IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 10, Issue 3 (Mar. - Apr. 2013), PP 51-59
www.iosrjournals.org

Secure Authentication for Mobile Banking Using Facial Recognition

Falaye Adeyinka Adesuyi[1], Osho Oluwafemi[2],
Alabi Isiaq Oludare[3] , Adama Ndako Victor[4] and Amanambu Victor Rick[5]
[1]*Department of Mathematics and Statistics, Federal University of Technology, Minna, Niger State, Nigeria*
[2]*Department of Cyber Security Science, Federal University of Technology, Minna, Niger State, Nigeria*
[3]*Department of Information and Media Technology, Federal University of Technology, Minna, Niger State, Nigeria*
[4]*Directorate for Collaboration, Affliation and Linkages, Federal University of Technology, Minna, Niger State, Nigeria*

[5]*Department of Mathematics and Statistics, Federal University of Technology, Minna, Niger State, Nigeria*

ABSTRACT: *THE CURRENT SYSTEM OF MOBILE BANKING IN NIGERIA CONSISTS OF TWO WAY AUTHENTICATION (USERNAME AND PASSWORD) WHICH CAN BE FORGOTTEN OR STOLEN. THIS PAPER PROPOSES A SECURE AUTHENTICATION FOR MOBILE BANKING USING FACIAL RECOGNITION TO THE EFFECT OF IMPROVING ON THE EXISTING SYSTEM, AND THEREBY SUPPORTING THE ACTUALIZATION OF CASHLESS SOCIETY. AN OVERVIEW AND LIMITATIONS OF THE CURRENT SYSTEM ARE PRESENTED. THE HIGH LEVEL DESIGNS OF THE PROPOSED SYSTEM ARE THEN PRESENTED. THE SYSTEM IS THEN SIMULATED USING JAVA PROGRAMMING LANGUAGE AND TESTED USING SIMULATED DATABASES OF NIGERIA COMMUNICATION COMMISSIONS (NCC) AND THE FACILITATING BANK. THE SYSTEM WAS FOUND TO PERFORM WITH A MAXIMUM RESPONSE TIME OF SEVEN MINUTES, AND FALSE ACCEPTANCE RATE (FAR) OF 3%. COMBINING THIS SYSTEM WITH ONE OR MORE OTHER FORMS OF BIOMETRIC TECHNOLOGIES SUCH AS FINGER VEIN, IRIS AMONG OTHERS WILL NO DOUBT GIVE A FRAUD PROOF PLATFORM FOR MOBILE PHONE BANKING.*

KEYWORDS: *MOBILE BANKING, SECURITY, AUTHENTICATION, CASHLESS SOCIETY*

I. INTRODUCTION

In the past decades, banking was done inside the banking hall which was tasking to both the customers and the bankers. The long queues, paper-based data and even the time taken to perform even the smallest transaction can be an uphill task. This has now been a thing of the past since the advent of the internet and mobile phones. The Nigerian system of banking has evolved and following the trend as obtainable in the western world. The number of online banking users has increased in Nigeria and indeed the world; this has led to many experts in mobile banking software and mobile phone technology to research new and convenient methods for customers to perform banking transactions remotely via their mobile phones. Mobile banking is also known as mobile phone bank. It is referred to as the using mobile phone for banking related business [1]. It offers convenience for customers to perform transactions. Its utilization is expected to increase as the cashless society gets more hold in Nigeria vis-à-vis the fact that number of mobile phones users is also increasing. At the moment Nigerian banks like GTB and Access bank provide mobile banking through SMS (Short Messaging Service) using the WIG (Wireless Internet Gateway) and the WAP (Wireless Application Protocol) over GPRS (General Packet Radio Service).

Security has become a primary concern in order to provide protected mobile transaction between the clients and the bank servers. Secure authentication of client information depends on some fundamental security approaches which will not jeopardize the client sensitive information. This has led to different researches ranging from single-factor authentication, two-way authentication, and multifactor authentication. Bearing in mind the cost of providing these services to clients, most banks are weary of balancing profit making and security. In Nigeria today, most mobile banking applications use the single-factor authentication which consist of the username and password.

