ISSN No:-2456-2165

Security against Shoulder Surfing Attack Adaptable to Feature Phones using USSD Technology

Binitie, Amaka Patience, Anujeonye, Nneamaka Christiana, Ezzeh, Peace Oguguo.
Department of Computer Science
Federal College of Education (Technical) Asaba, Nigeria

Abstract:- Security of users' data is of high importance, especially when the data has to do with personal details like health status, financial details and others. For financial details, it is important that details of customers like authentication data is secured by the financial institutions. This will boost the confidence of customers. Financial institutions uses various electronic means to serve their customers which requires additional security. Unstructured supplementary service data (USSD) is one of the technologies that banks use to provide electronic banking services to their customers at all locations. This technology is so common because it built in all GSM mobile phones. Despite its strong security features, user's data at mobile interface appears in plain text. This exposes user's data to shoulder surfing attack. The research therefore reviewed existing methods that can provide security against shoulder surfing attack and it was discovered that these methods cannot be implemented in USSD channel. This is because USSD channel conveys data in plaintext only, but some of the data contained by these method are images and colors. Also they are third party applications and cannot be accommodate by feature phones. This research, therefore, designed a new authentication model called "Transcare" to resist shoulder surfing attack during USSD transaction. In this model, challenge response approach is adopted to provide a secure authentication data entry method in the presence of human shoulder surfer, using Bag of Soft Biometrics (BoSB) details and one time password (OTP) during user authentication.

I. INTRODUCTION

The central bank of Nigeria launched a digital currency that serves as medium of exchange and store of value known as e-naira. The e-naira was launched by President Muhammad Buhari on 25th October, 2021 (CBN, 2021). The apex bank stated that the essence of introducing the e-naira was to promote and facilitate financial inclusion (Salami, nov10th, 2021). Also in order to ensure that the Nigerian citizens key into electronic transaction, cash withdrawal for individuals and organizations per week is reduced to 20,000 naira and 500,000 naira respectively. This implies that mobile phones will play a large role in financial transactions in Nigeria. Mobile phone is an equipment used in communication between users or between a user and the mobile network. It is a device possessed by both the rich and poor, learned and illiterate, though with difference in the level or quality. There are smartphones and feature phones. The smartphones are the mobile phones that have ability to accept third party applications, and they have complex operating systems that accommodates many fascinating features. Feature phones are low level mobile phones that do not have the capability to accept third party applications and equally do not have complex operating system (Turner, 2022). This limits the capability of feature phones. The world mobile industry has over 7. 26 billion subscribers currently(Turner, 2022). This means that more than two-third of the global population is now connected to mobile services of which Nigeria is part of.Research carried out by Newzoo, (2021) indicated that 74.61% population of people from top 10 developing countries which includes, Nigeria, Pakistan Bangladesh and others, do not own smartphones. PEW research center (2019)put the percentage of feature phone owners in Nigeria at 44%. The chief executive officer of Jumia Nigeria, Anammahasserted that "the availability of lower price point phones has paved way for more Nigerians to own mobile phones" (Adeputun, 2018). Taking into account the success of mobile content services such as ringtones, games, telephone calls, short messaging and other applications, the functional capabilities of mobile telephony have been rapidly expanding and have extended their usage well beyond the classical communication applications (Zang, 2012). It is apparent that consumers are more than willing to utilize mobile phones for several purposes. As a result, a large number of mobile applications are being built for multiple platforms (Android, J2ME, Symbian, etc.) and domains (mobile payments, mobile VAS, mobile commerce, etc.). According to Zang, (2012), although the IT infrastructure is usually undeveloped in rural areas, remarkably in most of the developing countries mobile telecommunication sector achieved rapid expansion in recent years, which is partly as a result of the significant decrease of the cost of mobile phones and mobile services (Zang, 2012).The fast increasing number of subscribers opened up new business ventures and gives financial institutions some additional channels to deliver services (Suhas, 2017). Several factors have led to the attraction for mobile services.

According to (Zang, 2012) mobile devices, and in particular, mobile phones have become the attraction for consumers, service providers and merchants in the business world, everyday life, and in fields of communication. Mobile phones are also providing an unprecedented opportunity for expansion of financial transactions of all types like: enquiry (balance enquiry/ mini statement/ currencies rates), money transfer, bill payment, cheque book request and many other banking services in developing countries where the number of phone users can exceed the number of those having bank accounts (Faisal,2017). Technologies like Wireless Application Protocol (WAP) which is best described as the mobile internet, short message service (SMS), Interactive Voice Response (IVR) allows

ISSN No:-2456-2165

customer to access mobile financial services, mobile application installed on mobile devices, and Unstructured supplementary service data (USSD), which is the focus of this research (Suhas, 2017).With the aid of the mobile phone, all Nigerians are expected to make use of existing technologies for financial transactions.

