Computing, Information Systems, Development Informatics & Allied Research Journal
Vol. 8 No. 3, September, 2017 - www.cisdijournal.net

Secured Application Based Mobile Banking Model for Nigeria

[1]Faisal Ali Garba, [2]Khadija Muhammad Musa, [3]Kabiru Ibrahim Kunya, [4]Zahra'u Ahmad Zakari, [5]Ishaq Dawaki.
Department of Computer Science Education
Sa'adatu Rimi College of Education
Kano, Nigeria.
E-mails: [1] alifa2try@gmail.com, [2] kdjmusa21@gmail.com, [3] kabiruikunya@gmail.com, [4]zaroukh84@yahoo.com, [5] ismuid@gmail.com
Phones: [1] +2348036028632, [2] +2348035875840, [3] +2348065377142, [4] +2348034280872, [5] +2347066734742

ABSTRACT

Fraud incidences in electronic banking is in continous rise and if not kept in check can discourage people from embracing the electronic banking option. Nigeria has approximately 140 million active mobile subscribers and if this number should embrace mobile banking, it will promote the Government's initiative for a cashless society. This research proposes a secured application based mobile banking model for Nigeria, that utilizes the recently introduced Bank Verification Number (BVN) policy of the Central Bank and that is based on a three level authentication mechanism: i. what the user knows (Bank Verification Number (BVN)), ii. what the user has (device's IMEI) iii. what the user is (user's fingerprints and finger vein multimodal biometric data). The dissertation proposes client server mutual authentication with the use of X.509 based Public Key Infrastructure (PKI). This proposal is demonstrated with Android application connected to a MySQL database via HTTPS and JSON Web Services implemented with PHP. The result of this work is a secured application based mobile banking model for Nigeria that will encourage more people to embrace mobile banking due to its increased level of security.

Keywords- Mobile-banking, multimodal-biometric, BVN, authentication, X.509 PKI.

CISDI Journal Reference Format
1Faisal Ali Garba, 2Khadija Muhammad Musa, 3Kabiru Ibrahim Kunya, 4Zahra'u Ahmad Zakari, 5Ishaq Dawaki. (2017 Secured Application Based Mobile Banking Model for Nigeria. Computing, Information Systems, Development Informatics & Allied Research Journal. Vol 8 No 3. Pp 27-34 Available online at www.cisdijournal.net

1. INTRODUCTION

There is currently 3.9 billion Internet users worldwide (Miniwatts Marketing Group, 2017). By the year 2020, the number of mobile smartphone users is forecasted to attain 2.87 billion (Statista, 2017). Africa and Asia had the highest percentage of mobile traffic, Asia with 65.1% and Africa with 59.49% (Statista, 2017). One hundred and ninety two (192) countries have active 3G mobile networks, which cover almost 50% of the global population. Smartphone sales are the majority of mobile handsets sold worldwide; tablet sales will soon exceed total PC sales. While there are at least five mobile platforms, Android has an 84% share of smartphones, and 72% of tablets. There are well over 1 million apps available, which have been downloaded more than 100 billion times. Time spent using apps exceeds time spent on mobile browsers, and in the US, at least, exceeds time spent on desktop and mobile browsers combined (Internet Society, 2015). Mobile banking is defined as the service which qualifies customers to receive information about their accounts and to make real transactions by using mobile phones in a secure and reliable way. Mobile banking can be executed using various channels like Short Message Service (SMS), Unstructured Supplementary Services Delivery (USSD), General Packet Radio Service (GPRS)/Wireless Application Protocol (WAP), Phone based Application and Subscriber's Identification Module (SIM) card Application. All of these channels are used separately or combined for various banking operations.

1.1 Problem Statements

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 (Komolafe *et al*., 2009). 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 (Adesuyi *et al*., 2013).

