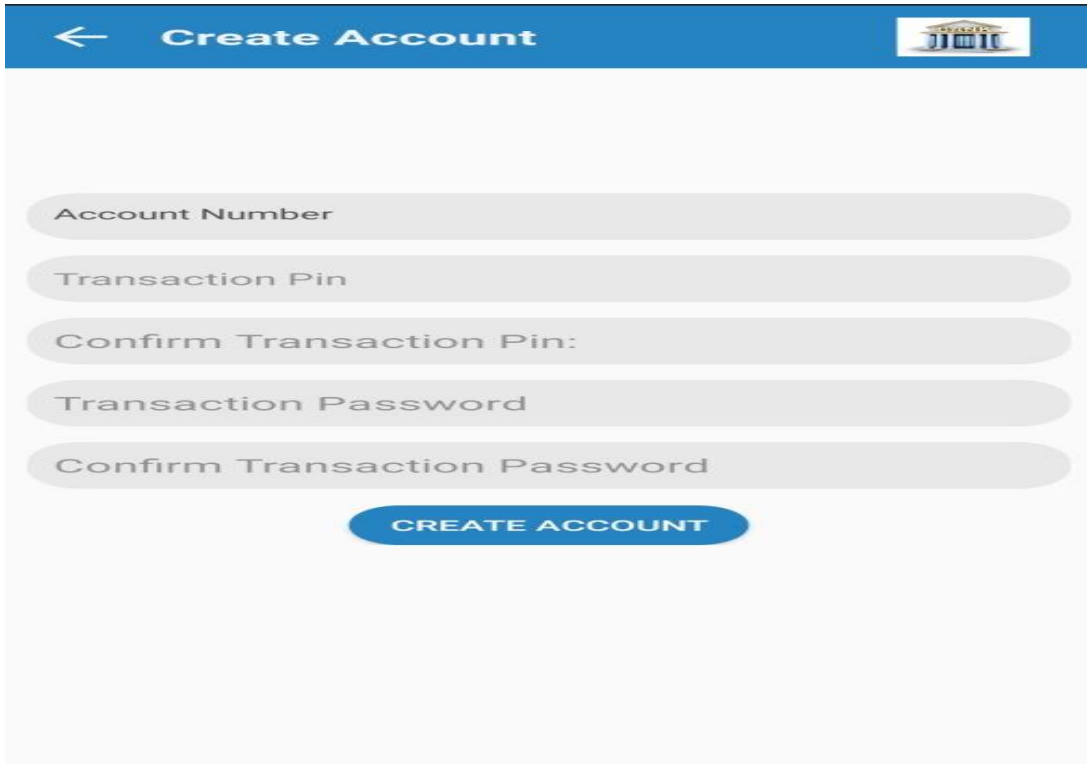Matric Number: CSC/2016/0046
Supervised by Dr. M.A Ibrahim

Figure 2: Home pages for mobile banking transactions

Figure 2 is the home page of the mobile banking application. It shows little information before the user's login into their account; it represents the screen shot of the system splash screen that uses voice to welcome the user into the mobile application. This is the page where the users are being welcomed to the mobile application. Figure 3 is the phone number verification page where the user can input his/her phone number that was used during registration and a transaction pin will be automatically sent to the number which will be inputted in the account creation page.
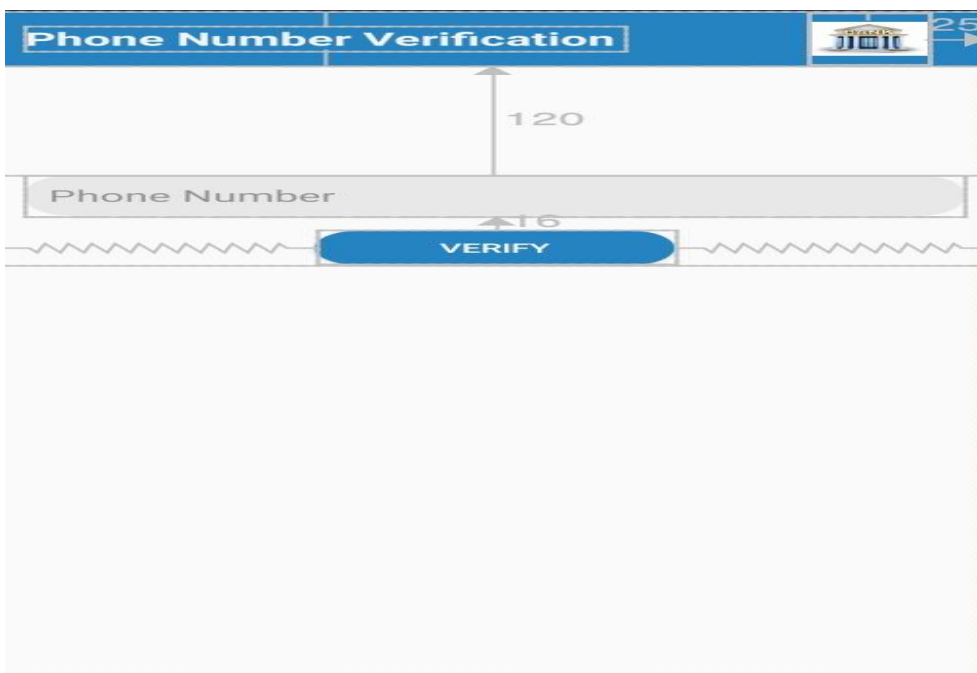
Figure 3: phone number verification page

