African Journal of Environment and Natural Science Research
ISSN: 2689-9434
Volume 7, Issue 1, 2024 (pp. 13-27)
www.abjournals.org

ADAPTING USER INTERFACE DESIGN TO MITIGATE SHOULDER SURFING ATTACKS IN USSD CHANNEL

Binitie, Amaka Patience[1] and Babatunde, J. Odetayo[2]

[1]Department of Computer Science

Federal College of Education Technical Asaba, Nigeria.

Email: Philpat4sure@gmail.com Tel.: +2347035901508

[2]Department of Computer Science,

Faculty of Physical Sciences,

University of Benin, PMB 1154, Benin City, Nigeria.

Email: babatunde.odetayo@uniben.edu

Cite this article:

Binitie A. P., Babatunde J. O. (2024), Adapting User Interface Design to Mitigate Shoulder Surfing Attacks in USSD Channel. African Journal of Environment and Natural Science Research 7(1), 13-27. DOI: 10.52589/AJENSR-DPCGWN0X

Manuscript History

Received: 2 Nov 2023

Accepted: 15 Dec 2023

Published: 24 Jan 2024

ABSTRACT: *The most widely accepted authentication method involves the use of a personal identification number (PIN). This method is applicable across many technologies, of which one of them is Unstructured Supplementary Service Data (USSD). USSD is a capability built into the Global System for Mobile Communication (GSM). In some developing countries like Nigeria, USSD is used in carrying out financial transactions. It has been observed that while carrying out banking transactions using this technology, users' personal identification number (PIN) entered for authentication appears in plain text on the mobile interface, thereby subjecting it to shoulder surfing attacks. Findings revealed that users' PIN appears in plain text because USSD technology is designed to convey only textual data. That is why many existing authentication methods against Human shoulder surfing attacks which contain features like images, colors, or graphical password, that can provide security to users' PIN on mobile interface are not implemented on the USSD channel. This is one of the reasons why many existing authentication methods, which are designed with features such as images, colors or graphical passwords to prevent shoulder surfing attack, are not implemented on the USSD channel. This research is, therefore, on the design of a new authentication method that can provide security to users' PIN at the mobile interface of the USSD channel and secure the users' transaction against shoulder surfing attacks. In this method, the challenge response approach is adopted to provide a secure PIN entry method in the presence of a human shoulder surfer, using the randomization obfuscation method that randomly places the user's chosen PIN within randomly generated 10-digit numbers, in Left to Right order. For further security, the designed model includes features like Bag of Soft Biometrics (BoSB) details and one-time password (OTP).*

KEYWORDS: Mobile Interface, Data Security, Authentication, USSD, mobile phone, Randomization Obfuscation, A bag of soft Biometrics.

Article DOI: 10.52589/AJENSR-DPCGWN0X
DOI URL: https://doi.org/10.52589/AJENSR-DPCGWN0X

African Journal of Environment and Natural Science Research
ISSN: 2689-9434
Volume 7, Issue 1, 2024 (pp. 13-27)

www.abjournals.org

INTRODUCTION

Security of users' data is important to computer, mobile, and electronic gadget users especially in today's technology-driven society where 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 (Zhang, 2012). Unstructured Supplementary Service Data (USSD) is a technology that conveys sensitive details of users, of which security is required. USSD is a technology that conveys and accepts data in plain text. User authentication is an important step in securing users' identities. Authentication is the process of ascertaining a legitimate user's identity. The data required to ascertain legitimate users' identities need to be secured. Various means of securing users' data include data obfuscation. Data obfuscation is the process of protecting sensitive data from an unauthorized user using fictitious data or characters. There are various obfuscation methods such as masking, tokenization, encryption, randomization (shuffling), substitution, nulling out, blurring, and others (Satoricyber.com, 2022). Attacks can occur in the network or at the device interface. The type of attack that can occur at the device interface includes a shoulder surfing attack. A shoulder surfing attack is an attack that involves an attacker physically looking over the shoulder of a legitimate user's device or using a video recorder to obtain the personal details of the user which appears at the device interface (Por et al., 2019). Sensitive details, such as PIN at the mobile interface, are susceptible to shoulder surfing attacks.