1.2 Research Motivation

Nigeria has approximately 139 million active mobile subscribers (Subscriber Statistics, 2017). 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 (Research, 2010), 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 (Research, 2010). 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 (Association, 2009), hence the need for multi-factor level of authentication. This is necessary to encourage customers to embrace mobile banking. (Komolafe *et al*., 2009). As a result, the goal of this research was to design and develop a secured application based mobile banking model for Nigeria, based on a three level of authentication: what the user has, what the user knows and what the user is.

2. LITERATURE REVIEW

Mobile banking is defined as the service which qualifies customers to receive information about their accounts and to make real transactions by using mobile phones in a secure and reliable way. Services like: enquiry (balance enquiry/ mini statement/ currencies rates), money transfer, bill payment, cheque book request and many other banking services (El-Safi, 2013). Growth in the mobile banking is driven by various facilities like convenience of banking operations, greater reach to consumers and integration of other mobile commerce services with mobile banking. In mobile banking there is no place restriction, it has a high penetration coefficient as growth of mobile phones are more than that of computers. It is fully personalized and private increasing transaction authenticity and is 100% available all the time with users (Pujitha *et al.*, 2013).

2.1 Mobile Banking Channels

Mobile banking can be executed using various channels like SMS, USSD, GPRS, WAP, Phone based Application and SIM Application. All of these channels are used separately or combined for various banking operations:

Short Message Service (SMS)
SMS is the simplest form of mobile banking. It is largely used for information-based services.

Unstructured Supplementary Services Delivery (USSD)
Unstructured Supplementary Services Delivery (USSD) is a technology unique to GSM. It is a capability built into the GSM standard for support of transmitting information over the signaling channels of the GSM network. USSD provides session-based communication.

Wireless Application Protocol (WAP) /General Packet Radio Service (GPRS)
General Packet Radio Service (GPRS) is a packet-switched data service available to GSM users. GPRS enables services such as WAP access, Multimedia Messaging Service (MMS), and Internet communication services such as email and World Wide Web access in mobile phones. WAP is wireless application protocol used over GPRS. It is similar to Internet banking. The consumer's handset needs to be WAP enabled. WAP banking is open to similar threats as Internet banking.

Phone-based Application
Phone based applications are developed in various languages like J2ME and .NET having advantages that it can use GPRS, USSD or SMS, MMS to carry the consumer data/instruction in an encrypted format and it is operator independent. These are secure application which resides on supported handset.

SIM Application Tool Kit
The SIM Application Toolkit allows for the service provider or bank to house the consumer's mobile banking menu within the SIM card. STK is the most secure method of mobile banking. It allows the bank to load its own encryption keys onto the SIM card with the bank's own developed application (Pujitha *et al.*, 2013).

2.2 Mobile Banking Security

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-factor authentication, and multifactor authentication. Bearing in mind the cost of providing these services to clients, most banks are wary 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. 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 (Adesuyi *et al.*, 2013).

A questionnaire was created by (Kaya, 2013) as an attempt to understand the difference in behaviour and to gather a sense of trust in mobile banking. The sample data revealed that more than 70% use mobile applications in general. The vast majority (77%) of users were concerned with security regarding mobile banking services and that is the main reason for not using mobile banking in 40% of the cases while the other 37% are still concerned but use it anyway (Kaya, 2013). The results of the questionnaire also revealed that only 30% of users carry out banking transactions via mobile browser or mobile banking application. 70% of the ones that carry out mobile banking prefer to use a mobile bank app. A possible reason for that could be because of its ease of use or maybe because of their trust in the mobile bank app which is a direct link to the bank instead of using a browser (third-party) in between the customer and the bank. Forty percent were unsure about the mobile banking application security level, but when asked about the online banking (using a browser) 92% believed that the level of security provided was medium or high. The sample data shows the sense of trust in online banking is much higher than the one of the banking application (Kaya, 2013).