The phone number tab that is in the snapshot below (Figure 3) is where the user can input his/her registered phone number that was used in opening the account and generate the transaction pin but If the phone number is not properly registered with the bank, the system would not send the transaction pin to the number provided. The user can also create account page as shown in Figure 4, where the user can input the transaction pin into the phone number provided with the appropriate password to generate the security word page. Once the phone number used in the registration page is verified, the account number will automatically come up on the account number tab in the creation page. It is important to go through this creation page process because the user would not be able to perform any transaction on the dash board without it.

Figure 4: create account page for transactions

The dashboard presented in Figure 5 is where all the transaction pages appear. It consists of the transfer page, loan page, bill page and balance page. Transfer page as can be seen in Figure 5 is where transfer can be made to another account, the loan page is where user can take loans, bill page is where user can pay cable bills online and the balance page is where user can check account balance.

Figure 5: Dashboard page for activating bank transactions

`Through the dashboard presented in Figure 5, the user can perform all banking transactions virtually without visiting the bank.

4.   Conclusion

This paper has successfully presented a recognition system with some levels of security that can make life difficult for hackers or criminals in our society. Most of the issues of concern in banking today have been practically addressed in this paper. The knowledge of machine learning techniques with some programming skills has been used to develop and improve on the existing methods to perform most banking transactions on mobile devices. Analysis and extraction of voice features that cannot be easily hacked by unauthorized users can help to take the security measures in our society to another level. The developed interface would go a long way in reducing the long queues that usually result during pick periods in our banks. In addition, the integration of the e-banking voice functionality will also assist the visually impaired, the aged and the pensioners to perform their banking transactions at suitable locations without physically going to the bank premises or using the ATM stand. Finally, the adoption of the product of this research in banking operations will offer a good contribution for banks and other financial institutions in providing better customer services thereby increasing the liquidity flow among individuals, small and medium scale companies, as well as big organisations, within a growing economy such as Nigeria.

References
[1]   S.L Choon, S.S. Hyung, and S.K. Dae (2004). A classification of mobile business models and its applications.   Industrial Management and Data System. Vol. 104, No. 1, pp.78–87.
[2]   M. Durkin, B. Howcroft., A. O'donnell, and D. Quinn (2003). Retail bank customer preferences: personal and remote interactions. International Journal of Retail and Distribution Management. Vol. 31, No. 4, pp.177–189.
[3]   T. Laukkanen (2006). Customer perceived value of financial services: a means-end approach. International Journal of Finance. Vol. 1, No. 1, pp.5–17.
[4]   Z. C. Abaenewe, O.M. Ogbulu and M.O. Ndugbu (2013). Electronic banking and bank performance in Nigeria. West African Journal of Industrial and Academic Research,Vol. 6,No. 1, pp. 171-187.
[5]   H. Karjaluoto (2002). Selection criteria for a mode of bill payment: Empirical investigation among Finnish bank customers. International Journal of Retail and Distribution Management. Vol. 30, No. 6, pp. 331–339.

[6]   T.Dahlberg, N. Mallat, J. Ondrus and A. Zmijewska (2008). Past, present and future of mobile payments research: a literature review. *Electronic Commerce Research and Applications*. Vol. 7, pp. 165-181.

[7]   S. Schwiderski-Grosche, and H. Knospe (2002). Secure mobile commerce, Journal of Electronics & Communication Engineering. Vol. 14, No. 5, pp. 228-238.

[8]   S. H. Choi, and S. G. Chang (2006). Digital convergence and the evolution of business governance: an exploratory study of the Korean mobile banking industry. *Telecommunications Review*. Vol. 16, No. 1, pp.102-113.

[9]   J. Bughin (2004). "Attack or convert?": early evidence from European on-line banking. *Omega*. Vol. 32, pp. 1-7.

[10]   S. Y. Chian (2012). Factors affecting individuals to adopt mobile banking: Empirical evidence from the UTAUT model. *Journal of Electronic Commerce Research,*   Vol. 13, No.   2, pp. 104-121.

[11]   A.A. Shaikh and H. Karjaluoto (2015). "Mobile Banking adoption", Telematics and Informatics, vol. 32, pp. 129-142.

[12]   C. M. Matei and C.I. Silvestru (2008). Internet Banking Integration within the Banking System. Integration the VLSI Journal. Vol. 2, No 2, 55-59.

[13]   M. Suoranta and M. Matilla (2003). Mobile banking and consumer behavior: new insights into the diffusion pattern. Journal of Financial Services Marketing. Vol. 8, No. 4, pp.354–356