II. STATEMENT OF PROBLEM

The new CBN policy on daily cash withdrawal limit has forced all Nigerians to key into electronic financial transaction. Though electronic means of financial transaction are fast, easy and cheap, there is high need for security of users' data. USSD technology which is the commonest technology that can be implemented on all types of mobile devices(Smartphones and feature phones) is susceptible to shoulder surfing attack (Binitie, et al, 2022). Users' data at mobile interface during authentication using USSD technology is in plain text and can be captured by a shoulder surfer. Smartphones can accept a third party application against shoulder surfing but feature phones do not have such capability. Since most of the users of feature phones are making use of USSD technology for financial transaction due to its adaptability, there is need to provide solution against shoulder surfing attack that can be adaptable to USSD channel and all types of GSM phones (Nyamtiga, et al, 2003).

III. THEORETICAL BACKGROUND

Unstructured Supplementary Service Data (USSD) is a capability built into the Global system for mobile communication (GSM) standard, that allows high-speed, bidirectional communications between mobile handsets and applications (Globitel, 2018). It works on all GSM mobile devices. It allows customers to request information regarding an account and also carry out other transactions. USSD codes or simply "shortcodes" 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. USSD applications are installed on the developer's network not on the user's device, thereby making it possible for feature phones to benefit from the application. Feature phones are commonly 2G phones with no Internet feature and lack features to accept a third-party application (Jalakasi, 2022). This makes it possible for USSD applications to reach a wider population than mobile applications. That is why banking, financial institutions, and other industries, businesses, and organizations have keyed into it in Nigeria.

USSD technology is text-based hence it accepts only PIN for authentication. Users' PIN appears in plaintext on mobile interfaces as shown in figure 1, which is the major challenge facing USSD banking (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).

Securing users data at mobile interface on USSD channel has not attracted much research interest. Many method proposed and implemented by many authors did not consider feature phones capability (Kwon et al., 2014; Choi et al., 2015; Chakraborty et al., 2019, Binitie, et al. 2020). The method of securing users data at mobile interface which will be implemented on USSD channel should consider feature phones.

IV. RELATED WORK

This section analyzed some selected existing works that proposed and implemented methods for securing data at mobile user interface. It will show the methodology and its weaknesses. The weakness of each method is considered in terms of possibility of implementing it on USSD channel and feature phones.

ISSN No:-2456-2165

S/N	Authors	Technique	Methodology	Findings /Weaknesses
1	Gokhale and Waghmare (2016)	Session Password	**Click point**. User clicks at 3 different points on an image.	It is an application that is required to be installed in the mobile device so it cannot be implemented on USSD channel since it uses images and also cannot be installed on low level phones due to low storage space in low level phones.
2	Chakraboty et al. (2019)	Black & White method	MIOC BW & introduced noise to the odd of probable PIN digits	Introduction of noise will reduce round redundancy. This method is a mobile application that uses colored images which cannot be implemented on USSD technology and it requires memory storage capacity which cannot work on Low level mobile phones.
3	Kwon et al. (2014)	Black and white method	Improved IOC BW method	Though it helps to improve the security challenges of black and white method but maintains the problem of round redundancy. This method uses graphical color based method which cannot be implemented on USSD technology.
4	Shubhangi et al. (2018)	Text(PIN code) based	Geometric shapes cover the users chosen PIN, though the user knows the location of the PINs.	It is based on shapes and images which cannot be implemented on USSD channel
5	Irfan et al. (2018)	text-based images	The right most grids move to confuse a shoulder surfer on the image selected	It makes use of images which is not supported by USSD technology. It is a mobile application that can take memory space, so it cannot be installed on low level phones due to low storage space in low level phones.
6	Heckathorn et al. (2001)	Soft biometric details	Details are supplied by user	It is not secure enough alone for authentication. It is a mobile application that can take memory space, so it cannot be installed on low level phones due to low storage space in low level phones.
7	Choi et al. (2015)	Face and hand gesture biometrics	The face and hand gesture are represented in feature matrices, to be used for authentication.	Image capturing password can be duplicated. It is mobile application that is based on graphical images which is not supported by USSD technology. Also can take memory space, so it cannot be installed on low level phones due to low storage space in low level phones.
8	Mtaho, 2015	PIN and Fingerprint	User is granted access when the fingerprint matches.	It is mobile application that works using image in its authentication. Image based authentication is not supported by USSD technology.
9	Lee, 2014	Black and white method	Improved IOC B/W method	Though it helps to improve the security challenges of black and white method but maintains the problem of round redundancy. This method uses graphical color based method which cannot be implemented on USSD technology.
10	Ho, et al. (2014)	Picture based Password	Password Concealing using pictures.	Picture based authentication method cannot be implemented on USSD technology.
11	Binitie, et al. 2020	Soft biometric based	Improved on direct PIN entry method	It is a third party application which requires space for storage. Feature phones do not have enough memory space to accommodate third party applications.

