Academic City University College, Accra, Ghana
Society for Multidisciplinary & Advanced Research Techniques (SMART)
Trinity University, Lagos, Nigeria
SMART Scientific Projects & Research Consortium (SMART SPaRC)
Harmarth Global Educational Services
ICT University Foundations USA
IEEE Computer Society Nigeria Chapter

33rd ECOWAS iSTEAMS ETech Multidisciplinary Conference (ECOWAS-ETech)

USSD Channel Resilient System for Financial Transactions: A Preliminary Study

Binitie, A.P., Egbokhare, F., Egwali, A.O., Kadiri, K.C. & Akhator, D.N.
[1,4,5]Dept. of Computer Science, FCE (T), Asaba, Nigeria
[2,3]Dept. of Computer Science, University of Benin, Benin City, Nigeria
E-mails: philpat4sure@gmail.com; fegbokhare@uniben.edu.ng, annie.egwali@uniben.edu.ng; Kc.mrose.kk@gmail.com; Akhatordoris@gmail.com
Phones: +2347035901508; +2348037180057, +2347033247730, +2348067857692, +2348100349200

ABSTRACT

Unstructured Supplementary Service Data (USSD) is a technology that is built into the Global System for Mobile Communication (GSM) standard. Services like account balance checks, banking transactions, and so on can be carried out on mobile devices through USSD. Banks make use of USSD technology in offering bank services to their customers. Many financial institutions in Africa and other countries have adopted USSD technology as a means of providing convenient financial services to their customers irrespective of their GSM phone type, location, time, as long as network service is available. Sensitive details carried through the USSD channel are in plaintext and can easily be retrieved by an attacker. Stakeholders involved in each USSD transaction ranges from registered customers down to application service providers. To identify the possible vulnerable attack points in USSD banking transactions and the existence of security measures at these points, this research, therefore, used a qualitative data collection method to collect data from the information technology staff of seventeen (17) commercial banks in Nigeria. The data obtained were analyzed using a deductive thematic approach and found that all the points through which the data passes can be attacked, but some points applied some form of security while points like mobile interface have no form of security. The security of the mobile interface is left for users. Finally, a method is proposed for security of data at mobile interface against shoulder surfing, during transaction.

Keywords— USSD, qualitative analysis, sensitive data, banking, vulnerable points.

Proceedings Citation Format
Binitie, A.P., Egbokhare, F., Egwali, A.O., Kadiri, K.C. & Akhator, D.N. (2022): USSD Channel Resilient System for Financial Transactions: A Preliminary Study. Multidisciplinary Conference. University of Ghana/Academic City University College, Ghana. 29th Sept – 1st Oct, 2022. Pp 249-260-. www.isteams.net/ecowasetech2022.
dx.doi.org/10.22624/AIMS-/ECOWASETECH2022P44

1. INTRODUCTION

USSD is a capability built into the global system for mobile communication (GSM) standard, which allows high speed, bidirectional communications between mobile handsets and applications (Globital, 2018; Bharat, 2015). This means it is available on all GSM mobile phones including low-level phones (2G mobile phones). It allows customers to request information regarding an account and also carry out other transactions (Chandran, 2014). The stakeholders involved in USSD communications are the customer at the front end, the mobile network operator, the USSD gateway handler at the middle, and the Content provider at the back end.

USSD has a number-dialing interface and does not require Internet which makes it easy to use by everyone. USSD can be Menu based or non-Menu- based. USSD codes or simply "short-codes" are formed using *, # keys, and a combination of an intermediate set of digits/ parameters, (0-9). The codes are standard messages predefined in the USSD platform (Sanganagouda, 2011). It can have variable lengths separated by the "*" key.