Mobile bank apps provide a direct link from the device to the bank, without having to go through any additional browser or third-party application. This means banks have much better control over the security and connection of customer interactions. Because these apps are built specifically for a particular bank and its customers, the bank can provide a secure connection using SSL encryption and two-factor authentication that meets the institution's unique needs. Even if someone is able to obtain a customer's phone, they will still be required to put in a username and password, and if available, provide a second factor of authentication, in order to gain access to the accounts. Along with these two factors of authentication, many banks have started implementing a third method of security: a profile of a customer's actions. Banks and other financial institutions are able to monitor a customer's actions when banking via a mobile app, creating a profile of those interactions. Another plus to using a mobile application is the fact that most smartphones and tablets can now be cleared or reset from remote locations. Thus, if someone steals or obtains a mobile device, the customer can use his or her computer or any other device with an Internet connection to clear any data and apps from the device, eliminating the possibility that someone else can use the phone to access the customer's account. As customers become more familiar with mobile banking app security and learn to trust a bank's mobile app brand, they will be more willing to use these tools (Kaya, 2013).

2.3 Biometric Authentication

Biometrics authentication mechanism identifies the physical individuality or uniqueness of the authorized person. The advantage of using finger print is that, communication can occur only through authorized persons and will be secure. Finger print technology is the most commonly used in telecommunication industry (Krevatin, 2010). If finger-print technology is introduced in mobile phones, then the risk of unauthorized persons using the mobile for mobile banking is significantly reduced (Bilal *et al.*, 2011). Finger-print takes only 256 bytes and its accuracy is high. The biometric device first captures the user's finger print and creates a reference template and it is stored in database and that ends the enrolling processes of user's finger print (Michaels, 2008).

2.4 Multimodal Biometrics

The concept of multimodal biometric system has gained enormous attention because of their reliable and accurate identity verification. Multimodal biometric systems based on fingerprint and finger vein modality provide promising features useful for robust and reliable identity verification. Among the different biometric modalities that can be used to constitute a multimodal biometric system, the use of fingerprint and finger vein appears to be more refined because:

The human fingers are highly convenient for imaging and disclose variety of features when captured in different spectrums. For instance, imaging the finger with visible spectrum will disclose the texture features present on the finger surface that in turn can be used to extract minutiae features of the fingerprint or the line features of the whole finger. While imaging the finger with a near infrared spectrum will allow one to capture the finger vein pattern.

- Low verification error rates can be achieved by combining these complementary features available from the single biometric modality i.e. finger.
- Use of finger-vein shows strong anti-spoofing nature as it is hidden inside the finger and cannot be stolen without subject co-operation.
- The two biometric characteristics can be acquired with one capture device and in principle with a single capture attempt (Raghavendra *et al.*).

2.5 Bank Verification Number (BVN)

Bank Verification Number (BVN) is an initiative of the Central Bank of Nigeria. It is a scheme initiated to address the increasing incidents of compromise on conventional security systems (password and PIN). The Central Bank of Nigeria through the Banker' Committee and in collaboration with all banks in Nigeria on February 14, 2014 launched a centralized biometric identification system for the banking industry tagged Bank Verification Number (BVN) (Home, 2016). Amongst the benefits of BVN are:

a. BVN gives a unique identity that can be verified across the Nigerian Banking Industry (not peculiar to one Bank)
b. Customers bank accounts are protected from unauthorized access
c. It will address issues of identity theft, thus reduce exposure to fraud

The purpose of the project (BVN) is to use biometric information as a means of first identifying and verifying all individuals that have account(s) in any Nigerian bank and consequently, as a means of authenticating customer's identity at the point of transactions. To provide a uniform industrially accepted unique identity for bank customers and to authenticate transactions without the use of cards using only biometric features and PIN (Home, 2016).