Statement of Problem

Security of users' data is important especially when it involves financial details. Nigerian commercial banks have adopted USSD technology in carrying out financial transactions. While using this technology, users' data at the mobile interface appears in plain text which makes it susceptible to shoulder surfing attacks. As a result of this, the Central Bank of Nigeria in September 2017 released a regulatory framework, which mandates all banks and financial institutions that make use of the USSD channel in communicating with their customers to provide maximum security to customers' sensitive data (CBN, 2017). The unique features of this technology that made banks key into it is its ability to work on all types of phones including feature phones, without requiring internet access. This makes it possible for their customers in remote villages and those with feature phones to carry out mobile transactions. Therefore, it is required that in complying with CBN's policy, a stronger authentication method be adopted. Most existing strong authentication methods against shoulder surfing attack require mobile devices to have features like a camera, primary biometrics capturing, and large memory space to accommodate the data for authentication (Chakraborty et al., 2019; Choi et al., 2015). Adopting these authentication models to secure users' data will cut off feature phones since they cannot accommodate the required features of these models. Also, these models cannot be implemented on the USSD channel since USSD technology accepts data in plain text only.

Therefore, there is a need to develop an authentication method that can be implemented on the USSD channel for securing users' details at mobile interface against shoulder surfing attacks, which can be available to all GSM phones.

Article DOI: 10.52589/AJENSR-DPCGWN0X
DOI URL: https://doi.org/10.52589/AJENSR-DPCGWN0X

African Journal of Environment and Natural Science Research
ISSN: 2689-9434
Volume 7, Issue 1, 2024 (pp. 13-27)

www.abjournals.org

Aims and Objective

This research aims to design a secure authentication model against shoulder surfing attacks that can be implemented on the USSD channel. This will be achieved through the following objectives:

1 Identify PIN entry challenges on USSD.

2 Design a secure model to authenticate users during a transaction.

THEORETICAL BACKGROUND

Authentication is a vital integral feature of any application that requires the user's details. This is necessary for the security of users' identities and details. Authentication is the process of ascertaining a legitimate user's identity. Various authentication models in existence involve textual, graphical, and biometrics features. Some models combine authentication features to make the system more secure. Three major factors determine a legitimate user: what the user knows, what the user has, and what the user is (Almuairfi et al., 2013). There is a need to secure authentication data right from the device interface to the database. Authentication based on the user's knowledge has been the oldest form of authentication and it is still in existence due to its ease of use (Waghmare, 2014). This method traditionally requires a user to key in a 4 to 8 digits Personal Identification Number (PIN) and username. It was first introduced in the 1960s together with Cash Automated Machine (ATM). The security of users' PINs has become an area of research interest as banks and other utility companies in Africa are using Unstructured Supplementary Service Data (USSD) technology standards in penetrating the African market. This is because USSD technology accepts PIN in plain text during user authentication. The security of users' PINs has become an area of research interest in Africa because banks and other utility companies in Africa use Unstructured Supplementary Service Data (USSD) technology standards in penetrating the African market, and the concept of USSD technology accepting PIN in plain text during user authentication exposes the system to shoulder surfing attacks.

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 which 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, and the reason why banking, financial institutions, industries, businesses, and organizations have keyed into it in Nigeria.

Article DOI: 10.52589/AJENSR-DPCGWN0X
DOI URL: https://doi.org/10.52589/AJENSR-DPCGWN0X

African Journal of Environment and Natural Science Research
ISSN: 2689-9434
Volume 7, Issue 1, 2024 (pp. 13-27)
www.abjournals.org

USSD technology is text-based; hence, it accepts only PIN for authentication. Users' PIN appears in plain text 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). The PIN in Figure 1 is a 5-digit PIN (18634) which a user keyed in to be authenticated while carrying out a USSD banking transaction. This is how users' PINs appear on the mobile interface while carrying out USSD banking transactions currently in Nigeria. The PIN can be captured by anyone standing closeby or a shoulder surfer.