Table 1: RELATED WORK

ISSN No:-2456-2165

All the methods presented above provided some level of security to users' data at mobile interface during transaction but contains various features that cannot be implemented in USSD channel and feature phones.

Therefore, there is need for a method that will consider the capabilities of feature phones and USSD channel.

V. DESIGN METHODOLOGY

The existing architecture of deployment of USSD in the banking system as shown in figure 1 is adapted for the model design. USSD technology in bankinguses the same general USSD architecture in its deployment (Nyamtiga et al., 2013).

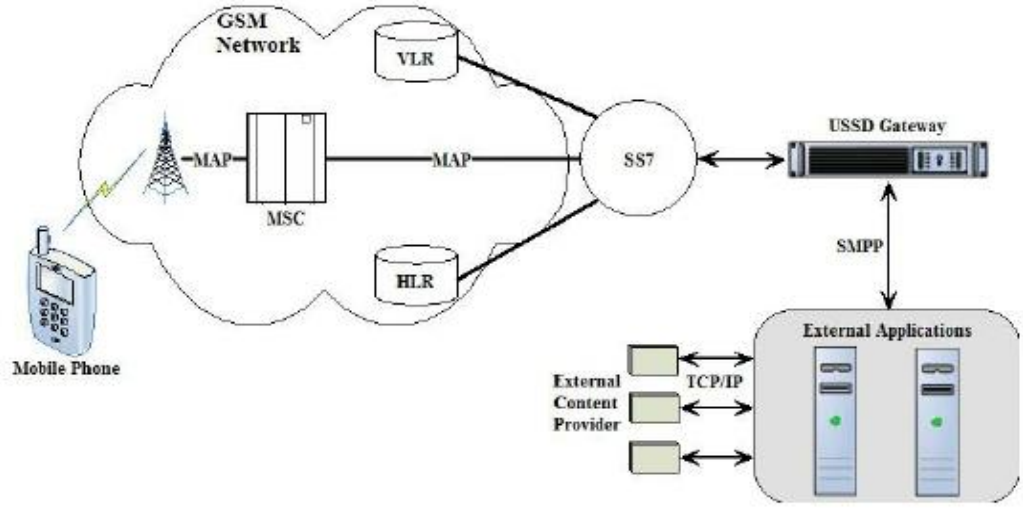

Fig. 1: General USSD architecture (Nyamtiga et al. 2013)

To provide confidentiality (security against shoulder surfing attack) to users' details at mobile interface, instead of the customer to key in 4 or 5 digit numbers as the case may be, the user will receive one time password. If the OTP is keyed in correctly, the user will finally provide answer to a soft biometric question before transaction becomes successful. The response to the query will be matched to the user's soft biometric details in the database. The user only has three attempts for each stage after which s/he is logged out. Using a unique encrypting and decrypting algorithm, the model will randomly produce a different identity credential for each transaction, thereby defending against shoulder surfing attacks.The response will be verified against securely stored BoSB details of the client. The Use of OTP and BOSB in place of PIN will provide solution to shoulder surfing attack.In this methodology, client registration plays an important role. The user provides answers to queries relating to soft biometrics with which the client is familiar with during registration. The data will be collected from the user through Computer Assisted Personal Interviewing (CAPI or Electronic) methodology (Handfield, 2017). Bag of Soft Biometrics Data collected from the user will be stored in a database. In the database, the client's phone number will be linked to the account number for easy identification. Figure 2 shows the components of the designed model.