All mobile financial service providers (mobile money operators, banks, payment services, and so on) operate unique codes in providing USSD services to customers. All USSD strings are registered with the Mobile Network Operator (MNO) for the MNO to recognize where to send the request. USSD technology is text-based hence it accepts only PIN for authentication but when a third-party application is provided for security, further features like primary biometrics and hashing algorithm can be embedded in the application (Handson, 2016). Users' PIN appears in plaintext on mobile interfaces as a result of Banks' server security policy (Nyamtiga et al., 2013). This is because, the encryption algorithm on the GSM network has been reverse engineered (Briceno et al., 1999) thereby putting sensitive data moving through the network (from the mobile application level through the service providers' level to the financial back-end infrastructure) at risk (Gupta, 2010).

This technology has been adopted by banks in carrying out banking transactions (Nyamtiga et al., 2013). The availability of USSD technology on feature phones makes it easy for banks to gain wider coverage of their banking services. Security of users' data is important to the mobile user that has keyed into USSD banking transactions today. This research aims to identify potential points of vulnerability in USSD deployment of mobile banking service architecture.

2. USSD BANKING ARCHITECTURE

The use of USSD in mobile banking is invoked by a registered customer and the request is received by the USSD Gateway through the Mobile Network Operator (MNO) and the Technology Vendor as shown in Figure. 1. The gateway forwards the request to the application server that communicates with the bank to service the requested transaction. The server response is returned through the 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.

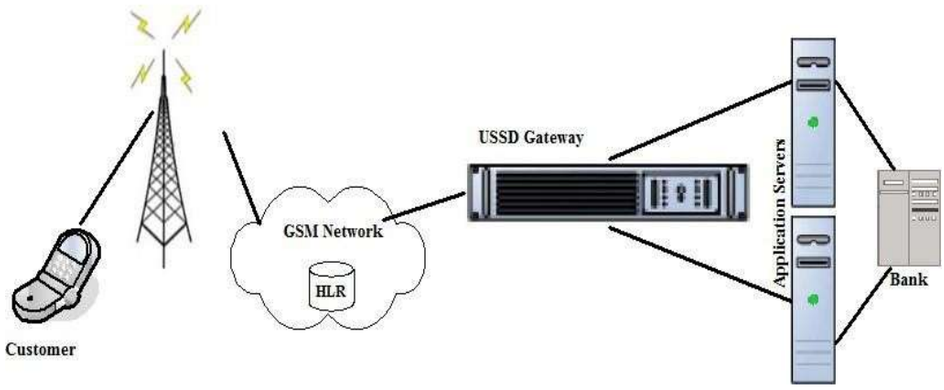

Figure 1. USSD Banking Architecture (Nyamtiga et al., 2013)

3. RESEARCH METHODOLOGY

A structured systems Analysis and design methodology (SSADM) was adopted in this study. To identify possible vulnerable points of attack in the deployment of USSD technology in banking, Key Informant Interview (KII) was the major tool used for data collection. The key informants consisted of Information Technology (IT) staff from selected banks in Nigeria.

3.1 Data Collection

Data were collected over 5 months (January to May 2021) from IT staff in selected banks in Nigeria to identify potential points of vulnerability in the deployment of USSD technology in banking, possible security in existence at these vulnerable points, and various banks deployment features. The interview questions were prepared so that the same protocol can be administered to all respondents for consistency. The questions were validated by the researcher's supervisors and five (5) IT staff from different banks. The suggestions made were used to adjust the final questions used for the interviews. In structuring the interview questions, knowledge of critical security issues in USSD deployments in banks obtained from literature played a vital role. Letters of introduction and permission to conduct the interviews were first sent to various Bank Managers (which took more than one month with constant reminders) to be granted access for interviews with their IT staff.

Out of the twenty-two Commercial Banks operating in Nigeria, that were approached, seventeen (17) granted the researcher permission to conduct the interviews. Nine (9) of the interview sessions were recorded with permission from the interviewees. All interviewees were assured confidentiality and privacy of information elicited hence Bank names are denoted as 'Bi'. A maximum of twenty (20) minutes was used for each interview session. To ensure the anonymity of the participants, each recorded conversation was assigned an identifier and securely stored in a folder.

