International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2020 IJSRCSEIT | Volume 6 | Issue 3 | ISSN : 2456-3307
DOI : https://doi.org/10.32628/CSEIT2063213

An Improved Security Model for Nigerian Unstructured Supplementary Services Data Mobile Banking Platform

Samera Uga Otor, Beatrice Obianiberi Akumba, Joseph Sunday Idikwu, Iorwuese Peter Achika
Department of Mathematics / Computer Science, Benue State University, Makurdi, Benue State, Nigeria

ABSTRACT

Unstructured Supplementary Services Data (USSD) is a menu driven, real time communication technology used for value added services. It is adopted by banks for financial transactions due to its ease of operation. However existing USSD are used by fraudster to commit identity theft through Subscriber Identification Module (SIM) swap, phone theft and kidnap, in other to access funds in the bank. One of the reasons this is made possible is because existing USSD platforms use Automated Teller Machine (ATM) Personal Identification Number (PIN) as second level authenticator and this compromises the ATM channel and violets one of the stated guidelines for USSD operation in Nigeria. More so, the PIN is entered bare on the platform and so can easily be stolen by shoulder surfing. Therefore, in this paper we developed and simulated an improved USSD security model for banking operations in Nigeria. The security of existing USSD platform was enhanced using answer to a secret question as another level of authentication. This was with the view to minimise identity theft. This secret question is registered in the bank during account opening for new customers while existing customers will have to update their details in the banks data base before registering for USSD services. This is done the same way customers verify their ATM PIN in the bank. Hence the answer is known by the customer alone. The model was implemented using php on XAMPP platform and simulated using hubtel USSD mocker. Results showed that security of the proposed system was enhanced through another level of authentication provided by the answer to the security question.

Keywords : USSD, Mobile banking, ATM, SIM-swap and XAMPP

I. INTRODUCTION

Mobile banking is the use of mobile devices such as phones and tablets to perform financial transactions with the help of a mobile service provider's network. It offers ease of operation because it is ubiquitous, convenient, flexible, time saving, efficient and accessible/available everywhere at any time provided the service providers' network is available. In Nigeria today, almost every person including those in the rural area have a personal mobile phone and can operate it rather than having a computer at home. It was reported in EFInA (2019) that mobile phone penetration in Nigeria is 68.9%, therefore, mobile phone is an obvious channel for Nigerians who are just getting abreast with the operation of Information Communication Technology (ICT) gadget to use as they adopt electronic financial services for the first time. With mobile banking, a customer can bank from anywhere and at any time. Mobile banking involves the use of the following technologies; Wireless Application Protocol (WAP), mobile internet Applications (MobileApp), Short Messaging Service (SMS), Interactive Voice Response (IVR), Unstructured Supplementary Services Data (USSD) among others, deployed over a Global System for

Mobile communication (GSM) network to conduct mobile transactions (Baraka et al., 2013).

Mobile internet applications (MobileApp) are software's designed by specific banks which can be used to perform financial transaction such as; funds transfers, balance enquiry among others. It is platform dependent and requires software download and internet connection. Therefore, customer needs a smart phone and mobile data connection which involves data subscription at some cost.

Short message services (SMS) on the other hand require the customer receiving financial services such as account balances, One Time Password (OTP) a second level authentication password for internet banking transaction among others through SMS. SMS is a store and forward kind of service that requires the message to be received and stored in the customers' phone and the service providers' Short Message Service Centre (SMSC) and it also requires the use of airtime at some cost. Therefore, it is insecure and expensive. While Interactive Voice Response (IVR) requires the customer making a call through a mobile phone to the banks' phone application server for short services and enquiries already programmed as voice response based on customers request. It may require the customer hanging on the line for a long time before being attended to depending on the number of customers waiting on the queue to be attended to. therefore it also involves the use of airtime at some cost. However, USSD is a real time, menu driven, session-oriented interactive technology used to perform banking transaction with or without the internet. A session is simply invoked by dialling strings of numbers that are composed of asterisks (*) and hashes (#). It is platform independent, can use all types of phones and requires neither software download nor data connection only the service providers' network. Therefore, USSD is considered to be relatively more secure because no copy of the message is stored on customer's phone or at the Short Message Service Centre (SMSC) unlike SMS, its turnaround response time is much shorter because it is not only interactive but session based unlike IVR and it is also better than internet MobileApp, SMS, IVR with respect to cost because it rely on existing Signalling System Number Seven (SS7) protocols which requires only the mobile operator's connection. No data subscription no phone recharge.

Despite the convenience offered by USSD to customers in accessing banking services, the technology is not without its associated security threats. Fraudsters take advantage of this convenience to perpetrate financial fraud. They conduct SIM swaps of targeted individuals and then, conduct USSD-based transactions which cost victims huge losses.

A presentation at the Mobile Payments Fraud Forum of June 11, 2019, identified fraud as one of the major reasons why the uptake and usage of Mobile Financial Services (MFS) in Nigeria has been persistently low (at 3.3%), despite its rapid growth in many other emerging markets (EFInA, 2019). According to The Nigeria Inter-Bank Settlement System (NIBSS) report in EFInA (2019), fraud volume in 2018 was the highest seen in the last four years. In 2018, about 89% of all financial services fraud in Nigeria occurred through electronic channels while only 11% were non-electronic, with mobile channel fraud taking the lead in both volume and actual loss value. Therefore, there is a need to fortify existing mobile banking platforms to achieve a significant fraud decrease. Hence, in this paper, an improved USSD security platform was developed to reduce identity theft using a secret question as another level of authentication. In section 2 we reviewed the concept of USSD and its usage, section 3 describes the materials and methodologies used in this work, while section 4 discusses the implementation and results obtained and our conclusion and future work are presented in section 5.

II. LITERATURE REVIEW

A. Conceptual Review of USSD

Unstructured Supplementary Services Data (USSD) is a session-based, real-time communication technology for value added services. USSD is used in sending messages across a Global System for Mobile Communications (GSM) network between a mobile client and an application server. USSD applications are menu-driven (that is, a short menu is presented for user to select from), interactive (that is, response is provided based on menu selected) and real time. Examples of services offered by USSD include; sports updates, movies, weather information, news, stock market, reservation applications (for planes/trains/ movies, etc.), voting/polling applications, mobile account balance checking and fund transfers, airtime top up among others.