To provide confidentiality to the user's identity, two methods are proposed;

- Bag of Soft Biometric (BoSB) authentication/verification method
- One-time Password (OTP)
  - BOSB: These are the details of an individual's physical appearance that are collected from the user during registration. Also, the use of BOSB questions makes the system more secure, as only users know the answers to these Soft biometric questions. The details can be updated at any time. To solve the problem of user Identity theft in USSD mobile transactions, our proposed system will make use of Soft Biometric details. In this case, users will provide answers to the soft biometric questions which will be stored in the database and referred to as Bag of Soft Biometrics (BoSB) for user identification. This is because USSD technology is text-based and will not support the use of a camera or hard biometric capturing features (Nyamtiga, et al., 2013).
  - One Time Password (OTP): OTP will be auto-generated at the end of every transaction starting from the time of registration and delivered to the user's registered mobile phone as Short Messaging Service (SMS). The OTP remains valid until usage. It will be required before a user can have access to any of the services.

ISSN No:-2456-2165

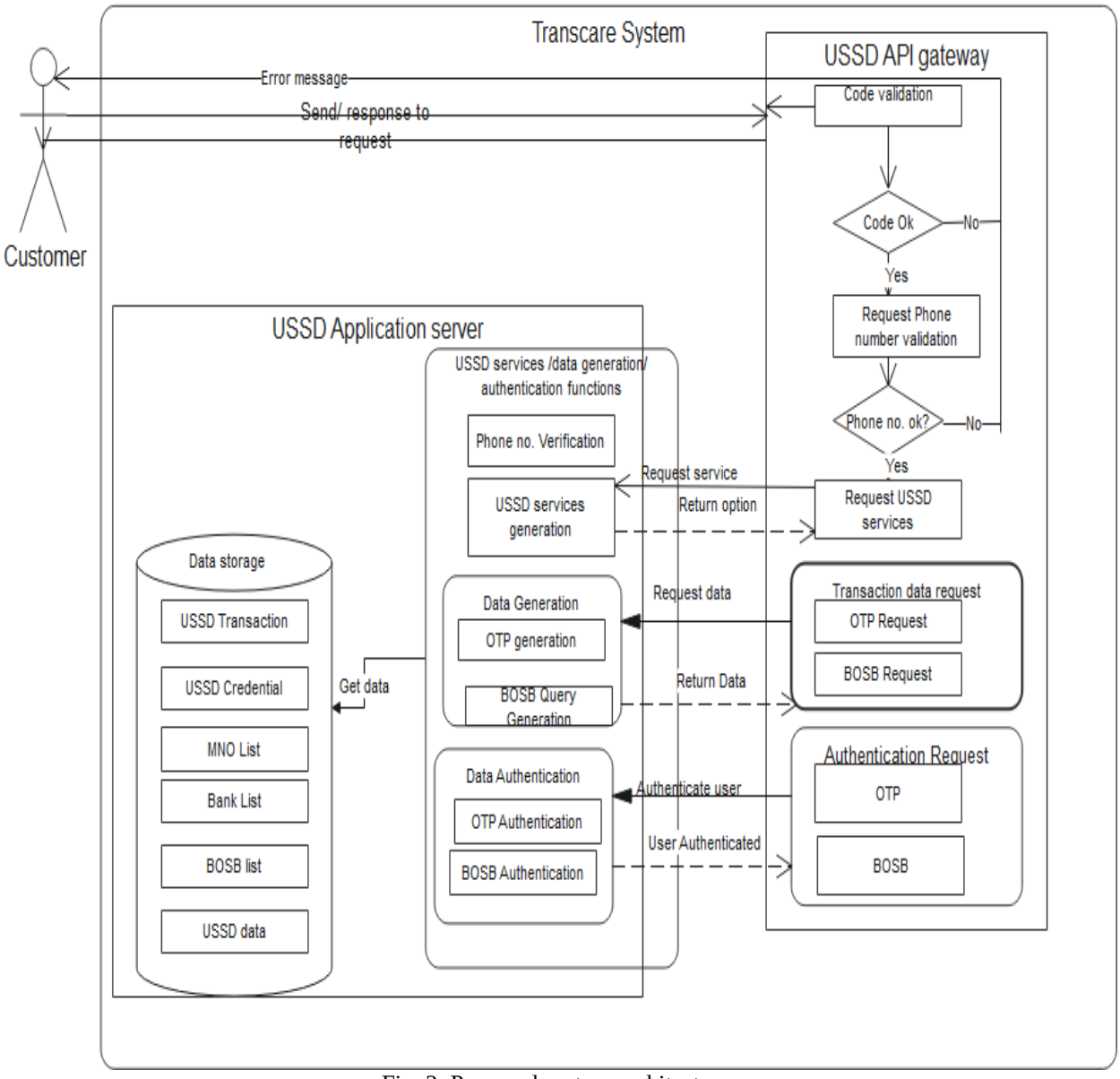

Fig. 2: Proposed system architecture

The designed system is based on a Representational State Transfer (REST) architecture. REST is a software architectural style that defines standards or rules that should be followed while creating web services or applications (Fielding, 2000). USSD application is a web application.