Mobile authentication can be the glue that binds together online banking, mobile banking and mobile payments in a way that couples security with convenience [2]. The single-factor authentication is prone to attacks, in cases of theft or perceived trusted third parties, the security can be breached with ease. Password hackers can easily break the security since most passwords are weak. Some customers using the online banking system in Nigeria have experienced unauthorized access to their banking information and, in some cases, unauthorized withdrawal from their accounts. Secure mobile banking will build confidence in customers knowing that their information is secure and they can carry out secure transactions without fear of man-in-the-

middle attacks. Though the issue of theft strongly depends on how a client protects his/her mobile phone device from third parties.

The future of Nigerian banking is mobile, due to the availability of mobile phones to remote customers in the villages, towns and places where banks or ATMs are not in close reach for customers. The proposed cashless society in Nigeria will propel this future as fast as possible for Nigeria to be recognized among world players in financial and technological innovations. Based on the facts above, we have tried to improve on the present security levels on mobile phone banking in Nigeria.

II. Literature Review

2.1. Mobile Banking

Mobile Banking simply involves performing banking transactions via a mobile device. Advancement in mobile technology, over time, has dictated the nature of transactions that can be performed. Beginning from services delivered only through SMS [3], today high-level transactions, including third-party transfer, bill payment, to mention but two, can be conveniently performed from the comfort of a phone.

According to [4], there are three main methods employable for performing transactions and accessing other banking services via a mobile phone. These include the Short Message Service (SMS), mobile web, and mobile client application. Summarized below is the performance level of each technology, considering some basic properties.

Table 1. Comparision Between Different Types Of Mobile Banking Architectures Table.

Types	Ubiquity	Ease of UI	Affordabilty	Security	Rich App
SMS	Strong	Strong	Strong	Weak	Poor
Mobile Web	Moderate	Moderate	Moderate	Moderate	Weak
Mobile Client App	Poor	Good	Moderate	Strong	Strong

2.2. Authentication

It simply connotes the verification of a user's identity, before access is granted. It is an access control mechanism that often precedes authorization, and its implementation is based on one or a combination of three factors: what you have (these includes debit card, smart card), what you know (these include passwords, usernames or pin numbers), and what you are **(**these requires biometric such as retina, fingerprints, facial recognition etc) [5].

2.3. Biometrics

Biometric technology is a means of automatically authenticating a person by traits, that is, based on what the person is. This includes fingerprints, hand geometry, signature, retina, iris, voice, thermal imaging etc [6]. Usually, a person's biometric data is acquired. The values of some defined parameters of the acquired data are then compared with those previously acquired and domiciled in the database [7].

The characteristics used in grading different biometrics are: universality, uniqueness, permanence, collectability, performance, acceptance and circumvention. For instance, considering one of the available biometrics, face, we have the assessment below [8].

Table 2. Grading one of the available biometrics, face.

Biometrics	Universality	Uniqueness	Permanence	Collectability	Performance	Acceptence	Circumvention
Face	High	Low	Medium	High	Low	High	Low

III. Statement Of The Problem

Nigeria has over 120 million mobile subscribers [9]. It can be expected that a percentage of this population, considering the government penchant for a cashless society, would embrace the mobile banking option. From a survey carried out by [10], 20% of respondents revealed they employ mobile banking platform. Though, the level of mobile banking adoption in the country is still relatively young, many of the banks currently provide mobile banking platforms for customers [10]. From observations, the platforms provided by these banks require only username and password to gain access.

Considering the fact that no system is perfect, mobile banking, like every other type of banking like ATM, credit card, mobile money, despite its immense benefits, is also not immune to security challenges. Yet, there is need for the available platforms to effectively control application and data access [11], hence the need for multi-factor level of authentication. This is necessary to encourage customers to embrace mobile banking.

According to Nigeria Deposit Insurance Commission (NDIC) report on electronic and related frauds for the quarter end of 2008 the incidence of frauds in banks maintained an upward surge. A typical example is the bank-wide increase in cases of ATM fraud. This is in spite of efforts by interswitch and member banks to raise awareness [12].

In 2008, the Economic and Financial Crimes Commission reports ranked Nigeria as the third among top ten source of electronic related fraud in the world. A society like Nigeria would be engulfed by electronic fraud if the system is not checked. These cases and statistics mentioned above have prompt the need to develop a secured mobile banking platform. This is also in line with the Central Bank's drive for a cashless society.