USSD code consists of strings comprising of asterisk (*), followed by a combination of digits (0 to 9) and a hash (#) such as *123*10#. The asterisk (*) and hash (#) codes are used to signify the beginning and end of the request. It supports messages up to 182 alphanumeric characters in length (longer than 160 characters SMS). USSD mobile banking session is initiated by a registered customer first dialling the banks USSD code from a phone number registered with the bank, to invoke the use of USSD bearer and communicate with the USSD infrastructure of the bank. Once the session is called, instead of invoking a voice call, a real-time session is initiated between the mobile user and the USSD application platform allowing data to be sent back and forth. The session request is received by the USSD Gateway through the Mobile Network Operator (MNO) and a single session is established between the mobile terminal and the application server. Furthermore, the gateway forwards the request to the application server which communicates with the bank to service the requested transaction. The server upon receipt of the request, returns a response through the Mobile Network Operator (MNO) containing either the information requested or a text-based menu that requires a customer to choose the desired option by entering the corresponding number. The session remains open over a radio connection until the USSD service is completed, the user terminates the application, an incorrect option is entered from the menu or a time-out occurs. The initiation of the communication can either originate from the providers' end and terminate at the mobile end (USSD-PUSH) or it may originate from the mobile end and terminate at the providers' end (USSD-PULL).

USSD architecture basically comprises of the following entities the Mobile station (Smart phones, PDAs and tablets), Mobile network operator (GSM network) and application servers (Technology vendors and financial institutions). It is as shown in Figure 1.

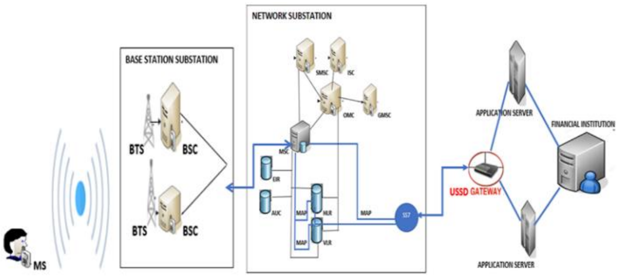


Figure 1: USSD Architecture

B. Review of USSD Applications for Nigerian Banks

The legal guideline for the operation of short codes was introduced in Nigeria by the Nigerian Communication Commission (NCC) in 2011 based on the Nigerian Communications Act 2003 (NCC, 2011). However, the regulatory framework with reference number BPS/DIR/GEN/CIR/05/002 was issued by the Central Bank of Nigeria (CBN) in April 17, 2018 to guide its operation through the director banking and payments system department headed by Dipo

Fatokun (CBN, 2018). This framework was supposed to be with effect from June 1, 2018. Nevertheless, it was postponed to October 1, 2018 in the circular referenced BPS/DIR/GEN/CIR/05/005. The guideline states under its Vulnerabilities and Mitigations section among others that financial institutions providing the use of the USSD channel shall:

i. Not use the USSD service to relay details of other electronic banking channels to their customers to prevent compromise of these channels through the USSD channel.
ii. Ensure encryption of USSD information within its environment by an auditable process.
iii. Ensure at least, radio encryption between users' SIM-enabled device and base stations.
iv. Ensure secure transmission of USSD signals between network operator and the USSD aggregators, and between the USSD aggregators and the bank.
v. Customer information that is logged by the USSD application as part of financial transactions should not include sensitive information such as customer PIN.
vi. Data stored by the USSD application at Financial Institutions shall be encrypted and the NCC shall define a minimum-security standard for MNOs and aggregators, as may be required.
vii. Avail the customers the option to opt in/out of the USSD channel for financial transactions.
viii. Put a limit of =N=100,000.00 per customer, per day for transactions as may be required. However, customers desirous of higher limits shall execute documented indemnities with their banks or MMOs.
ix. Mandate the use of an effective 2nd factor authentication (2FA) by customers for all transactions above N20,000. This shall be in addition to the PIN being used as 1st level authenticator, which applies to all transaction amounts.
x. Shall not send the 2FA to the customer's registered GSM number or device; and it shall not be generated or displayed on the USSD menu.
xi. Install a Behavioural Monitoring system with capability to detect SIM-Swap/Churn status, user location, unusual transactions at weekends, etc., achieved by 31st October 2018.

A brief review of USSD operation by selected Nigerian Banks will reveal how well they have complied with these directives regarding Vulnerability and Mitigations.

a. USSD Code for First Bank of Nigeria

First Bank of Nigeria's' USSD code for banking operation is *894#. Its services are available across all GSM networks and on all types of handsets; iphone, android, simple feature phones. It requires no internet connection and can only operate on customers registered phone numbers linked to his/her accounts with first bank. Customers can activate the services in two ways depending on whether there is debit card linked to the account or not; customers with debit cards, simply dials *894*0#, select a preferred card from list of cards, enter a four-digit Personal Identification Number (PIN) linked to the debit card and create a five-digit PIN. While those without a debit card can simply dial *894*0#, provide 10 digits first bank account number, create five digits PIN and the registration is complete.

Services available on this platform are: funds transfer, air time top-up, bills payments among others. For example, to send money, customers simply dial *894*Amount*Recipients Account Number#, select beneficiary bank, confirm amount, beneficiary name and enter five digits PIN created during registration and select account to debit.

Maximum single transaction and daily transfer limit is =N= 100, 000.00 and all transactions require five digits PIN.

b. USSD Code for Guarantee Trust Bank

The USSD code for Guarantee Trust Bank (GTBank) is *737#. To register or create transfer PIN, customers dial *737*5# with their phone number registered with GTBank, select option 1 from the menu presented to activate with ATM card or 2 to activate with account number depending also on whether they are activating with the ATM card or account number. If option 1 which is to activate with ATM is selected, the customer is prompted to enter the last 6 digits of the card, else if option 2 which is to activate with account number is selected, customer is prompted to enter the 10 digits account number. Afterwards any 4 digits that can easily be remember is entered to create new PIN or change existing transfer PIN and a confirmation of the entered PIN is checked by typing it again to complete the activation process. Services offered include; funds transfer, airtime recharge, bills payment, donations, generate OTP, balance enquiry etc: For instance, to transfer funds to GTBank account, users dial *737*1*Amount* Account Number# (example. *737*1*1000*1234567890#) from the phone number registered with GTBank, then follow the on-screen prompts. Transfer to other Banks, dial *737*2*Amount*Account Number# (e.g. *737*2*1000*1234567890#) from the registered phone, then authenticate the transfer with 737 PIN created, hardware token or last four digits of your GTBank debit card.

Daily transaction limit is =N=1,000,000 while =N=100 to 500,000.00 requires 737 PIN/hardware Token only, =N= 500,001.00 to 1,000,000.00 requires hardware token only. Transaction may also require the last 4 digits of ATM card (GTB, 2017). OTP can also be received on the USSD platform for transactions up to 500,000.00

c. USSD Code for First City Monument Bank

First City Monument Bank (FCMB) USSD code is *329#. Users must register to get started by dialling *329# from the registered phone with the bank. With the use of their account number or ATM card number they then create their transaction pin to access the FCMB USSD. The PIN (ATM PIN) and Transaction Code (USSD transaction PIN) are required to access the USSD banking services provided by this platform. Transfers beyond =N=20,000.00 requires both PIN and transaction code while transfers bellow 20,000.00 requires only transaction code. To access all services available on the platform customer dials *329# and follow the menu. Services available include; airtime top-up, transfer funds among others. For funds transfer customers simply dial, *329*amount* recipients account number# follows the onscreen prompt and completes the transaction with the PIN.