A. REGISTRATION

Users' details will be collected through challenge response method common in USSD technology. Each time the USSD code is dialed from a new mobile number, there will be options for the new user to "create account". Bag of Soft Biometrics Data (BOSB) shown in figure 3 (BOSB detail), collected from the user stored in the database.To avoid usability issue, the BOSB details will continue be updated at every transaction until all the existing queries are exhausted and new one will continue to be generated as decided. The data provided are subject to updating.

ISSN No:-2456-2165

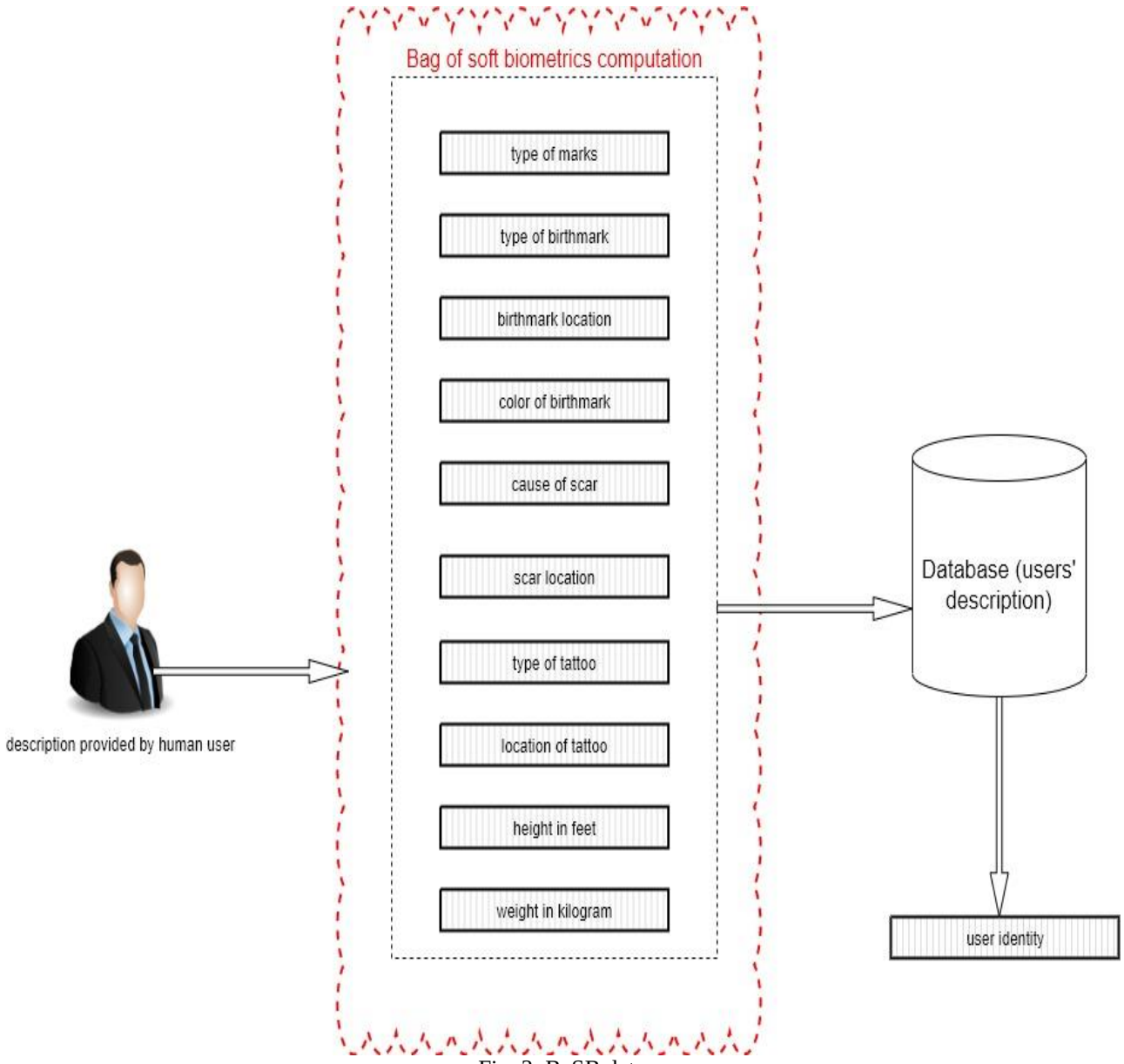

Fig. 3: BoSB data

B. Authentication Algorithm

One-Time Password (OTP), and Bag of Soft Biometric Data (BoSB) is designed to provide security to the system. For the system/transaction to be authorized, these security features must be successfully verified. OTP will be the first security feature used to allow a user access to the USSD service. The BoSB will serve as "what the user is" for final user identification. All these features make the system more secure than the existing authentication model deployed in USSD banking transactions today.