IV. Overview Of The Current System

The analysis of the current system will help determine the feasibility of the system. Since the advent of mobile banking in Nigeria, the major goal of software designers has been to make mobile banking more secure for end users. Achieving this goal however, has been met with many challenges.

For instance, Access Bank, one of the leading banks in the country, uses only the popular username and password level of security (2-way authentication) which poses a level of security that cannot stand the test of time. The features provided by the platform allow for account operations, like fund transfer, checking of balance, bill payments. Also, it provides functionality for account administration. With such features, a security level higher than the 2-way authentication is needed to provide optimum security to curb scam/theft on users' account.

4.1. Problem Identification of the Current System

i. 2-Way Authentication consists of Username and password only.
ii. Poor level of security.
iii. It is easy for hackers to breach into the account.
iv. It is possible for hackers to clone the SIM card.
v. When SIM card is cloned, the bank server will assume the hacker as the authentic user.
vi. Prone to unauthorized access by perceived third parties.
vii. In case of theft, mobile phone can be hacked into, whilst the bank server would allow access into the account assuming the hacker to be the authentic user.

V. OVERVIEW OF THE PROPOSED SYSTEM

The proposed system is expected to provide higher level of authentication (multifactor authentication) which will bring unauthorized access to the barest minimum. Before access will be granted, the user will have to take a facial photograph to have access to his/her account, the geometry of the face, distance of the eyes and the nose is compared. This photograph will be compared with the photograph in the bank server and the NCC server for verification, if it passes the verification, access will be granted, otherwise it will denied. In the event of unauthorized access, a security alert message will be sent to the bank.

5.1. Advantages of the Proposed System

i. High security level.
ii. Facial recognition of user.
iii. Verification is compared within the NCC and bank server.
iv. Theft message alert is sent to the bank server.
v. It guarantees physical location of the user.
vi. The biometric trait is unforgettable.
vii. The biometric trait cannot be lost.
viii. The biometric trait cannot be shared.
ix. It can provide emergency identification
x. It prevents identity theft.

VI. SYSTEM COMPONENTS

6.1. New Account Creation

New users using the application for the first time can create a new account by filling out a form that includes his/her name, sex, occupation, address, passport photograph, phone number, secret question and answer. These details will be used when a new session is started.

6.2. New Session

A session starts when a customer logs in his/her username and password and takes a facial photograph. If it matches the corresponding image in the NCC and bank databases, the customer is then allowed to proceed

to select a transaction he/she wishes to perform from the menu of possible transactions in each case. A session is aborted when invalid entries exceed five trials. An intruder alert message will be sent to security operatives.

6.3. Transaction

Before any transaction is started, every level of authentication must be obliged. At this level, transaction is securely carried out either in form of fund transfer, bill payment, to mention but two.

6.4. Database Design

MySQL was used as the database because it is relational, cost effective, quick and powerful as well as compatible.