Cumulative transfer limit is N100, 000.00 (One hundred thousand Naira) daily.

d. USSD Code for Fidelity Bank

The USSD code for Fidelity Bank is *770#. To register users simply dial *770# on their mobile phone, select 1 for Instant Banking 770, enter Fidelity account number, Setup a 4-digits PIN or password and registration is complete. PIN/password is required for all transactions on instant banking except for self-recharge. Services available are funds transfer, airtime top-up, balance enquiry, ATM card less withdrawal, etc.

e. USSD Code for United Bank for Africa

The USSD code for United Bank for Africa (UBA) is *919#. Getting started, you must first register on the platform by dialling *919# from a registered phone number with UBA and input any number for the banking option that shows up on the menu. A welcome page where you will be asked to enter option 1 to sign up will be displayed. You must choose between registering with a UBA account number or prepaid card. To register with account number, 10 digits UBA account is entered and Bank Verification Number (BVN) then a magic banking

PIN is created. To register with prepaid card, a prepaid card is selected, the last 4 numbers on the card is entered and a magic PIN is created. Then the PIN is confirmed to complete the registration.

Services offered include funds transfer, airtime to-up, balance enquiry among others and follows the same pattern as the other banks but initiated by dialling *919#. For example, to transfer to another UBA account dial *919*3*account number*amount# from the phone number you registered with UBA, complete the transaction with the PIN created during registration. To transfer to other banks dial *919*4*account number*amount#, choose the beneficiary's bank, confirm the recipient's details and complete the transfer with the transaction PIN created during registration.

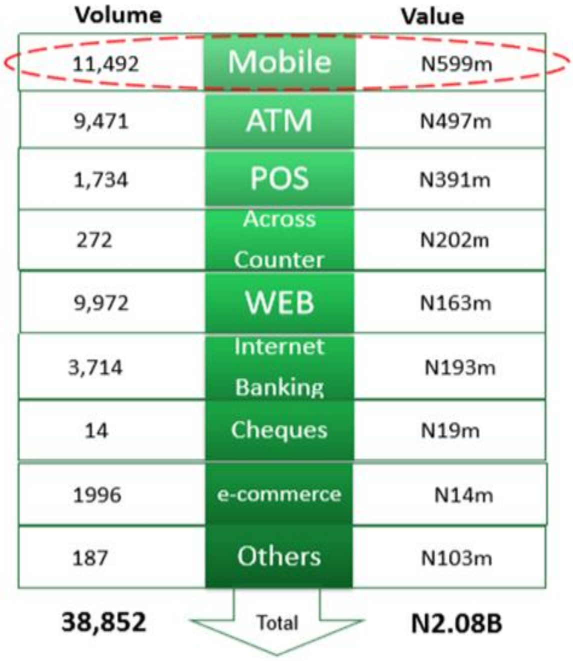
f. USSD Code for Zenith Bank

USSD code for Zenith Bank Nigeria is *966#. To register user's dial *966# from an AlertZ number (the phone number used to receive alert from your zenith bank account), enters the last 4 digits of Zenith bank debit card, create 4 digits PIN and confirm PIN to complete the registration. Services offered include balance enquiry, fund transfers, airtime top up among others. For balance enquiry users dial *966*00#, enter 4 digits PIN and a message, "Retrieving balance, you will receive an SMS shortly" is displayed, customer then gets an SMS with balances on his account (Savings and Current). For fund transfers users dial *966*amount*account number#, select beneficiary bank by entering the corresponding number. After the selection, a confirmation page is displayed showing beneficiary name, bank and the amount and a prompt to enter your 4 digits PIN, if successful, a message is displayed showing the transferred amount, beneficiary's account number and the senders account balance. Cumulative transfer limit is =N=100,000 (One hundred thousand Naira) daily.

C. Existing Literatures on Mobile banking Related Frauds

Mobile banking plays a key role in our individual lives and the economy as it provides ease of banking from the fingertip of the customer anywhere any time. It also has impacted positively on employee job security as it has substituted labour intensive processes by rendering some skills obsolete through the deployment of high level information technology skills in financial institutions (Babatunde and Sunday, 2017; Onodugo, 2015). It has also improved service delivery by banks in terms of convenience and reduced cost and time of rendering services to customers (Adewole, 2013). Therefore, the volume and value of transactions performed on this channel increase every year from the previous year (Fadoju et al., 2018).

Despite the convenience offered by USSD to customers in accessing banking services, the technology is still faced with threats of fraud. Mobile banking fraud increases exponentially with its increase in awareness, sophistication and availability. Adebisi Shonubi, Managing Director, NIBBS, disclosed that "while fraud trend is generally on the decline, mobile fraud trend alone is on the increase." He said that mobile fraud would overtake ATM fraud by 2020 with the rate of increasing fraud in the channel. He listed the top three mobile threats in Nigeria to include phone theft, SIM swaps and kidnap (INDEPENDENT, 2018). Mobile fraud volume for 2017 and 2018 stood at 5,055 and 11,492 and actual loss value was 347,645,783.00 and 598,811,187.60 respectively (Ibanichuka and Oko, 2019). Figure 2 shows the overview of fraud loss in Nigeria as at 2018.



Volume		Value
11,492	Mobile	N599m
9,471	ATM	N497m
1,734	POS	N391m
272	Across Counter	N202m
9,972	WEB	N163m
3,714	Internet Banking	N193m
14	Cheques	N19m
1996	e-commerce	N14m
187	Others	N103m
38,852	Total	N2.08B

Figure 2: Overview of fraud landscape in Nigeria (Source: EFInA (2019))

Researches on strengthening the security of USSD applications of Nigerian banks are scarce. Most of the researches focus on the analysis of the impact, effect and cost among others of frauds perpetrated through electronic banking channels rather than the application itself. For instance, Muoghalu et al., (2018), researched on how frauds on electronic channels impacts on the performance of deposit money banks in Nigeria, with focus on automated teller machines, mobile banking, point of sale terminals and web. The Ordinary Least Square (OLS) was applied in estimating the regression equation to ascertain return on assets, return on equity, interest income and non-interest income of deposit money banks. The study concludes that electronic banking fraud has negative and devastative effect on financial performance of deposit money banks in Nigeria.

In the same vein, Braimah and Okonkwo (2016) investigated the fraud actual loss amount in Nigeria between the period of 2013 and 2014 statistically. They adopted Standard Cumulative Sum (CUSUM) technique to monitor e-fraud rate in Nigeria for two years. It was observed that the fraud rate was in statistical control, though on the increasing trend.