3.2 Data Preparation and Analysis

The audio recordings were played several times and transcribed using the edited transcription method (Walker, 2020) on Microsoft word application for easier identification of themes set out to be searched for and discovered by the researcher. This method enabled the researcher to expunge irrelevant phrases, sentences, and noise (such as; cough, stammer, laughter, irrelevant side comments, and so on) from the interview data. The transcriptions were done one interviewee at a time. Thematic analysis was conducted on the transcribed data to obtain relevant information (Braun and Clarke, 2006).

Thematic Analysis is a method applied to text data such as interviews that closely examines data to identify common themes: topics, ideas, and meanings. The thematic analysis uses two main approaches: the inductive and deductive approaches. The inductive approach allows the data to determine the theme while the deductive approach, which was used in this study involves a systematic analysis of the data with some preconceived themes based on existing knowledge. The first step in the analysis of the data collected was to become familiar with the data collected.

In this study, all the interview data were transcribed individually and checked for consistency concerning the questions asked. The transcribed details were coded manually using a table in an MS word document. Since the size of data is not large, manual qualitative analysis is applicable (Basit, 2003). Microsoft Word, Microsoft Excel, and Nvivo software are possible software to be used in the analysis of qualitative research data (Basit, 2003; Mohammad, 2015). The use of a table also made the comparison and merging of codes generated from each respondent easier.

The table made it easier to derive themes from these codes. They were then merged according to the questions asked with redundancies removed. This was followed by a walkthrough of the interview data and highlighting sections of text (usually phrases and sentences) to produce shorthand labels (code) to describe their content. These labels (codes) were later analyzed to formulate themes that contained patterns reflecting the desired information. Finally, succinct and meaningful names were given to each identified theme (data item).

4. FINDINGS AND DISCUSSIONS

The study carried out is summarized in three different tables ranging from attack points (table 3), Security in place at the vulnerable points/possible attack point (table 4), and finally deployment features (table 5). Table 3 below shows possible attack points.
Attack Points

Table 1 below shows various points in the channel of USSD banking transactions that can be attacked unless there are security measures in place.

Table 1: Vulnerable Points In Ussd Deployment In Banks

Bank List	USSD Bank Transfer Channel				
	Mobile station interface	MNO	USSD gateway	Air Pathway	Bank Database
B 1	√	√	√	√	√
B 2	√	√	√	√	√
B 3	√	√	√	√	√
B 4	√	√	√	√	√
B 5	√	√	√	√	√
B6	√	√	√	√	√
B 7	√	√	√	√	√
B 8	√	√	√	√	√
B 9	√	√	√	√	√
B10	√	√	√	√	√
B11	√	√	√	√	√
B12	√	√	√	√	√
B 13	√	√	√	√	√
B 14	√	√	√	√	√
B 15	√	√	√	√	√
B 16	√	√	√	√	√
B 17	√	√	√	√	√

All the interviewed banks admitted that any point in the channel of transfer can be attacked. The findings from the study show that possible attack points are Mobile interface, Mobile Network Operator (MNO), USSD gateway, air pathways, banks database. The air pathway mentioned here refers to the channel or path through which the data passes after leaving the Mobile Network operators base before getting to the USSD gateway. USSD Gateway is a mobile network element that connects GSM networks (MNO's) to USSD applications. During the interview, it was gathered that not only banks can be a potential attack point but other stakeholders involved in USSD transactions.

Security

Table 2 below shows the existence or lack of security at these possible attack points.

Table 2. Security At The Vulnerable Points

Vulnerable points	Security Measure	
	Secured (encryption/hashing)	None(plain text)
Mobile station interface	X	√
Mobile Network Operator	√	X
USSD Gateway	√	X
Air pathway	X	√
Bank Database	√	X

From the findings made during the study, it can be seen from the table that except for the mobile interface and air pathway, all the other points in the channel of USSD banking transfer are secured. The details at the mobile interface are left in plain text, making it subject to a shoulder surfing attack.