A unique ID number is to every bank customer at enrolment and linked to every account that the customer has in ALL Nigerian Banks. Individuals are required to submit an acceptable means of identification as prescribed for enrolment. During enrollment all ten (10) fingers and facial image are captured. For authentication purposes, individuals performing banking transactions are required to identify themselves using their biometric features which will be matched against information in the central database. To enroll for BVN customers are required to walk into any branch of their bank to fill out and submit the BVN Enrolment form. They are then required to present themselves for biometric data capturing (such as fingerprint, facial image etc). An acknowledgment slip with the transaction ID is issued to customer and within 24 hours the system confirms customer's application, the BVN is generated and an SMS is sent to him for pickup. The BVN and unique features of an individual shall be used in conjunction with a PIN on a point of transaction (Home, 2016).

2.6 Public Key Infrastructure

PKI enables users of a basically unsecure public network such as the Internet, to securely and privately exchange data and money through the use of a public and a private cryptographic key pair that is obtained and shared through a trusted authority. The public key infrastructure provides for a digital certificate that can identify an individual or an organization and directory services referred to as Certification Authorities (CAs) that can store and, when necessary, revoke the certificates. The public key infrastructure assumes the use of public key cryptography, which is the most common method on the Internet for authenticating a message sender or encrypting a message. Traditional cryptography has usually involved the creation and sharing of a secret key for the encryption and decryption of messages. This secret or private key system has the significant flaw that if the key is discovered or intercepted by someone else, messages can easily be decrypted. For this reason, public key cryptography and the public key infrastructure is the preferred approach on the Internet. (The private key system is sometimes known as symmetric cryptography and the public key system as asymmetric cryptography). PKI implementation of a system can ensure confidentiality, integrity, authentication and non-repudiation.

Digital signature is a related concept to asymmetric encryption. Digital signatures are created using asymmetric cryptography, the approach on which digital signatures are based. Asymmetric Cryptography is distinguished by having two different keys which are created using algorithms like RSA and AES, a private key to encrypt messages and a public key to decrypt them. The cryptographic private key K0 (a suitable array of bytes) is used with an appropriate algorithm to transform the initial human-readable message into a different message that is encrypted. A second public cryptographic key K1, which is related to the private one, is used to change the encrypted message back to its original decrypted form via a second related algorithm. The process of creating digital signatures starts with the hashing of data to be transmitted. The reason for performing hashing is to ensure data integrity. Hashing is simply a process whereby you calculate a hash code from some data. The generated hash code is mathematically derived and is unique and specific for the data it was derived from. If any byte changes in the data then a completely different hash code is generated. Hash codes are a means to check that data was received/read as it was sent/written, any accidental damage/modification or malicious changes are checkable using hashes.

Some hashing algorithms include MD5, SHA1, and SHA 256. One of the problems with hashing is that it is wide open to man in the middle attacks. Without doubt hashing has its uses but in terms of sending data there is nothing stopping someone from intercepting the data, modifying it, and then resending the new message with a new hash. What the receiver gets is a message where the hash code matches the data, even though the data has been modified. The use of digital signatures can avoid this scenario. In digital signatures public/private asymmetric keys are used. The two keys of asymmetric encryption are mathematically related to each other and one key can be used to verify that the encryption was done with the other key. With digital signatures the sender encrypts the hash using their private key while the receiver verifies the digital signature using the sender's public key. Of course since the public key is more freely available then anyone can verify the message's source. So, for example, Buhari wants to send Aisha some data and Aisha wants to be able to check the data was unchanged and came from Buhari. Buhari creates the hash and encrypts it into a digital signature using his private key. He sends the data and the digital signature over to Aisha.