In another research by Olatunde and Fasunle (2019), on the nature of electronic banking related fraud on deposit money banks in Nigeria, it effects and the controls put in place to prevent financial loss, it was revealed that e-banking significantly increased the volume of banking transactions and improved service delivery to customers by making it easier. However, it also showed that the effect of electronic fraud results in loss of money which belongs to either the bank or customers and could also destroy the bank's reputation among others. Therefore, the researchers concluded that despite the security problems associated with electronic banking practice in Nigeria, it has improved the operational efficiency of banks. Based on these findings, the researchers recommend that Government through CBN should provide adequate security measures for various electronic banking channels, review BVN framework and sensitize customers on electronic banking operations among others.

D. Gaps Identified from Literature

From the review of literatures above, the following gaps were identified:

i. The customers PIN and second level authentication factor 2FA can be received or displayed on the USSD menu for some banks which compromises other electronics channel such as ATM. This is against the CBN guideline

ii. The second level authentication factor used by most banks is the ATM PIN which puts at risk both the ATM and USSD.

iii. Any one in possession of users' device (mobile phone) and ATM card can easily transact using the device in the case where a customer's bag containing those items are stolen, which is likely.

iv. PINs are displayed on the USSD platform as figures instead of asterisks which can easily be stolen by shoulder surfing

v. Development of more secured USSD mobile platforms or applications in Nigeria are scarce.

Therefore, this paper provides an enhanced second level authentication factor using answer to a secret question registered with the bank and also provides a platform that hides the PIN using asterisks to avoid PIN theft through shoulder surfing, to alleviate identity theft.

III.METHODS AND MATERIALS

Investigation of USSD platforms of some Nigerian banks and how they operate was carried out through practical use of the platforms, direct interview of customers on their experiences with the platform and existing literatures where also investigated. It was observed that customers PIN could easily be stolen by shoulder surfing since it is not encoded. Hence, with the PIN handy, anyone in possession of user's device (phone) and ATM can easily have access to the USSD platform, especially, when the users' stolen SIM is used to register for USSD transaction for the first time. Therefore, this system developed a second factor authentication model using secret question to provide a more secured platform against identity theft, in other to minimise frauds committed on USSD platform using stolen SIM card to register on USSD platform.

Assumptions are that:

i. A person opening an account in the bank must provide an answer to a secret question known only to him/her on the account opening platform
ii. An existing customer must also update his/her account with an answer to a secret question.

For the user to be able to use the USSD platform, the user must provide in addition to the ATM PIN and Transaction PIN, the answer to the secret question. This answer must not be less than 8 characters. The answer is in text format but translated to numbers in the database with the letters Aa to Zz represented by their corresponding numbers on the phone keyboard. The proposed system was modelled using pseudo-code inform of algorithm and flowchart as presented in Figure 3 and algorithm 1.

The model was further implemented using php programming language and mysql database on XAMPP (Cross-Platform, Apache, Mysql, Php, and Perl) application v3.2.4. The performance of the system was tested through simulation in windows 10 and Google chrome browser using hubtel USSD Mocker. Hubtel USSD Mocker Provides a user-friendly interface and a USSD flow that mimics a real USSD session, and runs on nodejs-12.16.1-0 application server. The node js server is launched by running a windows batch file

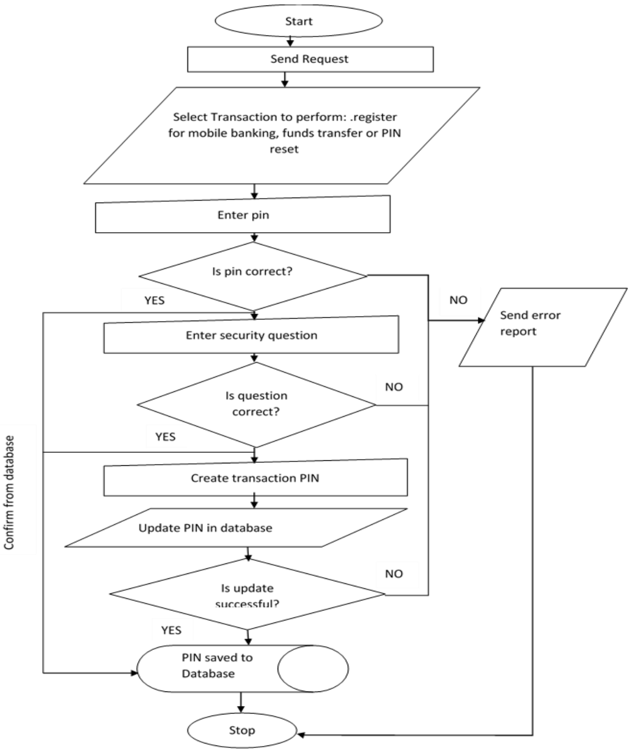


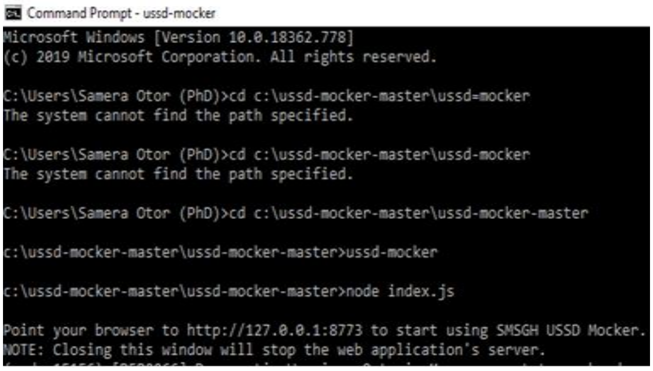
Figure 3 : Flowchart of Security Flow of Proposed Model