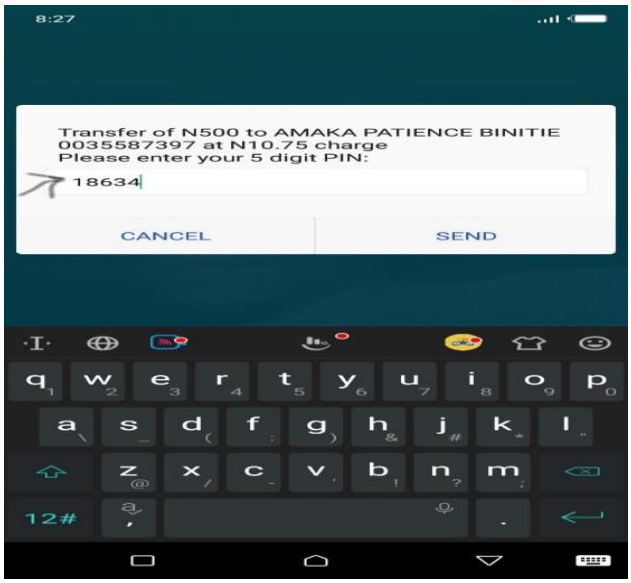

Figure 1: A PIN in plain text

Many researchers have come up with authentication models to counter shoulder surfing attacks using what the user knows, for example, PIN; what the user is, for example, Biometric features (fingerprint, iris recognition); what the user has, for example, hardware token (Kwon et al., 2014; Choi et al., 2015; Chakraborty et al., 2019), while some combine these features (hybrid) to come up with stronger resistant models (Mekala, 2015; Bryan, 2021). Despite the numerous authentication models that have been proposed, to date, Unstructured Supplementary Service Data (USSD) technology deployed in banking services has not received much research attention in terms of providing an authentication model that can secure users' PIN at the mobile interface (Binitie et al., 2021). Sensitive details at the mobile interface are susceptible to shoulder surfing attacks (Nyamtiga et al., 2013). Introducing further features like primary biometrics and hashing algorithm for the security of the PIN on the mobile interface can only be achieved using a third-party application outside the USSD channel (Handson, 2016). This cannot be implemented on the USSD channel and will cut off feature phones.

Article DOI: 10.52589/AJENSR-DPCGWN0X
DOI URL: https://doi.org/10.52589/AJENSR-DPCGWN0X

African Journal of Environment and Natural Science Research
ISSN: 2689-9434
Volume 7, Issue 1, 2024 (pp. 13-27)

www.abjournals.org

RELATED WORKS

Some researchers have designed and developed authentication models to secure users' sensitive details at mobile interfaces against shoulder surfing attacks. Some of these models are discussed below.

Mtaho (2015) designed a model to tackle shoulder-surfing at the mobile application point. The proposed model has two main authentication phases: authentication with PIN and authentication by fingerprint. The user enrolls the phone number, PIN, and fingerprint which are saved at the financial institution's server for future authentication. During the authentication phase, first, the user will be authenticated by the traditional model (PIN). If the PIN authentication is successful, the user will proceed to the second authentication by fingerprint. The designed model assumed that the smartphones should have embedded fingerprint recognition technology (for example, iPhone 5s, Samsung Galaxy S5, Motorola Atrix 4G, HTC One Max, and Huawei Ascend Mate 7). During the USSD transaction, the fingerprint is then scanned by the smartphone's fingerprint recognition software and matched with the fingerprint template saved during the enrollment phase. If the fingerprint matches, the user will be given access to the MMSs menu. If the fingerprint does not match, access to the MMSs menu will be denied. Primary biometric authentication can be implemented on certain smartphones and not on feature phones. It is a third-party application which is implemented outside the USSD channel.

Chakraborty et al. (2016) developed a shoulder-surfing resistant password authentication model based on alphanumeric passwords which the authors called "Mobsecure." During authentication, the user is presented with colored alphabets and numbers from where a response to the challenge is made. In order to key in the characters of the alphanumeric password, the system communicates a challenge to the user through an earphone. The user follows already memorized rules to provide an answer to each challenge. Once the challenges are correctly responded to, the user will be logged in. This is a third-party application solution to securing users' PIN at the mobile interface and will not be implemented on feature phones and the USSD channel.