Aisha uses Buhari's public key to verify that the digital signature was created using Buhari's corresponding private key. If everything checks Aisha knows the message hasn't been modified and that it came from Buhari. Asymmetric key encryption by itself is not enough because it is necessary to trust the public key received. An attacker can deceive you by signing a message with his private key and send you a digitally con whilst pretending he is someone else. The public-key infrastructure (PKI) avoids this by utilizing a third-party entity, called Certification Authority (CA) that, under its responsibility, binds a public key to its owner. The binding occurs when the Certification Authority digitally sign a message that contain obtained. With this mechanism, the recipient is sure that the message that she/he received is your message, because only you hold the private key the shared, key. This way, you digitally 'sign' your message. Asymmetric encryption has an overhead and not suitable for large texts. As a result, combination of two methods is employed for secure transmission on the web. HTTPS and SSL are using this combination. It starts with Asymmetric communication between client and server during which key is transferred in asymmetrically encrypted form. Once key is delivered it is then used to decrypt the symmetrically encrypted text. When dealing with applications offering services like online banking as is the case for this project, authenticating the server as well as the client may become necessary in order to ensure a higher level of security (Jinor, 2011)

2.7 Mutual authentication

One-way SSL simply means that only the server certificate passes from the server to the client but not the other way around. Thus, only the server is authenticated using the mechanism on PKI explained above. With mutual authentication, both sides pass certificates to each other to establish an SSL link, we have mutual authentication via two- way SSL. Both sides now know the identity of the other from their respective certificates (Jinor, 2011).

3. REVIEW OF RELATED WORKS

A biometric based mobile banking has been proposed by (Bilal *et al.*, 2011). Their proposal work thus: Registered users will directly go to login form while new users will go to registration form. They proposed scanner that utilizes Radio Frequency (RF) scanning. Their reason is that with RF scanning, it is possible to differentiate between living cells and dead or copied cells. After the verification of data, the customer will be able to access the database through web server. If the finger print matches with that of the database then customer will be able to start mobile banking services through mobile handset. For additional security Lightweight Directory Access Protocol (LDAP) server is used. If first finger prints authentication is not found in database then it will be checked in LDAP server for more verification.

New users are required to register any three finger print in database and also need to fill in a registration form. If the finger print of the bank customer is registered successfully then customer will be able to use mobile bank services. For secure authentication purposes they proposed finger print scanner device. Mobile manufacturing companies will make the biometric scanner device with mobile hand set. The mobile customer will used it for authentication purposes. After capturing finger print, the data will be transmitted through internet. And the data can be accessed through bank server. The finger print scanner device can be attached to mobile phone though a port. They narrated that the process which statistically gives the best possible template is called *consolidation*. Consolidation of three finger template produce high quality enrolled template according to Statistical Research, they reported. With the help of the finger scanner device, mobile handset gets three samples as shown in the figure. These samples are stored in bank server with appropriate account holder. In case of cut, burn, damage of one finger the other finger print data will still serve as a unique identifier they claimed. Finger print is present for matching in the database record. Every time new finger print is compared to the stored finger print.

For authentication purposes and to secure customer data at server end additional server known as Server LDAP authentication is used. In LDAP, the client sends the query packet through TCP/IP to the server. The server confirms the identifier on LDAP Directory Information Tree (DIT) which is stored on LDAP server. When the result is found, it is sent back to client. In case of result not found then query will be sent to another LDAP server. This LDAP verify the data in tree model structure method. They claimed that LDAP authentication has many advantages like centralized usage, privileges, management, and storage of user information and user accounts (Bilal *et al.*, 2011). A mobile client application that uses wireless access protocol to enable customers securely transmits banking information was proposed by (El-Safi, 2013). He proposes a MIDlet (Java 2 Micro Edition) application that will transmits banking information through a secure communication path. The MIDlet role was to prevent unauthorized access by imposing login form that connects to backend database to investigate from it the identity of the entered user, then allows the user to proceed to transactions and inquires form. He proposes an interface between the backend database and MIDlet represented in a web service, the idea of putting the web service in the middle to exploit the properties of the web services like language independence and interoperability, thus enables using any language to develop the client applications, thus the mobile application client can invoke different functions described in the web service. Web service bear effort of dealing with the backend database and return the result to mobile application client.