VII. System Architecture Design

7.1. Entity Relationship Diagram

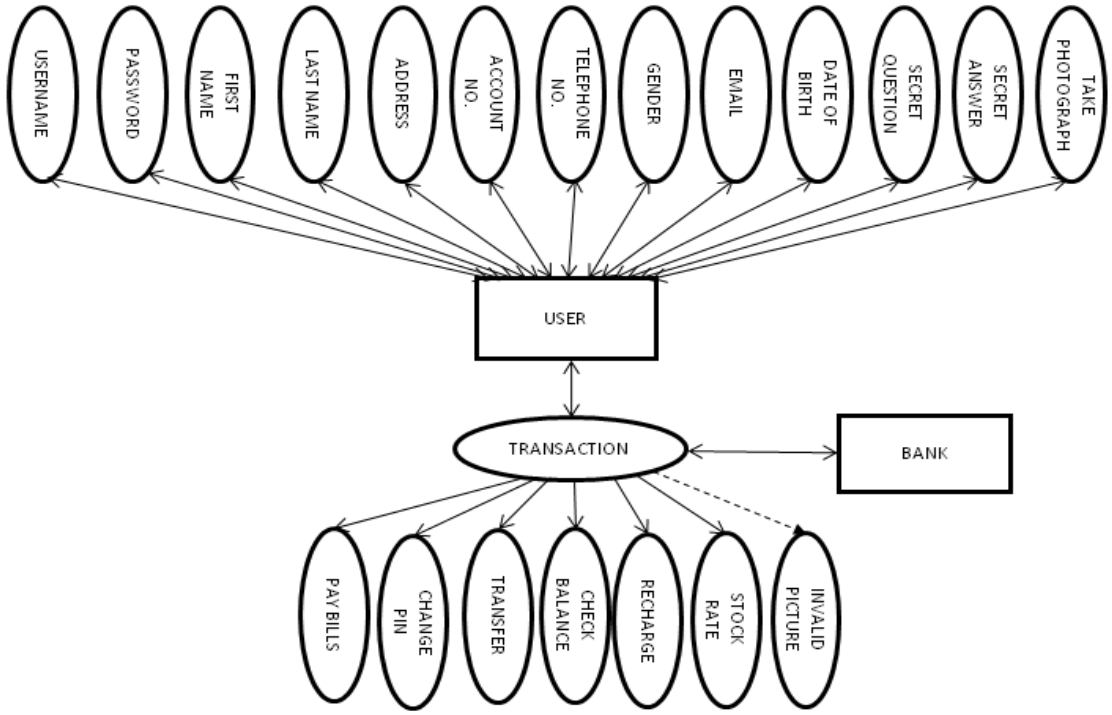

Figure 1. UML diagram of proposed system

7.2. Class Diagram

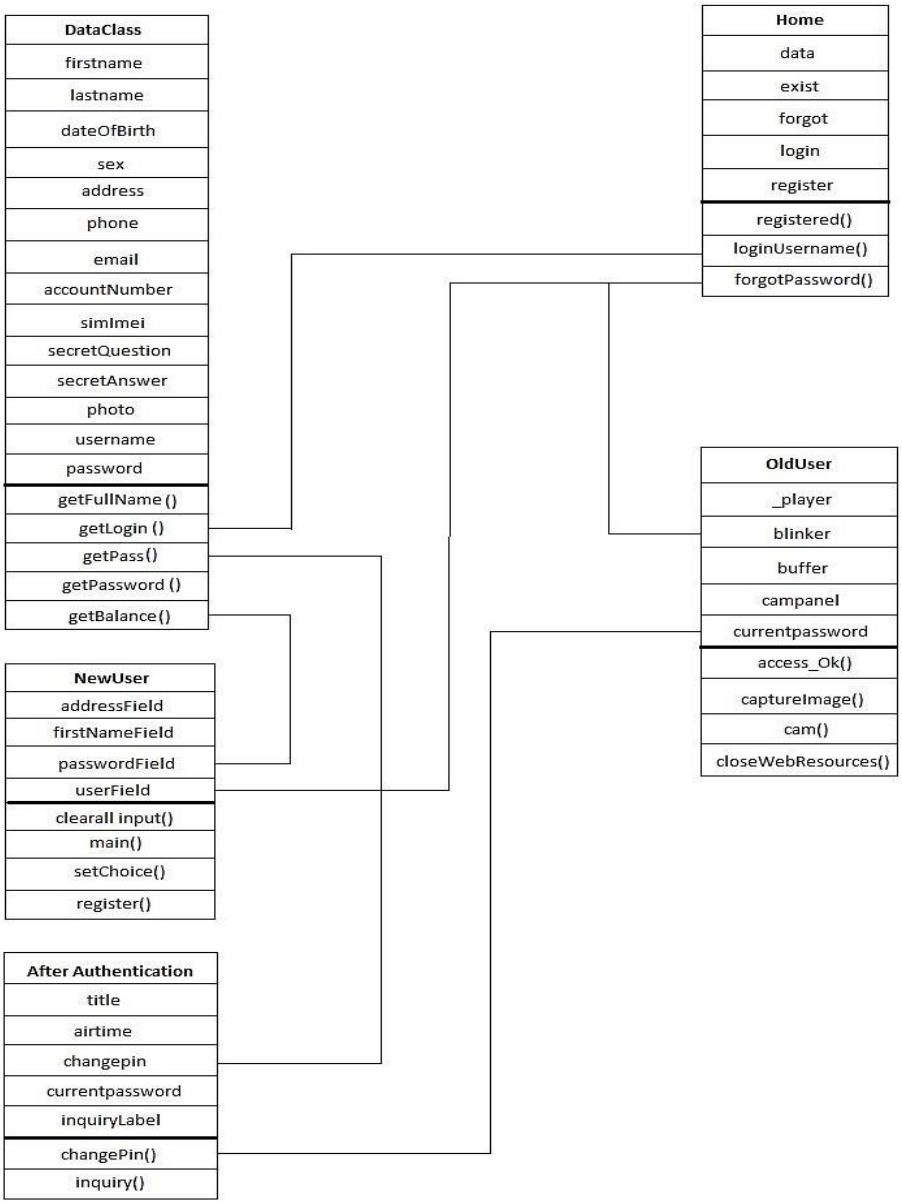

Figure 2. Class diagram of proposed systems

7.3. Database Transaction Sequence

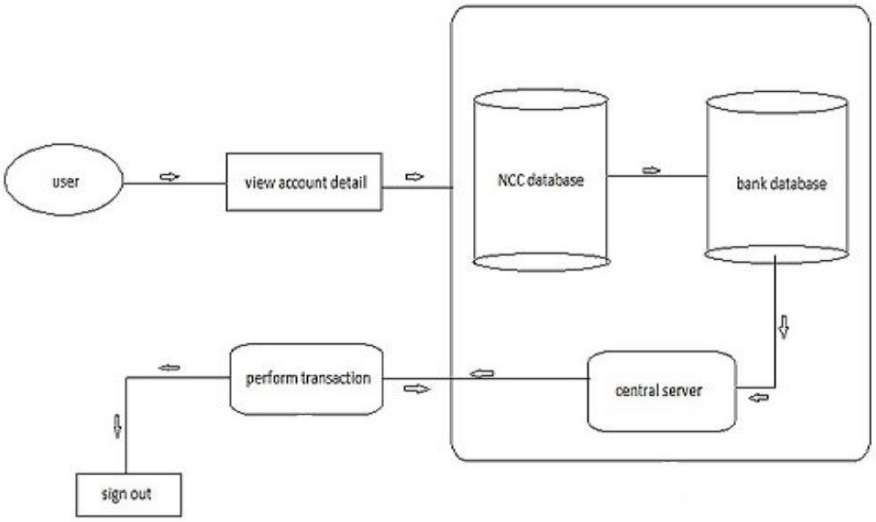

Figure 3. Database transaction sequence of proposed system

7.4. Process/Procedure Design:

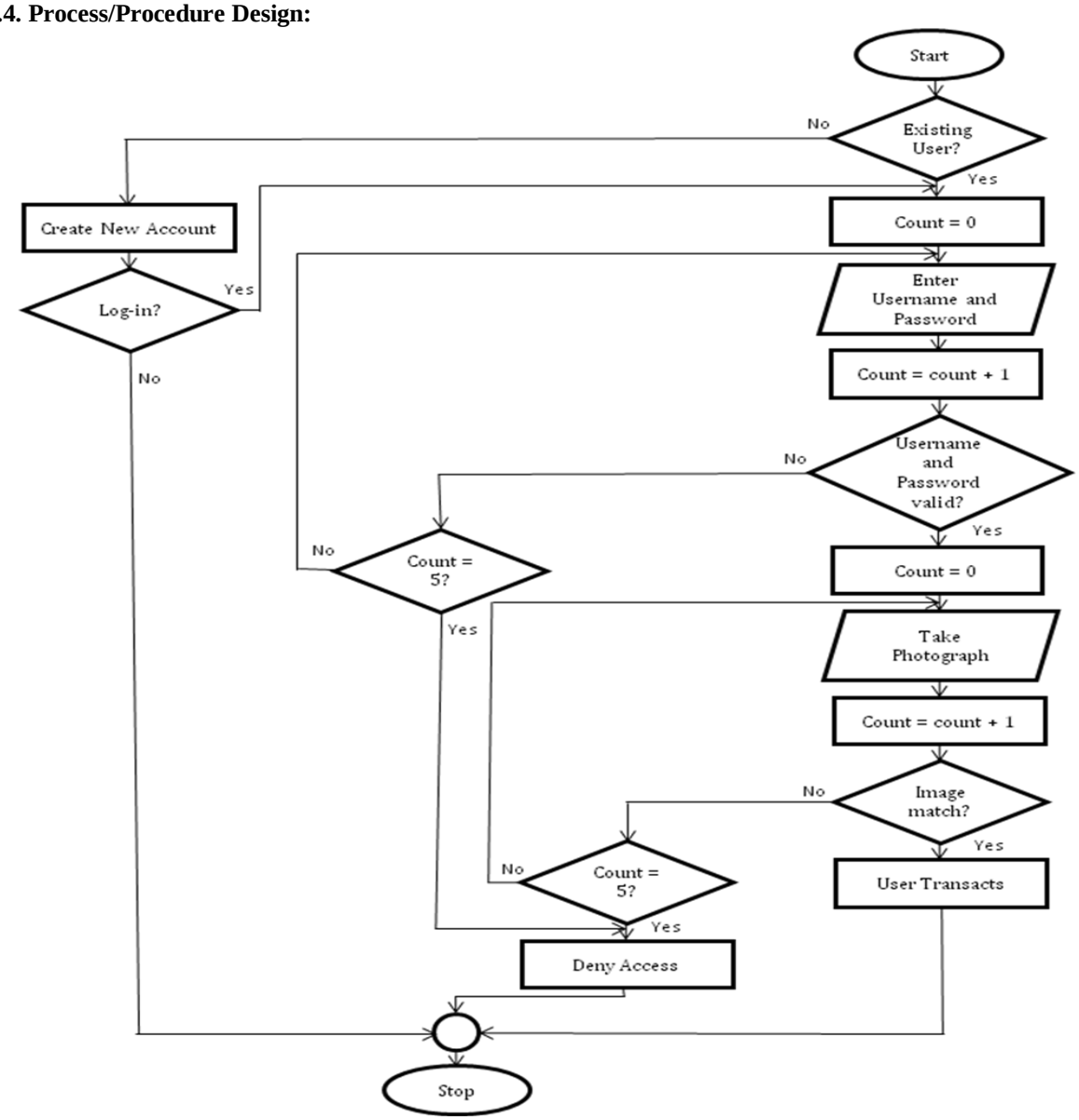

Figure 4. Flowchart of implementation procedure

VIII. System Implementation

Test case #1
Use Case: Create mobile Account
Background: Non-existing User want to fill form
Event Sequence:

1. Click Create account and submit.
2. Login as existing user.

Test case #2
Use Case : Take photograph
Background : User wants to take a photograph to authenticate genuine account holder.
Event Sequence:

1. Click on take photograph.
2. Hold phone to capture face.

Test case #3
Use Case : Perform transaction
Background : User wants to access bank account.
Event Sequence:

1. Click on transaction you want to perform.

Test case #4
Use Case : Disconnect to server
Background : User wants to close the session.
Event Sequence:

1. Click on logout option in menu

In this way we tested using different test cases that found lot of errors which were corrected by recoding of that related procedures..

IX. Result And Discussion

On the program end, the security is multi-factored. A username and password level, a facial recognition level and a secret question and answer level. Users are limited to five trials after which access is denied. Two dependable databases are also used to authenticate genuine users; these databases are the NCC database and the issuing bank database. In an advent of facial defection, users are advised to see their bank information technology operators. The response time for a complete transaction is seven minutes maximum putting other limiting factors into consideration; the false acceptance rate is 3%.the implication of false acceptance rate is given by elements on image background and facial defects. The advantages of this system include;

i. Secure and transaction
ii. Cost effective
iii. Transaction can be done anywhere remotely (with availability of mobile network)