Shinde and Shedge (2018) noted that shoulder surfing attacks are a big security threat for authentication processes based on applications such as mobile phones, computers, and banking systems. The authors designed an authentication system containing PassMatrix, which is based on password images. During authentication, a one-time login indicator which is sent to the user through an audio message enables a user to locate their image password grid without clicking or touching it. An attacker can make use of the indicator to identify the pass image. During registration, the user selects a desired number of password images, but each image contains only one pass square. During authentication, the user provides the username which the system uses to generate pass-images. The generated random number (indicator) is communicated to the user through audio means. The images are displayed in a 6*6 bar, where each image has a horizontal and vertical bar running through it. It is equally a third-party application to be implemented on smart devices and not on feature phones and USSD channels.

Alhusainy and Uliyan (2018) designed a textual password authentication model to protect users' passwords against shoulder surfing. The designed model does not require the user to press the keys representing the password. The model presents a 6*6 keyboard to the user, instead of the device keyboard. The user is required to click on the arrow pointing to the column

Article DOI: 10.52589/AJENSR-DPCGWN0X
DOI URL: https://doi.org/10.52589/AJENSR-DPCGWN0X

containing the desired character of the password. After first clicking, the keyboard is transposed, changing all characters on the column to be on rows. This process continues till all the characters of the password are completed. This process is a third-party application; it will cut off feature phones and will not be implemented on the USSD channel.

Binitie et al. (2020) designed a model to secure users' data at the mobile interface during USSD transactions based on Bag of Soft Biometrics (BoSB) data only. The designed model preserved the existing protocol services, transaction, and message structures of USSD banking in Nigeria. The client's soft biometric details were collected during registration and stored in the database. These soft biometric details were assigned identifiers known to the user and were requested from the user during authentication in place of a PIN. This is a third-party application stored in the user's mobile device and is activated at the authentication stage during the USSD banking transaction. This model cannot be implemented on the USSD channel and feature phones since it is a third-party application.

These models discussed above share similar features. They are all third-party application solutions that could not be implemented on the USSD channel and will cut off feature phones.

DESIGN METHODOLOGY

For the model design, the existing architecture of deployment of USSD in the banking system, as shown in Figure 2, is adapted. In the deployment of USSD technology in banking, it uses the same general USSD architecture (Nyamtiga et al., 2013).

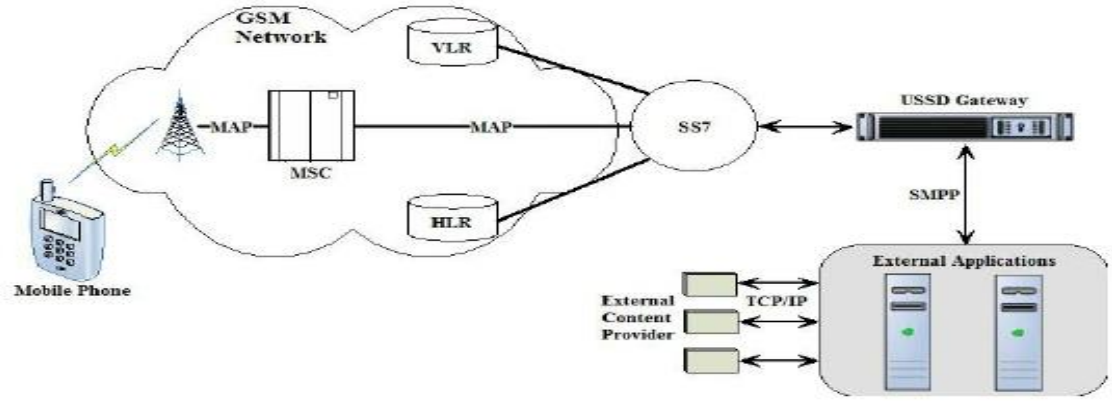

Figure 2: General USSD architecture (Nyamtiga et al., 2013)