For identification purpose (El-Safi, 2013) proposes the use of account number which is already known by bank and customer, user name which is a unique name given to a customer, mobile pin (m-pin) a one-time password given to a customer and imposed to change it at first login, mobile application client version to help identify which version is used by the customer and to let him know if there are some upgrades, IMEI used as a log of used phones, this may help if a fraud case occurred and security achieved with the use of SSL's PKI. The server initiate's a session to keep track of the authenticated customer and a cookie saved in mobile application. An automatic logout is carried out if the client becomes idle for a long time (El-Safi, 2013). The bank server is responsible for respond to coming requests and it is represented by the web service which is implemented using SOAP protocol and data are represented as XML format. Web Service provides the ability to call different methods without need to about their implementation. The method signature is described by WSDL. Web service description language (WSDL) is used for describing the functionality offered by a web service; WSDL is used by MIDlet to generate Stubs that work as proxies to invoke the remote functions. The backend data base represents the container for customers' confidential information. Stored procedures are developed to be called by web service, interaction between web service and database is done through it. This enables bank to veil their database architecture. The connection between the web service and the database should be the responsibility of the bank to provide secure environment (El-Safi, 2013).

A biometric based mobile banking on android device was proposed by (Belkhede *et al.*, 2012). They proposed a system that captures the fingerprint of a client with the use of his/her smartphone camera. "The solution involves the use a biometric authentication mechanism. A payment application would be installed onto an android device, for authentication finger print is taken at run time. The finger print template would be captured by the phone and compared against a stored template on a database server. The fingerprint template is encrypted by using the RSA algorithms and sends it to the host server (i.e. Bank). Fingerprint is used for the login purpose for the bank application on mobile". (Belkhede *et al.*, 2012). Mobile device act as a client and the bank website act as a server (host server). Once fingerprint is taken as a login, it is sent to the server for matching as request, and server send the reply message. If matched then login will be successful and user can do the transaction. In the client server module for providing the enhanced security authors use the encryption technique so the wireless transmission cannot be hacked to reveal the fingerprint template. (Belkhede *et al.*, 2012)

4. THE PROPOSED APPLICATION BASED MOBILE BANKING MODEL FOR NIGERIA

This proposal is an enhancement to the work of (El-Safi, 2013). This proposal introduces multifactor authentication not just a username and password. This proposal also introduces the idea of a panic finger login as suggested by (Jinor, 2011) to act as coercion trigger to redirect to honeypot and alert the proper authorities. This proposal also uses Android as a platform, which is the most popular mobile operating system. However, both proposals use Public Key Infrastructure (PKI) for encryption and authentication. To get the proposed model up and running, the following steps were taken:

a. Android mobile application developed as a client.
b. A database server developed in MySQL.
c. A JSON web service implemented using PHP to work like a mediator between mobile client application and the MySQL database server.
d. Established connection between client and server using HTTPS and JSON.
e. Setup a custom X.509 PKI using OpenSSL.
f. Setup a XAMPP server
g. Configured the server to support SSL server authentication (i.e., HTTPS) using a custom server certificate.
h. Configured the server to support SSL client authentication.
i. Setup an HTTPS connection with the server from within the Android banking App on the mobile with server authentication.
j. Setup an HTTPS connection with the server from within the Android banking App on the mobile with client authentication.
k. A sample fingerprints images from Fingerprints Verification Competition, FVC2006 database taken as user's fingerprints.

Functions developed in the web service:

a. Log in and authentication function (El-Safi, 2013)
b. Sign up function
c. Balance inquiry function Send money
d. Help function
e. Transaction history function

The server has also been set to initiate a session to keep track of the authenticated customer and a cookie saved in mobile application. An automatic logout is carried out if the client becomes idle for a long time (El-Safi, 2013). It is the research expectation that mobile phone manufacturers would come up a with mobile phones that have sensors capable of capturing both fingerprint and finger vein simultaneously. Such sensor proposal has been presented by Raghavendra *et al* ( ).