Algorithm 1: Proposed System Algorithm

```
Input: ussdRequest->Message
Output: ussdResponse->Message
1.Initiate the session by dialing *123*1# from the hubtel USSD mocker platform
2.USSD Session is initiated
```

```
    Switch(ussdRequest->Type){
    Case 'initialization'
    ussdResponse->Message = Welcome to Sami Mobile Banking.
    i. Open Account ii. Register for Mobile Banking iii. Account Balance. iv Reset Pin.v. About App.vi Transfer
    break;
3.Select from options in 2
    Case 'Response'
    if (ussdRequest->Message=='i'){
ussdResponse->Message = 'Select Account Type '
xi.Savings
xii.Current
0. Exit
}elseif(ussdRequest->Message=='ii'){
ussdResponse->Message = 'Register with '
xiii. Card.
xiv. No Card
0. Exit
}elseif(ussdRequest->Message=='iii'){
ussdResponse->Message = "Enter your 10-digit Account number "."\n0. Exit";
}elseif(ussdRequest->Message=='iv'){
          ussdResponse->Message = "Enter Old Pin "."\n0. Exit";
}elseif(ussdRequest->Message=='v'){
ussdResponse->Message = about()."\n0. Exit";
}elseif(ussdRequest->Message=='vi'){
ussdResponse->Message = 'Select Recipient Bank '
lxxi. Access
lxxii. FCMB
lxxiii. FBN
lxxiv. Fidelity Plc
lxxv. GTB
lxxvi. UBA
lxxvii. Union Bank
lxxviii. Zenith Plc
0. Exit";
}
if(ussdRequest->Message=='xi'OR ussdRequest->Message=='xii') {
ussdResponse->Message = 'Thank you. An agent will contact you shortly. ';
}if(ussdRequest->Message=='xiii' ){
ussdResponse->Message = 'Enter the last 6 digits of your ATM card'."\n0. Exit ";
}elseif(ussdRequest->Message=='xiv' ){
ussdResponse->Message = 'Enter your 10-digit Account number'."\n0. Exit ";
}elseif(ussdRequest->Sequence=='3'AND (strlen($ussdRequest->Message)==10 OR strlen($ussdRequest->Message) ==6)){
Confirm_account= ussdResponse->Message
If confirmed{
ussdResponse->Message = Account Balance
}}elseif(ussdRequest->Sequence=='3'AND (strlen(ussdRequest->Message)>10)){
ussdResponse->Message = 'Invalid Entry. ';
}if(ussdRequest->Sequence=='4'AND (strlen(ussdRequest->Message)==6)AND is_numeric($ussdRequest->Message)){
confirm_ATMnumber=ussdRequest->Message
if confirmed
ussdResponse->Message =  Enter the 4 digit pin for this card "\n0. Exit ";
}}elseif(ussdRequest->Sequence=='4'AND (strlen(ussdRequest->Message)==10)AND is_numeric(ussdRequest->Message)){
confirm_accnumber= ussdRequest->Message
 if confirmed{
ussdResponse->Message = "Enter the 4 digit pin for this card"."\n0. Exit ";
}}if((ussdRequest->Sequence=='5'OR ussdRequest->Sequence=='3')AND (strlen(ussdRequest->Message)==4)AND is_numeric(ussdRequest->Message)){
ussdResponse->Message = "Enter answer to security question"."\n0. Exit";
}if(ussdRequest->Sequence=='6'AND (strlen(ussdRequest->ClientState)==4)){
ussdResponse->Message = 'Create a 5-digit pin for transactions'."\n0. Exit ";}if((ussdRequest->Sequence=='7'OR $ussdRequest->Sequence=='5')AND (strlen(ussdRequest->Message)==5)){
update the customers information by saving the pin in the database
$sql = "UPDATE customers SET fivedigitpin ='$ussdRequest->Message' WHERE custname='$custname'";
if (mysqli_query($conn, $sql)) {
ussdResponse->Message = 'Registration Successful';
else{ussdResponse->Message = 'Registration failed'.mysqli_error($conn);
if($ussdRequest->Sequence=='3'AND ($ussdRequest->ClientState=='4' )){
ussdResponse->Message = 'Enter the answer to your security question,not less than 8 characters'."\n0. Exit "
}if(ussdRequest->Sequence=='3' AND(ussdRequest->Message=='71'OR ussdRequest->Message=='72' OR ussdRequest->Message=='73'OR ussdRequest->Message=='74' OR ussdRequest->Message=='75'OR ussdRequest->Message=='76' OR ussdRequest->Message=='77'OR ussdRequest->Message=='78')){
ussdResponse->Message = 'Enter your 4-digit pin'."\n0. Exit ";
}if(ussdRequest->Sequence=='4'AND (strlen($ussdRequest->Message)==8)){
ussdResponse->Message = 'Create a 5-digit pin for transactions'."\n0. Exit ";}if(ussdRequest->Sequence=='4'AND (ussdRequest->ClientState=='71'OR $ussdRequest->ClientState=='72'OR $ussdRequest->ClientState=='73'OR ussdRequest->ClientState=='74'OR ussdRequest->ClientState=='75'OR ussdRequest->ClientState=='76'OR ussdRequest->ClientState=='77'OR ussdRequest->ClientState=='78')){
ussdResponse->Message = "Enter Recipient Account Number ";
}if(ussdRequest->Sequence=='5'AND strlen(ussdRequest->Message)==10AND is_numeric(ussdRequest->Message)){
ussdResponse->Message = "Enter the answer to your security question ";
}if(ussdRequest->Sequence=='6'AND strlen(ussdRequest->ClientState)==10AND is_numeric(ussdRequest->Message)){
ussdResponse->Message = "Enter Amount:\n Then enter # key at the end";
}if(substr(ussdRequest->Message,-1)=='#'AND strlen(ussdRequest->Message)>0){
ussdResponse->Message = "Transaction Successful ";
break;
default:
ussdResponse->Message = "Good bye";
break;}
4.Encode the response object as JSON and send.
echo json_encode(ussdResponse);}
5.End.
```

ussd-mocker.bat which opens the application server on the windows command prompt as shown in Figure 4. The URL of the server is then copied to the web browser to start the USSD session. The hubtel USSD mocker provides a user interface that serves as the users' phone and a session initiator with the parameters set up as seen in Figure 5. This interface interacts with the user application in XAMPP to initiate a USSD session. Relating this to the real life USSD architecture the user interface serves as the phone, the hubtel mocker session serves as the gateway that interacts with the application server (XAMPP) and the financial institution server (nodejs). A real-life test was not carried out because it involves using a banks server, financial card institutions such as Interswitch and mobile operators such as MTN which are not easy to access due to security reasons

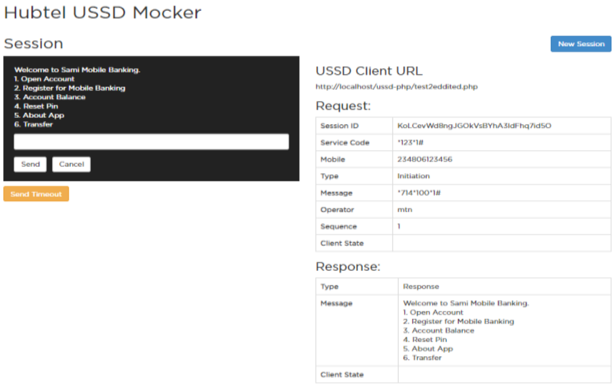


```
Command Prompt - ussd-mocker
Microsoft Windows [Version 10.0.18362.778]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\Samera Otor (PhD)>cd c:\ussd-mocker-master\ussd=mocker
The system cannot find the path specified.

C:\Users\Samera Otor (PhD)>cd c:\ussd-mocker-master\ussd-mocker
The system cannot find the path specified.

C:\Users\Samera Otor (PhD)>cd c:\ussd-mocker-master\ussd-mocker-master

c:\ussd-mocker-master\ussd-mocker-master>ussd-mocker

c:\ussd-mocker-master\ussd-mocker-master>node index.js

Point your browser to http://127.0.0.1:8773 to start using SMSGH USSD Mocker.
NOTE: Closing this window will stop the web application's server.
```