C. Data Generation Algorithms 1

As seen in algorithm 1i, the system generates a one-time password which will be delivered to the users registered phone number. The system will finally generate a BOSB question for the user to provide response to, based on the details created by the user during registration, as seen in algorithm 1ii.

D. OTP Generation Pseudocode:

- **Output:** This algorithm generates 5 cryptographic random integers that are suitable for use where unbiased results are critical
- **Generate Numbers:** dotp =rand_int(10000,99999);
- **Return generated otp:** dotp;
- **Push otp to database:** update('ussdtransact', 'nextotp',dotp,duser);

E. BoSB Generation/Retrieval Pseudocode:

- **Output:** This algorithm outputs BOSB questions for a user or applicant from the bosblist table
- **Select from table:**
- bosblist = dataset(bosbquest, optlist);
- **Get random bosb questions (2) from arraylist(bosblist) above:**
- thisbosb =array_rand(bosblist,2);
- **Push** thisbosb**[0] to USSD interface:** thisquest= toussd(thisbosb**[0]**);

- **Part B(i):** This algorithm collects and saves user response to BoSB questions and saves into database table **ussdcred** to be used for future validation
  - Input - Pick an option for the question presented: bosbresp = get(useropt);
  - Push bosbresp to database:
  - if(new){insert('ussdcred', 'userbosb', 'lastbosb', 'new',duser);}
  - else{update('ussdcred', 'userbosb', 'lastbosb', duser);

As soon as the user submits the OTP, the system uses algorithm 2i to check the submitted OTP against the one generated by the system. The response provided by the user is compared to the details created by the user, based on algorithm 2ii

User Response Validation Algorithm 2

- OTP Validation Pseudocode
  - **Input:**This algorithm takes input as ***otp (int***), against the submitted phone number. ***H(otp)*** is compared with last generated otp for user (account/phone) ***H(lastotp)*** extracted from the database.
  - Validate H(otp): if ***H(otp)*** == ***H(lastotp) {OUTPUT: return true ;}***
  - **Else Error** (log: count attempt)return to**a;**
- BoSB Validation Pseudocode
  - **Input:** This algorithm takes input as ***opt(int***), and compares against the valid answer to the bosb output to user. Each option serves as array key to value of string (BOSB Response/Answers). The ***(opt)*** is compared with user BoSB valid answer extracted from **ussdcred. userbosb** extracted from the database.
  - **Get userbosb valid answer key:**
  - userbosb = getdata('userbosb, 'ussdcred', 'duser', duser);
  - validkey= userbosb[key];
  - Validate (opt): if ***(opt)*** == validkey ***{OUTPUT: return true ;}***
  - **Else Error** (log: count attempt)return to **1a;**

Figure4 shows how the system presents the six digits OTP request and response submitted by the user. The response is validated once the user clicks "send".