Client registration plays an important role in the methodology. It is during this stage that the user provides answers to queries relating to soft biometrics with which the client is familiar. 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

Article DOI: 10.52589/AJENSR-DPCGWN0X
DOI URL: https://doi.org/10.52589/AJENSR-DPCGWN0X

linked to the account number for easy identification. Figure 3 shows the components of the designed model. To provide confidentiality (security against shoulder surfing attack) to users' PIN, instead of the customer entering the PIN directly as it is common in the direct or standard PIN entry method being used in USSD banking today, the system will present 8 different options, each containing 10 digits, among which one of the options contains the PIN digit in left to right (LTR) order. It is important to note that the user's chosen PIN is 5 digits, and this digit will be presented in two stages of 3 digits at each stage. After successful PIN authentication, the user will be presented with a question relating to soft biometric details provided during registration to select the right option. 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 before being 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 PIN as shown in algorithm 2 and BoSB details of the client. Securing the PIN from the mobile interface against shoulder surfing, and the use of BoSB makes the Replay attack impossible.

To provide confidentiality to the user's identity, three methods are proposed:

i. Randomization Obfuscation method

ii. Bag of Soft Biometric (BoSB) authentication/verification method

iii. One-time Password (OTP).

1. **"Randomization Obfuscation" Technique:** Obfuscation is a technique that makes binary and textual data hard to understand. It is hard for the shoulder surfer to understand which of the displayed options contains the PIN digits, but easy for the user. Obfuscation method will make the original PIN difficult or complicated for shoulder surfers or hackers to understand (Brooks, 2005). It also requires less computing power and a less expensive measure against reverse engineering (Brooks et al., 2012). Users' 5-digit numbers will be obfuscated within the 10 random numbers generated at each instance of the two stages of PIN authentication. The integer generated is converted to an array and shuffled. The PIN will be obfuscated by randomizing the placement of the real PIN within the 10-digit number. Randomization obfuscation is a technique that randomly inserts or changes some elements of code without changing the semantics (Jodavi et al., 2015). Though this method is commonly applied by researchers in data mining and databases, it can be applied equally in the production of a usable dataset that can be directly displayed to end users, and this is supported by data obfuscation (Baken et al., 2004). Randomization obfuscation technique will be applied in the formation of the option with the correct PIN digits, which will be displayed among other options for the user to select from. This method will not pay attention to the position of the digits of the PIN. This technique allows the system to link the data back to the original owner. This is necessary not just to create security but also a smooth payment experience among users with feature phones.

2. **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

Article DOI: 10.52589/AJENSR-DPCGWN0X
DOI URL: https://doi.org/10.52589/AJENSR-DPCGWN0X

African Journal of Environment and Natural Science Research
ISSN: 2689-9434
Volume 7, Issue 1, 2024 (pp. 13-27)
www.abjournals.org

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).

3. **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). It will be required before a user can have access to any of the services.