Figure 4: USSD Mocker.bat command prompt

IV. THE USSD MODEL IMPLEMENTATION

This will focus on the security aspects of the application. They include; registration for USSD, PIN reset and Fund transfers as follows:



Hubtel USSD Mocker

Session

Welcome to Sami Mobile Banking.
1. Open Account
2. Register for Mobile Banking
3. Account Balance
4. Reset Pin
5. About App
6. Transfer

USSD Client URL

http://localhost/ussd-php/test2eddited.php

Request:

Session ID	KoLCevWd8ngJGOkVsBYhA3ldFhq7id5O
Service Code	*123*1#
Mobile	234806123456
Type	Initiation
Message	*714*100*1#
Operator	mtn
Sequence	1
Client State	

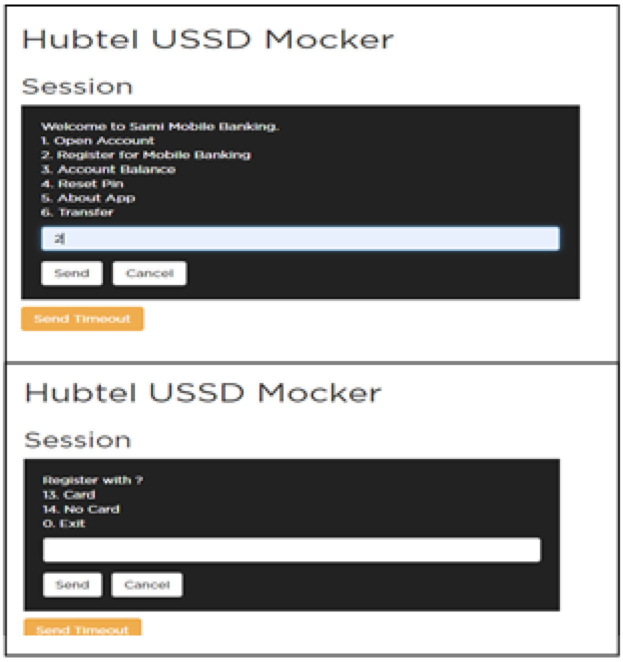
Response:

Type	Response
Message	Welcome to Sami Mobile Banking. 1. Open Account 2. Register for Mobile Banking 3. Account Balance 4. Reset Pin 5. About App 6. Transfer
Client State	

Figure 5: Hubtel USSD Mocker User Interface and Session parameters

A. Register for Mobile Banking

As soon as a session is initiated using the parameter set up in Figure 5, to register for mobile banking the user selects option 2. The system prompt user to register with either ATM card or no ATM (in this case the customer will have to register with ten-digit account number) as shown in Figure 6. If the user selects option 13, the customer is prompted for the last six digits of the ATM card else if its option 14 the customer is asked to supply ten digits account number as shown in Figure 7.



Hubtel USSD Mocker

Session

Welcome to Sami Mobile Banking.
1. Open Account
2. Register for Mobile Banking
3. Account Balance
4. Reset Pin
5. About App
6. Transfer

2

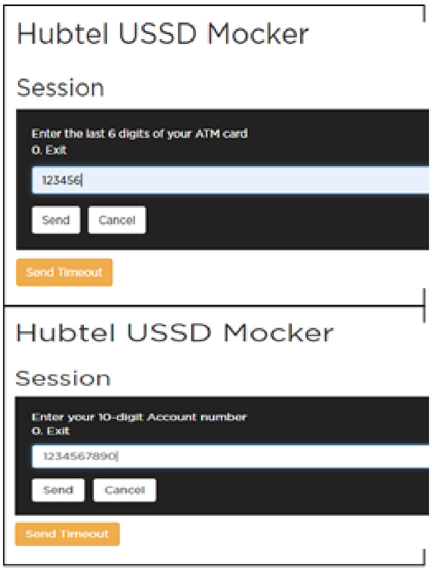
Hubtel USSD Mocker

Session

Register with ?
13. Card
14. No Card
0. Exit

Figure 6: USSD Session Home Page Showing Selection of Option 2 and its Response

Afterwards, the customer is prompted for his/her ATM PIN which in the proposed system is displayed as asterisks instead of plain figures displayed by existing system to minimise PIN theft through shoulder surfing. Furthermore, the customer will have to provide the answer to security question as another level of authentication as shown in Figure 8. If the PIN and Security question are correct, the user is asked to create 5 digits transaction PIN and registration is complete



Hubtel USSD Mocker

Session

Enter the last 6 digits of your ATM card
0. Exit

123456

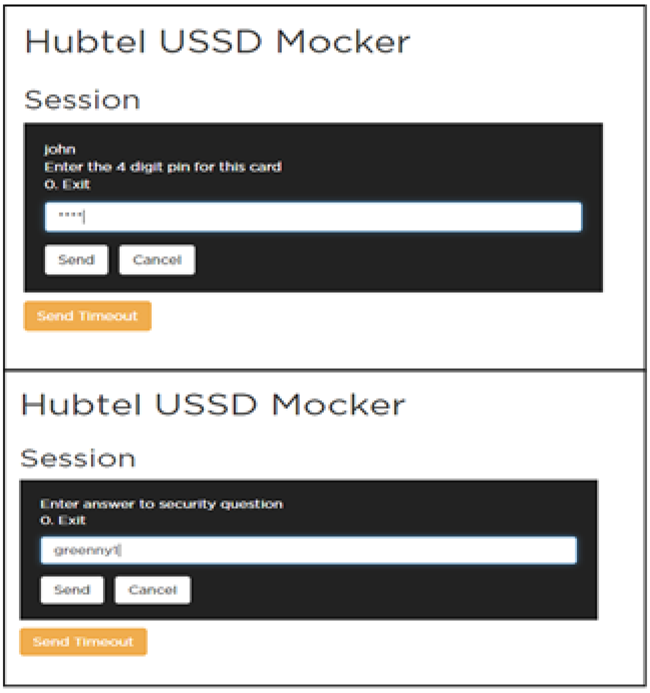
Hubtel USSD Mocker

Session

Enter your 10-digit Account number
0. Exit

1234567890

Figure 7: Response for Option 13 and 14



john
Enter the 4 digit pin for this card
0. Exit

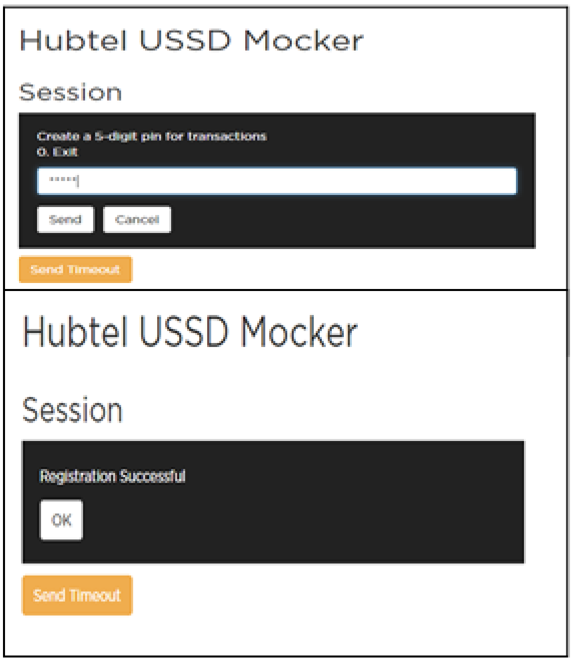
****

Enter answer to security question
0. Exit

greenny1

Figure 8: Authenticating User with Four Digit PIN and Answer to Security Question