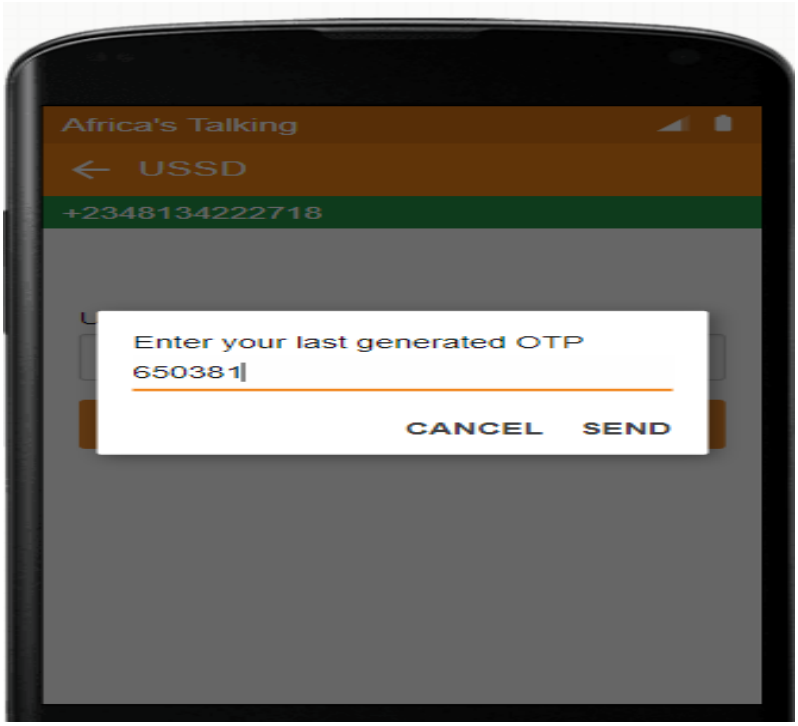

Fig. 4: OTP request

Figure 5 shows how the system presents a BOSB questions with options for user to select from. Once the user enters the identifier that represents the correct answer and clicks "send", the system validates the response.

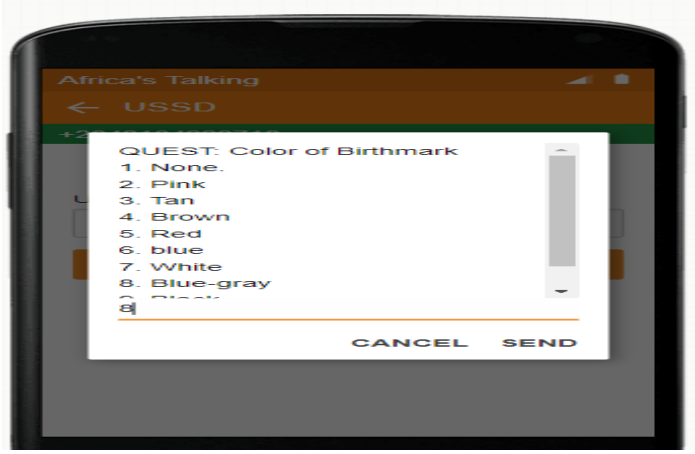

Fig. 5: BoSB generated question

VI. DISCUSSION AND FINDINGS

It has been observed through the course of the research that users details appear in plain text while using USSD technology for financial transaction. This makes it vulnerable to a shoulder surfer, who can observe the sensitive detail and use it against the user. The users' details appears in plain text on a mobile interface because the USSD channel accepts data in plain text only. This requires any improvement to the existing method against shoulder surfing attack to be in plain text. These findings led to the design of an authentication model named "Transcare"

VII. CONCLUSION

The designed model called "Transcare" replaces users PIN entered during USSD transaction with OTP and BOSB data. Since the Password is used once an attacker who captured it cannot reuse it once used by the user. Also the BoSB uses different credentials during each transaction, thereby making it difficult for an attacker to capture and reuse. The implementation of the "Transcare" system will provide security against shoulder surfing attack during USSD transaction.

REFERENCES

[1.] Adeputun, A. (2018, March 16). Nigeria's mobile phone penetration hits 84 percent. *The Guardian Newspaper*. Available at: https://www.guardian.ng/business-services//nigerias-mobile-phone-penetration-hits-84-per-cent/amp/

[2.] Binitie A.P, Egbokhare, F. and Egwali, A.O, Ezekwe, C.G and Madaki, S.D (2020). Secured android based USSD financial transaction system: an improved virtual banking system for pandemic outbreak related financial transaction challenges, Proceedings of the Third International Conference of UNIZIK Business School (UBS), Nnamdi Azikiwe University, Awka, pp. 70-79.

[3.] Binitie, A. P., Egbokhare, F., Egwali, A. O. and Innocent, O.S. (2021). Implementing existing authentication models in ussd channel. *Proceedings of the International Conference on Electrical, Computer and Energy Technologies (ICECET) Dec 9th-10th, 2021, Cape Town- South Africa.*

[4.] Briceno, M., Goldberg, I., and Wagner, D. (1999). A pedagogical implementation of A5/1, Available at: http://www.scard.org/gsm/a51.html

[5.] Central Bank of Nigeria (2017).Exposure draft of regulatory framework for Unstructured supplementary service data (USSD) for the Nigerian financial system. Available at: https://www.cbn.gov.ng/out/2017/ccd/ussd%20framework.pdf

[6.] Chakraborty, N., Li, J., Mondal, S., Chen, F, and Pan, Y. (2019). On overcoming the Identified limitations of a usable pin entry method. *Special Section on Innovation and Application of Internet of things and Emerging Technologies in Smart Sensing.* Vol 7, Pp. 124366-124378.