Features of USSD Banking Deployment

During USSD transactions, various features or requirements are incorporated in step by step procedure till the transaction is completed. Table 3 below shows features that are common among various banks during USSD transactions.

Table 3: Deployment Features

Bank List	Deployment features				
	Transaction limit	USSD Transfer code	PIN Length	Session Time	Session Timeout
B 1	N20,000	*894#	5	120/480seconds	20/60 seconds
B 2	N20,000	*901#	4	120/480seconds	20/60 seconds
B 3	N20,000	*326#	4	120/480seconds	20/60 seconds
B 4	N20,000	*329#	4	120/480seconds	20/60 seconds
B 5	N20,000	*770#	4	120/480seconds	20/60 seconds
B 6	N20,000	*737#	4	120/480seconds	20/60 seconds
B 7	N20,000	*745#	4	120/480seconds	20/60 seconds
B 8	N20,000	*773#	4	120/480seconds	20/60 seconds
B 9	N20,000	*7111#	4	120/480seconds	20/60 seconds
B 10	N20,000	*833#	4	120/480seconds	20/60 seconds
B 11	N20,000	*909#	4	120/480seconds	20/60 seconds
B 12	N20,000	*7799#	4	120/480seconds	20/60 seconds
B 13	N20,000	*919#	4	120/480seconds	20/60 seconds
B 14	N20,000	*826#	4	120/480seconds	20/60 seconds
B 15	N20,000	*945#	4	120/480seconds	20/60 seconds
B 16	N20,000	*966#	4	120/480seconds	20/60 seconds
B 17	N20,000	*822#	4	120/480seconds	20/60 seconds

From table 3, it can be seen that all banks followed CBN's policy of having a transaction limit of ₦20, 000. Each bank has a unique code that starts with * and ends with #. The table shows that the time allocated to complete any session is 120/480seconds. Session time is the amount of time required for an initiated transaction to complete. The session times out after the 20/60 seconds of inactivity within the allotted time, depending on the telecommunication company of the customer.

Session timeout which can equally be referred to as idle time is the maximum time that telecommunication companies allow USSD applications to stay idle without any response from the user through the application, after which the session is terminated. So, a user is to be authenticated within 20/60 seconds. The session for MTN, 9Mobile, and GLO networks are 120seconds, while AIRTEL is 480seconds. The session timeout for MTN and GLO is 20 seconds, while that of AIRTEL and 9MOBILE are 60seconds. So it is obvious that the AIRTEL network has the maximum session time as well as a session timeout. This will play a role in the design of the new system to ensure that the proposed authentication and security features fall within the existing session time and session time out, to avoid transaction failure.

5. PROPOSED METHOD

Existing PIN entry method in USSD banking follows the general Direct PIN entry method. Figure 1 shows a PIN entry during USSSD bank transfer.