with a Registration Successful message as shown in Figure 9



Create a 5-digit pin for transactions
0. Exit

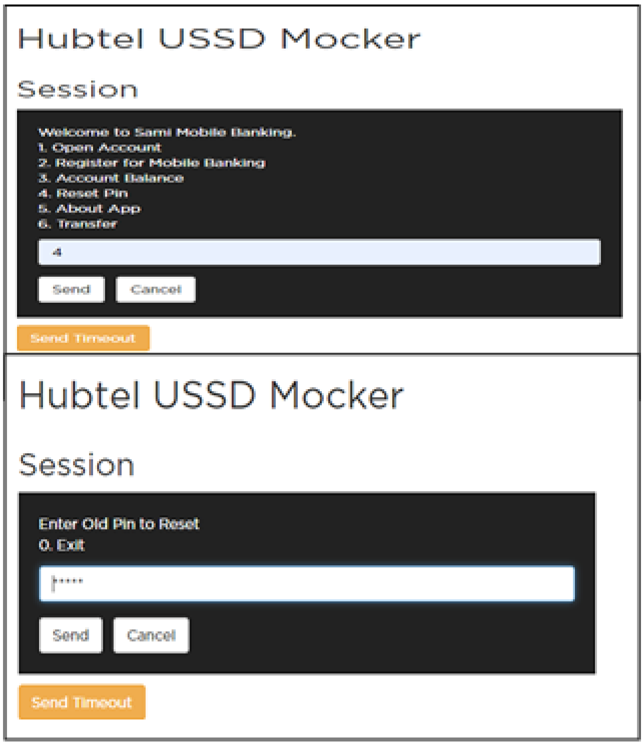
*****

Registration Successful

Figure 9: Creation of 5 Digit PIN to Register Successfully.

B. Pin Reset

To reset old PIN the customer selects option 4 from the home page. In other to asertain the authorised user, the customer is prompted to supply the old PIN as shown in Figure 10. To further minimise identity theft, the customer is asked to provide the answer to security question before a new PIN is created to reset the old PIN as shown in Figure 11.



Welcome to Sami Mobile Banking.
1. Open Account
2. Register for Mobile Banking
3. Account Balance
4. Reset Pin
5. About App
6. Transfer

4

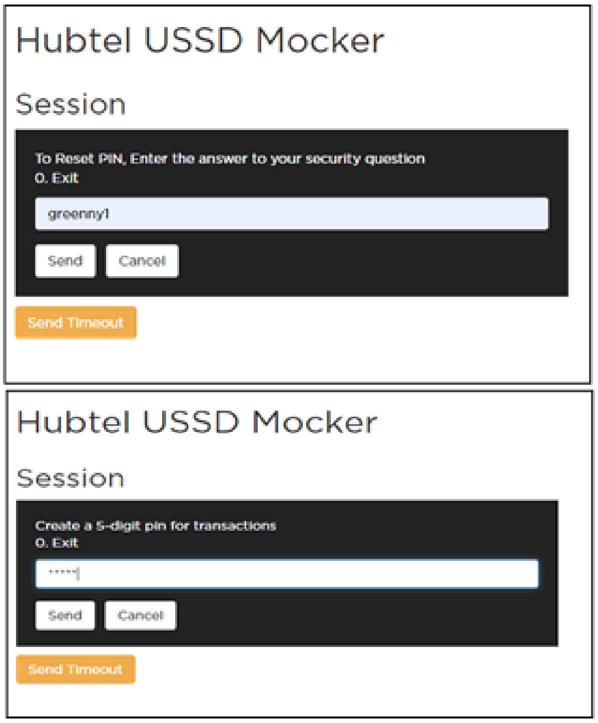
Enter Old Pin to Reset
0. Exit

*****

Figure 10: PIN Reset Option and its Response

C. Funds Transfer

To transfer funds, customer selects option 6 from the home menu options. Then, the customer is prompted for recipients account number, bank details and amount as usual, then authenticates the transfer with the 5-digit transaction Pin. However, in addition to the 5 digits transaction PIN created during registration, the proposed system requests for the answer to security question as a second level of authentication to minimise identity theft. It's as shown in Figure 12.



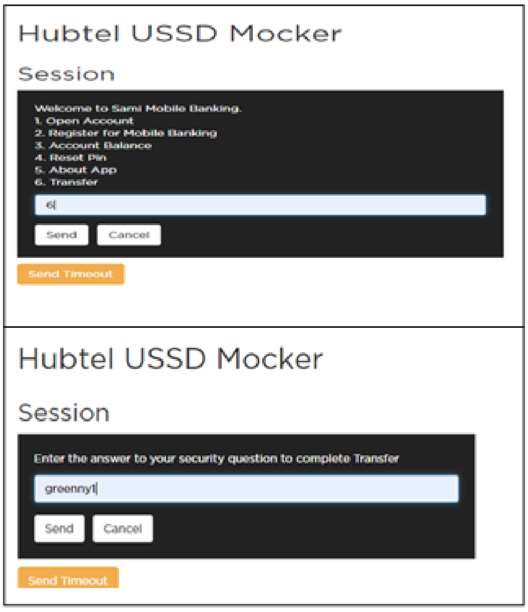
To Reset PIN, Enter the answer to your security question
0. Exit

greenny1

Create a 5-digit pin for transactions
0. Exit

*****|

Figure 11: Authenticating User with Security Question to Reset Pin



Welcome to Sami Mobile Banking.
1. Open Account
2. Register for Mobile Banking
3. Account Balance
4. Reset Pin
5. About App
6. Transfer

6|

Enter the answer to your security question to complete Transfer

greenny1|

Figure 12: Authenticating Funds Transfer with Answer to Security question

V. DISCUSSIONS

The results of the comparison of the Existing USSD mobile banking implementations and the proposed solution using, security, cost, speed, time spent on transaction and transmission speed as metrics are as shown in Table 1.