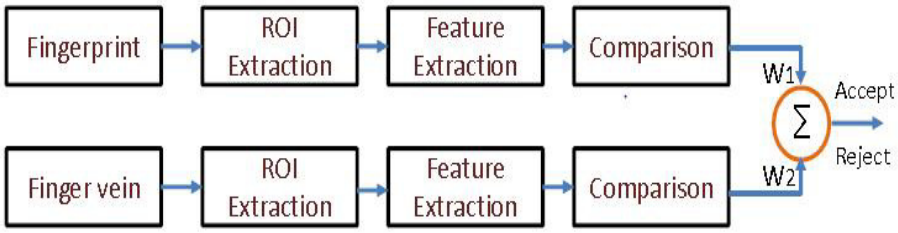

Fig.1: Block Diagram of fingerprint & finger vein Verification Scheme (Raghavendra *et al.*)

A. Proposed Model Pseudocode

a. A new user will be prompted to register first.
b. Mobile client application prompts the user to enter his eleven digits BVN to login to the mobile banking application.
c. Next the mobile client application will require the user to scan any of his fingers for authentication, or a panic finger in case of coercion.
d. The mobile application client, transmits the device IMEI (the IMEI of the primary SIM in case of a dual SIM phone), the biometric data and BVN to the bank server for verification.
e. Positive verification allows access to banking services.
f. Negative verification redirect user to a honeypot server and alert the proper authorities.
g. For every transaction above N150 000, the application invokes an OTP (One Time Password) which is send to the user's registered mobile number.
h. The OTP serves as a transaction confirmation number, which he/she must input to confirm the transaction.
i. If the customer selects logout on the menu, the mobile application is closed automatically, notifying the user, signaling the end of operation.

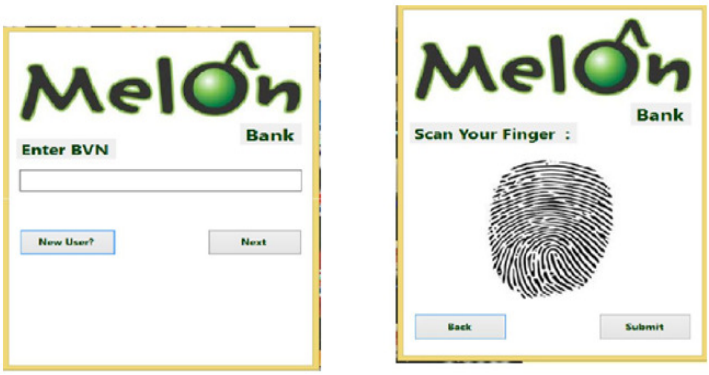

Fig 2: BVN and fingerprint log in screens

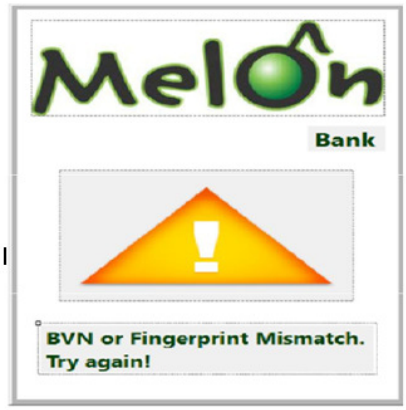

Fig 3: BVN and Fingerprint mismatch log in screen

5. RESEARCH RESULTS

The outcome of this research has been a complete secured application based mobile banking model for Nigeria that utilizes the Bank Verification Number policy of the Central Bank and based on a three level of user authentication.

6. RESEARCH IMPLICATIONS

This research will further drive the cashless policy of the Central Bank of Nigeria. It will increase people trust in the usage of application based mobile banking. It will reduce the number of queues in the bank. It will reduce the operational cost of banks. It will bring banking to the remote areas considering the pervasiveness of mobile phones.