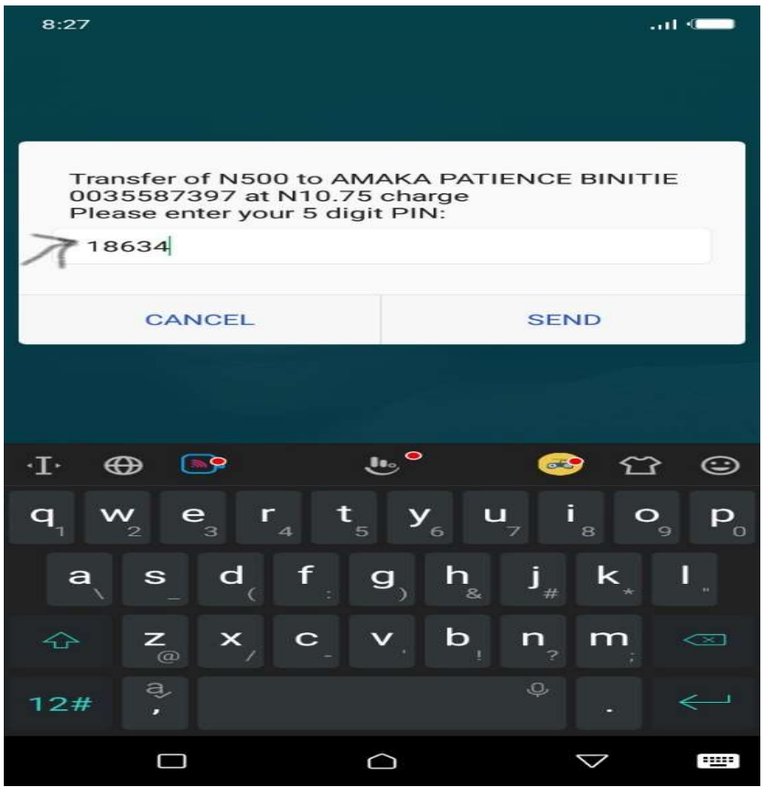

Figure 2: PIN entry method

The arrow in figure 2 points to the users' 5-digit PIN required for authentication. It can be observed that the PIN being entered by a user appears in plain text to the full view of anyone shoulder surfing. Allowing the PIN to appear without concealing has exposed it to possible attack. This form of Pin entry method does not provide any security against shoulder surfing attack. By covertly observing the user while entering PIN, users Pin can be retrieved without waste of time. The existing PIN entry method implemented in USSD financial transaction exposes users a great deal to shoulder surfing attack (Binitie, et al., 2021). In algorithm 1, a modification to the existing PIN entry method in USSD banking is proposed to provide the needed security.

The proposal here includes;

1. Present the 5-digit PIN in two stages/rounds, having the first 3-digit PIN and the last 3-digit PIN. This shows that the central PIN will appear twice.
2. Place the PINs within an array of 10 digits which appears amidst 10 options to be selected from
3. Place the PINs within randomly generated 10-digit number using Randomization Obfuscation Technique in Left to right order (L-R). PIN generation algorithm using Randomization Obfuscation Technique is presented in algorithm 1 while algorithm 2 shows how Mobisafe model derives the 5-digit PIN from users' response.

Algorithm 1: PIN generation algorithm based on Randomization Obfuscation Technique

Output: This algorithm generates 10 digits and injects pin numbers in various order

i. **Generate Numbers:** dnum = rand(1000000000,9999999999); **//Generates 10 digit integer**

ii. **Convert to array:** dnumarr = array_map('intval', str_split($dnum)); **//Convert the number t oarray with 10 entries**

iii. **Test and remove pin digits:** oneopt **= array_walk** (dnumarr,"replacenum") **//Walk through the array and test each against the hashed pin digit by digit, if tally found, replace with other number**

iv. **Get set of digits:**

```
numset = array();
for ($x = 0; $x<=9; $x++) {
//do i to iii
numset[] = oneopt
}
```

//Get the complete list of number groups to be presented(All wrong)

v. **Inject real pin nums:**

```
getreal(x){
dnum = rand(1000000000,9999999999);
oneopt = array_map('intval', str_split(dnum));
if(x == 1){
realopt = array_walk (oneopt,"insertreal1") //insert first 3
else{
realopt = array_walk (oneopt,"insertreal2") //inject last 3 pindigits
}
return realopt;
}
realopt = getreal(1); // getreal(2);
arrkey = rand(0,9);
```

//Pick a random set by key from iv to insert the real pins(3) LTR

```
numset[arrkey] = realopt ;
```

// Reaplace randomly selected key / numset values with real option

Return array: numset;

vi. **Get 10 set of numbers:** numshow = shuffle(numset); **// shuffle them and output as**

a set (10 groups of 10 digits with only one Return array: numshow ; //Return vii to the USSD interface for use

To conceal the PIN from shoulder surfer, the user-defined function, insertreal1(), inserts randomly the first three digits of users chosen PIN in left to right (LTR) order defined by the user function insertreal1() so as to conceal it from an attacker. The same process is followed in generating the last 3 digits of the user's chosen number, but using the user-defined function insertreal2 ().