Table 1: Existing USSD mobile banking solutions versus the proposed solution

Metrics	Existing USSD Platform	Proposed USSD Platform
Security	Authentication is done using ATM PIN and 4 digits Transaction PIN, both displayed as plain figures on the platform. This is not fully secured because a customer's stolen bag containing his/her phone and ATM card can easily be registered and used by fraudsters to perform USSD transaction. Furthermore, Displaying the PINs as plain figure can lead to PIN theft through shoulder surfing.	Authentication is done using ATM PIN, 5-digit transaction PIN both displayed as asterisk and an answer to a security question. Displaying PIN as asterisk minimises PIN theft through shoulder surfing, furthermore adding another level of authentication using security question helps to minimise access to the platform especially for users whose stolen SIM card are used for the first time on the platform
Cost	Free: USSD depends on mobile providers network no charges	Free: USSD depends on mobile providers network no charges
Time Spent on Transaction	Time spent is less because the level of user feedback is less	Time spent on transaction is higher because, introducing another level of authentication increases users' feedback.
Transmission Speed	The speed of transmission of mobile solutions depends on several factors: i. It depends on the strength of the signal received from mobile providers' network. This signal depends on the location of the user, the traffic of the network, the number of base towers in the area around the users mobile and etc. ii. it also depends on the user's device specifications such as the memory size, RAM, the number of running applications at that particular time etc. All these factors can influence the speed of transmission; thus, no actual experiment was conducted.	

VI. CONCLUSION AND RECOMMENDATIONS

It has been observed over the years that one of the major targets of thieves and robbers is the victim's ATM card and mobile phone. This is due to the advent of electronic and mobile banking, ease of access to customers' funds in the bank. Therefore, the rate at which customers' identities are breached on most electronic banking platforms such as USSD platform is also on the increase, especially when the fraudster is in possession of the authorised user's ATM card and PIN and the user is yet to register on these platforms. In this paper an enhanced USSD platform for mobile banking was developed. The proposed system employed an answer to a security question provided by the customer to create a second level of authentication in other to minimise identity theft. This security answer is provided by the customer during the account opening for new customers and an existing customer can still update his information in the bank before registering for USSD. However, the security answer is only shared between the customer and the bank server. The proposed system was implemented using PHP and simulated using Hubtel USSD mocker as a cross platform to initiate the USSD session.

Simulation results using security, cost, time spent on transaction and transmission speed showed that the system was able to meet specified requirement of a more secured platform by providing a second level of authentication to minimise identity theft.

In future, we recommend a real live test of this system in other to test users' satisfaction and application performance index.

A behavioural monitoring system is also recommended to mitigate identity theft through SIM swap.

VII. REFERENCES

[1]. Adewole, J. O. (2013). Impact of Mobile Banking on Service Delivery in the Nigerian Commercial Banks. International Review of Management and Business Research. Vol.2 No.2, pp 333-344.

[2]. Babatunde, O., and Sunday, O. (2017). E-Banking in Nigeria: Issues and Challenges. Research Journal of Finance and Accounting , Vol.8 No.6, pp 16-24.

[3]. Baraka, N., Anael, S., and Loserian, L. (2013). Enhanced Security Model For Mobile Banking Systems In Tanzania. International Journal of Technology Enhancements and Emerging Engineering Research, Vol.1 No. 4, pp 4-20.

[4]. Braimah, O., and Okonkwo, I. (2016). Statistical Monitoring (SM) of Electronic Fraud Occurring in Nigerian Banks . Advances in Multidisciplinary Research Journal. Vol.2 No.3, pp 93-104.

[5]. Department of Banking and Payments System, Central Bank of Nigeria (CBN, 2018). Regulatory Framework For The Use Of Unstructured Supplementary Service Data (Ussd) For Financial Services In Nigeria . Abuja: Central Bank of Nigeria, Online] https://www.cbn.gov.ng/Out/2018/BPSD/USSD %20Regulatory%20Framework.pdf. (Accessed 20 April, 2019)

[6]. Enhancing Financial Innovation and Access EFInA. (2019). Overview of Mobile Financial Services Fraud in Nigeria: Building Trust to increase Uptake and Usage A Presentation at the Mobile Payments Fraud Forum of June 11, 2019. Online] https://www.efina.org.ng/wp-content/uploads/2019/06/Overview-of-Mobile-Financial-Services-Fraud-in-Nigeria.pdf. (Accessed 11 February 2020)

[7]. Fadoju, O. S., Evbuomwan, G., Olokoyo, F., Oyedele, O., Ogunwale, O., and Kolawole, O. O. (2018). Dataset for electronic payment performance in Nigerian banking system: A trend analysis from 2012 to 2017. Elsevier journal of Data in Brief , Vol.20 No.20, pp 85–89.

[8]. Guaranty Trust Bank Nigeria GTB *737# Features, (2017). Online]: https://737.gtbank.com/features#110 (Accessed 23 April 2020)

[9]. Ibanichuka, E., and Oko, I. A. (2019). Electronic Fraud and Financial Performance of Quoted Commercial Banks in Nigeria. International Journal of Advanced Academic Research | Management Practice , Vol.4 No.4, pp15-35.

[10]. INDEPENDENT. (2018). Independent news paper. Nigerian Banks Lose N12.30bn To Fraud In Four Years Online] : https://www.independent.ng/nigerian-banks-lose-n12-30bn-to-fraud-in-four-years/ (Accessed 23 April 2020)

[11]. Muoghalu, A. I., Okonkwo. Jisike, J., and Ananwude, A. C. (2018). Effect of electronic banking related fraud on deposit money banks financial performance in Nigeria . Discovery, Vol.276 No.54 pp 496-503.

[12]. NCC. (2011), The Nigerian Communications Commission Nigerian Communications Act 2003: Guidelines On Short Code Operation In Nigeria. Nigerian Communication Commission Abuja, Online] https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=14&cad=rja&uact=8&ved=2ahUKEwjuluq2waDlAhVGh1wKHak9D7EQFjANegQIARAC&url=https%3A%2F%2Fwww.ncc.gov.ng%2Fdocman-main%2Flegal-regulatory%2Fguidelines%2F141-guidelines-on-shortcode-operation-in-nig (Accessed 16 October, 2019)

[13]. Olatunde, O. J., and Fasunle, F. A. (2019). Electronic Banking Fraud in Nigeria: Effects and Controls . Global Scientific Journals Vol.7 No.8, pp52-65.

[14]. Onodugo, I. C. (2015). Overview of Electronic Banking in Nigeria. International Journal of Multidisciplinary Reseaerch and Development , Vol.2 No.7, pp336-342.

Cite this article as :

Samera Uga Otor, Beatrice Obianiberi Akumba, Joseph Sunday Idikwu, Iorwuese Peter Achika, "An Improved Security Model for Nigerian Unstructured Supplementary Services Data Mobile Banking Platform ", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 6, Issue 3, pp.974-987, May-June-2020.
Available at
doi : https://doi.org/10.32628/CSEIT2063213
Journal URL : http://ijsrcseit.com/CSEIT2063213