[7.] Choi,M.,Lee,J.,Kim,S.,Jeong,Y.S.,andPark,J.H.(2016).Location-based authentication scheme using BLE for a high-performance digital content management system. Neuro computing,209,25–38.

[8.] Fielding, R.T. (2000). Architectural styles and the design of network-based software architectures. Ph.D. Dissertation in Information and Computer Science at University of California, Irvine.

[9.] Faisal, G. A. (2017). A new secure application based mobile banking model for Nigeria. Available at: https://www.researchgate.net/publication/320291138_A_NEW_SECURED_APPLICATION_BASED_MOBILE_BANKING_MODEL_FOR_NIGERIA

[10.] Globitel, (2018). USSD gateway, Available at: www.globitel.com/ussd-gateway/

[11.] Gokhale,M.A.S.,andWaghmare,V.S.(2016).The shoulder surfing esistant graphical passwordauthentication technique. *Proceedings of 7th International conference on Communication, Computing and Visualization*,79,490–498.

[12.] Gupta, P.(2010). *End-to-End USSD System*. Tata Teleservices Ltd, India

[13.] Handfield, R. (2017). Data collection: electronic or manual? NC State University. Retrieved from scm.ncsu.edu/scm-ar… on 12th June 2018.

[14.] Heckathorn, D. D., Broadhead, R.S. and Segeyev, B. (2001). A methodology for reducing respondent

duplication and impersonation in samples of hidden populations. *Journal of Drug Issues,31*(2), 543-564.

[15.] Ho, P.F., Kam, Y.H.S., Wee, M.C., and Por, L.Y. (2014). Preventing shoulder surfing attack with the concept of concealing the password objects information. *The Scientific World Journal.* Retrieved from, https://www.hindawi.com/journals/tswj/2014/838623/&ved on 15th October, 2019.

[16.] Irfan, K., Anas, A., Malik, S. and Amir, S. (2018). Text based graphical password system to obscure shoulder surfing, *Proceedings o the 15th International Bhruban Conference on Applied Aciences& Technology (IBCAST),* 422-426.

[17.] Jalakasi, Wiza. (July 20th, 2022). How a 20-year-old mobile technology is revolutionizing africa. Retrieved from, https://www.google.com/amp/s/qz.com/Africa/1296120/

[18.] Kwon, T., Shin, S. and Na, S. (2014). Covert attentional shoulder surfing: human adversariesare more powerful than expected," *IEEE Transactions on System, Man and Cybernetics: System*, 44(6), pp. 716-727.

[19.] Lee, M. (2014). Security notions and advanced method for human shoulder-surfing resistant pin-entry. *IEEE Transactions on Information Forensics and Security*, Vol. 9, No. 4, April 2014 695

[20.] Mtaho, A. B. (2015). Improving Mobile Money Security with Two-Factor Authentication. *International Journal of Computer Applications, 109(*07*),* 0975 – 8887.

[21.] Newzoo (2021). Top countries by smartphone users. Retrieved from www.newzoo.com/insight/rankings…

[22.] Nyamtiga, B. W., Sam, A. and Laizer, L.S. (2013). Security perspectives for USSD versus SMS in conducting mobile transaction: a case study of Tanzania. *International Journal of Technology Enhancements and Emerging Engineering Researches*, 1(3), 38-43.

[23.] Pew Research Center (February, 5th, 2019). Smartphone ownership is growing rapidly around the world, but not always equally. Retrieved from www.pewresearch.org/global/2019/02/05...

[24.] Salami, I. (November 10th, 2021). Nigerians digital currency: what the e-naira is for and why it is not perfect. *The conversion.* Retrieved from www.theconversion.com.

[25.] Sanganagouda, J. (2011). USSD- a potential communication technology that can ouster SMS dependency. *International Journal of Research and Reviews in Computer Science*, 2(2), 295.

[26.] Shubhangi, D., Shardul, H., Nikhil, S. and Tatwadaershi, P.N.(2018). A hybrid approach to resist shoulder surfing attack. *Proceedings of ARSSS International Conference, New Delhi, India,* 83-85.

[27.] Subhas, D. (2017). Mitigating security risks in ussd-based mobile payment applications. *Aujas executive summary*. Retrieved on 9th, October 2018, from www.aujas.com

[28.] Turner, A. (2021).how many phones are in the world. Retrieved from www.bankmycell.com Zhang, F. (2012).*Secure mobile service-oriented architecture*. Doctoral Dissertation, KTH Royal Institute of Technology, Stockholm, Sweden. Retrieved from, https://www.diva-portal.org/smash/get/diva2:527836/FULLTEXT01.pdf, on January 23rd, 2018.