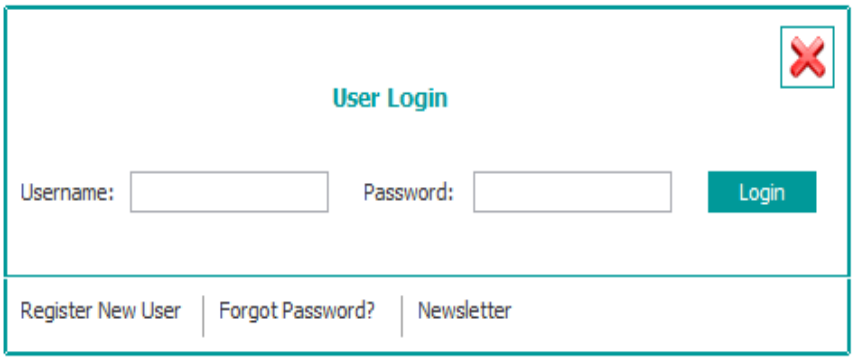

Figure 5. Login interface

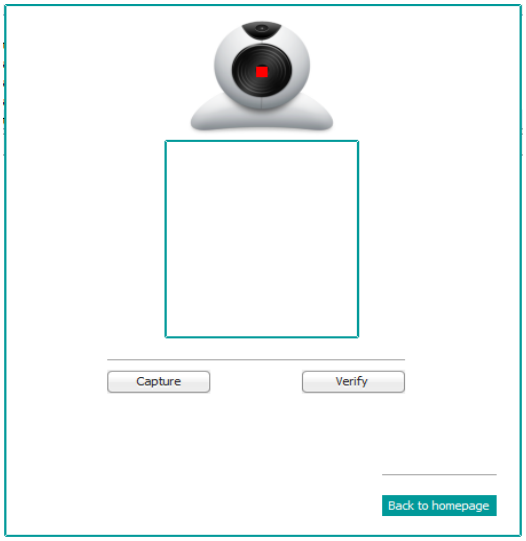

Figure 6. Facial capture/recognition interface

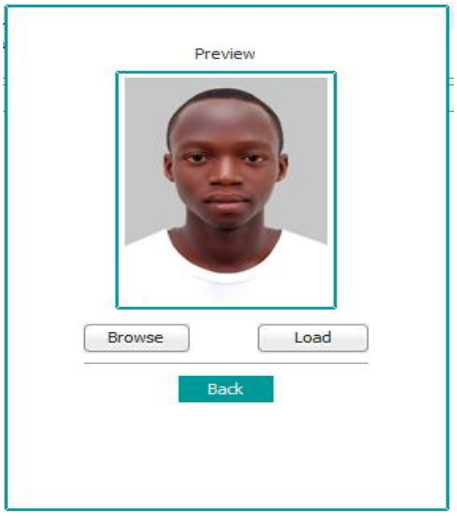

Figure 7. Snapshot of a verified user

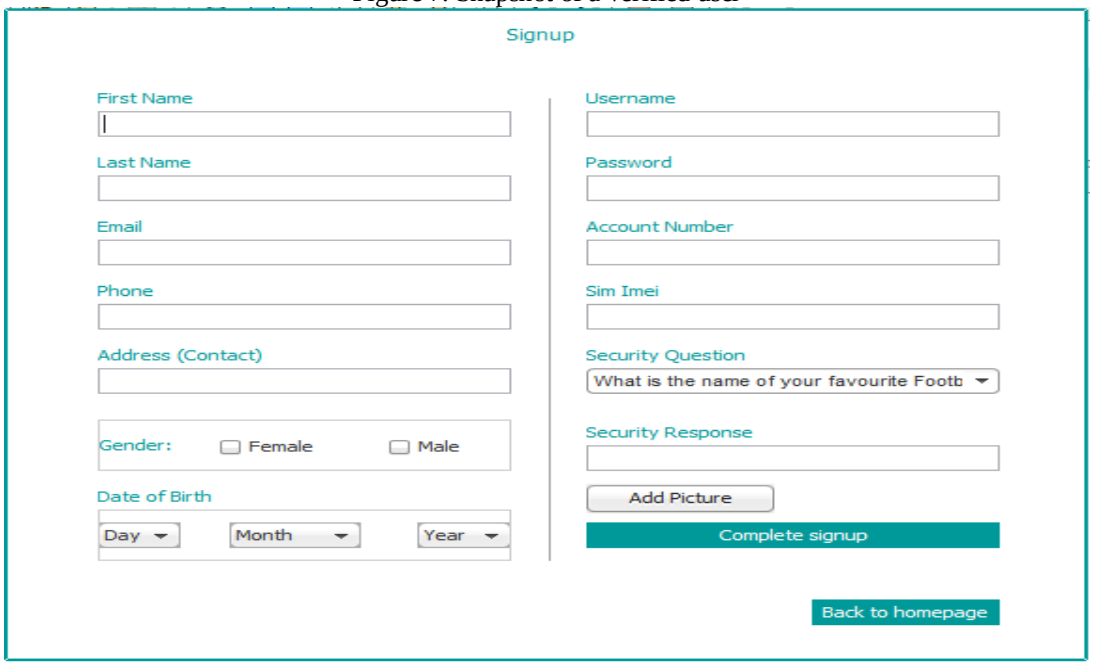

Figure 8. New user registration interface

X. Conclusion

In a bid to make the Nigerian economy cashless, attention should be focused on security. When the security is trusted, it will build customer satisfaction and discourage the use of cash. The number of mobile phone users increases by the day and the success of the security on mobile banking will encourage new users to adopt the trend. Introducing this level of authentication using facial recognition on users' account to authenticate from the Nigeria Communication Commission's database and the facilitating bank's database, will no doubt contribute to mitigate mobile banking fraud.

REFERENCES

[1] Sun, Z. W. (2009). Design And Implementation Of Mobile Payment Based On Multi-Interface Of Mobile Terminal. Zhejiang.
[2] Nagel, B. (2007). Mobile Authentication Marries Security With Covenience.
[3] http://en.wikipedia.org/wiki/Mobile_banking.
[4] Punithavathi, R. and Duraiswamy, K. (2011). Secure Authenticated Mobile Agent Based Mobile Banking System. European Journal of Scientific Research. ISSN 1450-216X Vol.57 No.3 (2011), pp.494-501.
[5] Krutz, R. L. and Vines, R. D. (2003). The CISSP Prep Guide: Gold Edition. Wiley Publishing, Inc., Indianapolis, Indiana.
[6] Capoor. (2006). Electronic Banking Journal.
[7] Gafurov, D., Helkala, K., and Sondrol, T. (2006). Biometric Gait Authentication Using Accelerometer Sensor. Journal of Computers, Vol. 1, No. 7, Oct./Nov. 2006, pp. 51-59.
[8] Povocnicu, A. (2009). Biometric Security for Cell Phones. Informatica Economica, vol. 13, no. 1/2009, pp 57-63.
[9] www2.ncc.gov.ng
[10] The Impact of Mobile Services in Nigeria. Pyramid Research, March 2010.