Algorithm 2: Systematic PIN authentication Procedure

a. **Input:**This algorithm searches for ussd pin numbers within randomized pin obfuscation

i. **Convert response to array:** urnumarr = array_map('intval', str_split($urnum));

ii. **Search for pin numbers:** numorder = array(); numorder []= array_search(pinno,urnumarr);

iii. **Compare pin order (LTR):** result=array_diff_assoc(numorder,pinorder); If(is_empty(result)){ return true; //OK } else{ return false //ERROR MESSAGE }

The submitted PIN will be extracted following the algorithm 2.

6. CONCLUSION AND FUTURE WORK

In the course of this research, an interview of relevant bank staff to identify the possible vulnerable points in USSD banking, to provide a solution was conducted. Consequently, this work identified the mobile interface as a vulnerable point without any form of security, making the mobile interface vulnerable to shoulder surfing attacks. Further a modification to the existing PIN entry method is proposed, so as to provide a resilient PIN entry method. Future work will focus on the system design of the proposed method against shoulder surfing attacks at the mobile interface.

REFERENCES

1. Basit, I. (2003). "Manual or electronic? The role of coding in qualitative data analysis", Educational Research, 45(2), pp. 143-154.
2. Bharat, B. (2018). "Unstructured Supplementary service data", Available at: www.cymn.bsnl.co.in/cymn3/generatepdf.aspx
3. Binitie, A. P., Egbokhare, F., Egwali, A. O., Innocent, O.S. (2021). Implementing existing authentication models in ussd channel. Proceedings of the International Conference on Electrical, Computer and Energy Technologies \(ICECET) 9-10 Dec, 2021, Cape Town-South Africa.
4. Braun, V. and Clarke, V. (2006). "Using thematic analysis in Psychology", Qualitative Research in Psychology, 3(2), pp77-101.
5. Briceno, M., Goldberg, I and Wagner, U. (1999). "A pedagogical implementation of A5/1", Available at http://www.scard.org/gsm/a51.html
6. Chandran, R. (2014). "Pros and cons of mobile banking" International Journal of Scientific and Research Publications, (101), 1-5. Available at: www.ijsrp.org
7. Globitel, (2018). " USSD gateway", Available at: www.globitel.com/ussd-gateway/
8. Gupta, P. (2010). End to end USSD system", Tata Teleservices LTD, India.
9. Handson, O.Z.B, (2016). "Mobile –based multifactor authentication scheme for mobile banking", master Thesis, University of Nairobi, Nairobi Kenya, Retrieved from, uonbi.ac.ke.
10. Nyamtiga, B.W, Sam, A. amd Laizer, L.S (2013). " Security perspective for USSD versus SMS in conducting mobile transaction: a case study of Tanzania", IniernationalJournal of Technology Enhancements and Emerging Resources, 1(3), 38-43.
11. Mohammad, M.M., Sulaiman, N.L, Sern, L.C. and Salleh, K.M. (2015). " Measuring the validty and reliability of research instrument, Procedia-Social and Behavioural Science, Elsevier, 201, PP.164-171.
12. Sanganagouda, J. (2011). "USSD- a potential communication technology that can ouster SMS dependency", Internation journal of Research and Reviews in Computer Science, 2(2), 295.
13. Walker, S. (21st December, 2020). "3 types of transcription: edited, verbatim and intelligent", New Media Services, Retrieved from www.newmediaservices.com.au/types-of-transaction on February 15th, 2021.