7. SUMMARY AND CONCLUSION

The outcome of this research has been a complete model for a three level secured application based mobile banking model for Nigeria, which will cater for all the security requirements i.e. confidentiality, integrity, authentication & authorization, non-repudiation, access control. The outcome of this dissertation is a complete model for a three level authentication based mobile banking. However, there is more to application based mobile banking security than what this research proposed. This proposal ensures the security of data transmission to and fro client and server and that the right user is allowed access to the app. The research has not looked into mobile application vulnerabilities such as: insecure data storage, lack of binary protections, client-side injection, hard-coded passwords/keys and leakage of sensitive data.

8. FUTURE RESEARCH

Future research will consider the following:

a. The implementation of the honeypot module of the proposed model.
b. A Research into the security of mobile applications.

REFERENCES

1. Adesuyi, F. A., Oluwafemi, O., Oludare, A. I., Victor, A. N., & Rick, A. V. (2013). Secure Authentication for Mobile Banking Using Facial Recognition. *IOSR-JCE*, 51-59.
2. Association, M. B. (2009). *Mobile Banking Overview.*
3. Belkhede, M., Gulhane, V., & Bajaj, D. P. (2012). Biometric Mechanism for Enhanced Security of Online Transaction on Android System: A Design Approach. *ICACT2012.*
4. Bilal, M., & Sankar, G. (2011). *Trust & Security Issues in Mobile Banking and it's Effect on Customers.* Karlskroma: Blekinge Institute of Technology.
5. El-Safi, A. A. (2013). *Mobile Banking Project.* Sudan: Faculty of Mathematical Sciences, University of Kharthoum .
6. *Home*. (2016, 01 01). Retrieved 01 01, 2016, from http://www.bvn.com.ng/
7. Internet Society. (2015). *Mobile Evoulution and the Development of the Internet.* Internet Society.
8. Jinor, A. D. (2011). *Pro-active Architecture and Implementation of a Secure Online Banking System that Uses Fingerprint Data as Part of Client Side Digital Signatures.* Copenhagen: Information Technology University of Copenhagen, Software Development Technology Department.
9. Kaya, M. M. (2013). *Trust and Security Risks in Mobile Banking.* Kellogg College, University of Oxford .
10. Komolafe, B., Agwuegbo, A., & Agunlehin, T. (2009). *Nigeria: Banks' Customers Agonise as ATM Fraud Persist*. Retrieved from www.allafrica.com/stories/200911300313.html
11. Krevatin, I. (2010). Biometric Recognition in Telecom Environment. *Intelligence in Next Generation Networks (ICIN).* Berlin: IEEE.
12. Miniwatts Marketing Group. (2017, June 30). *Internet Usage Statistics*. Retrieved 10 28, 2017, from Internet World Stats: http://www.internetworldstats.com/stats.htm
13. Michaels, L. (2008). Biometric Security for Mobile Banking.
14. NCC. (2016, 01 01). *Index*. Retrieved 01 01, 2016, from www.ncc.gov.ng/index.php?option=com_content&view=article&id=125:subscriber-statistics&catid=65:industry-information&item=73
15. Pujitha, S., & Mallu, B. V. (2013). SMS Based Mobile Banking. *IJETT*.
16. Raghavendra, R., Raja, B. K., Surbiryala, J., & Busch, C. (n.d.). A Low Cost Multimodal Biometric Sensor to Capture Finger Vein and Fingerprint.
17. Research, P. (2010). The Impact of Mobile Services in Nigeria.
18. Statista. (2017). *Mobile phone internet user penetration worldwide from 2014 to 2019*. Retrieved October 28, 2017, from Statista: https://www.statista.com/statistics/284202/mobile-phone-internet-user-penetration-worldwide/
19. *Subscriber Statistics*. (2017, September). Retrieved November 1, 2017, from Nigerian Communications Commission: http://www.ncc.gov.ng/stakeholder/statistics-reports/subscriber-data