[11] Mobile Banking Overview (NA). Mobile Banking Association, January 2009.
[12] Komolafe, B., Agwuegbo, A., and Adegunlehin, T. (2009). Nigeria: Banks' Customers Agonise as ATM Fraud Persist. Available on: http://allafrica.com/stories/200911300313.html.

Authors

Falaye Adeyinka Adesuyi
Lecturer, Department of Mathematics/Statistics, Federal University of Technology Minna
Falaye holds B.Tech (Mathematics/Computer Sc.) and M.Sc. (Computer Sc.). He is a member of National mathematical Society (NMS) as well as Nigeria Computer Society(NCS). His areas of interest are risk and security in Network Systems, mobile and internet banking.

OSHO OLUWAFEMI holds an M.Tech in Mathematics. Formerly a banker, where he headed the IT department, he presently lectures in the Department of Cyber Security Science, Federal University of Technology, Minna, Nigeria. His research interests include information security, data mining/machine learning, and software development.

ALABI, ISIAQ OLUDARE is an industry-experienced IT professional and an academic. He obtained his Bachelor's degree at the University of Ibadan and Master in Information Technology at Ladoke Akintola University of Technology, Ogbomoso, both in Nigeria. Currently, he is teaching Database and Data mining in the department of Information and Media technology, School of Information and Communication Technology (SICT) at Federal University of Technology, Minna, Nigeria.

Adama Ndako Victor
System Analyst, Directorate for Coolaboratiion Affiliations and Linkages, Federal University of Technology Minna.
Victor holds B.Tech (Mathematics/Computer Sc.) and is presently a System Analyst at the Directorate for Collaboration Affiliations and Linkages FUT Minna. His areas of interest are Software Engineering and Artificial Intelligence.

AMANAMBU VICTOR RICK has a B.Tech in Mathematics/Computer Science from the Department of Mathematics, Federal University of Technology, Minna, Nigeria