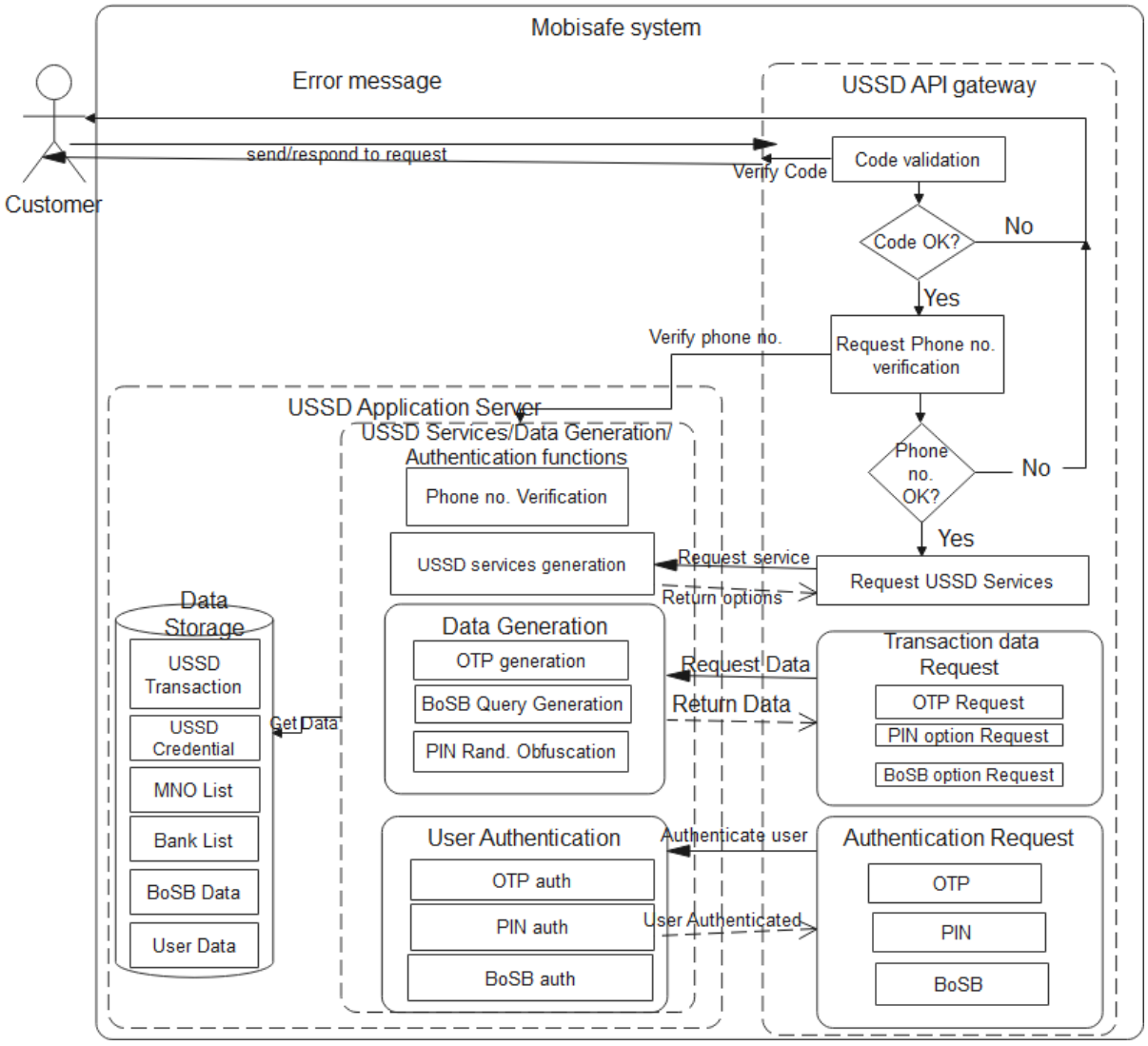

Figure 3: Proposed System Architecture

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.

Article DOI: 10.52589/AJENSR-DPCGWN0X
DOI URL: https://doi.org/10.52589/AJENSR-DPCGWN0X

The six (6) architectural constraints of the REST Application Programming Interface (API) are Uniform Interface, Client-Server, Stateless, Cacheable, Layered, and Code on Demand.

Authentication Algorithm

One-Time Password (OTP), Personal Identification Number (PIN), and Bag of Soft Biometric Data (BoSB) provides security to the system. The transaction will not be authorized until all of these security features are verified successfully. OTP will be the first security feature used to allow a user access to the USSD service, followed by the PIN (from randomization) to authenticate a user and finally, 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.

Randomization Obfuscation Technique

Unlike the "direct entry PIN" method, our system is designed to automatically generate ten (10) random integer numbers which will further be converted to an array (options) of eight sets, as shown in Algorithm 1. Out of the eight array sets, one will be selected at random and the user's chosen digit PIN will be randomly placed in left to right order and presented to the user in two stages, as shown in Algorithm IV. At the first stage, the user will be presented with eight different options containing ten (10) different digit numbers from which the user is requested to select the option that contains the "first" three (3) digits of the user's PIN, as shown in Figure 4. Next, eight options are presented to the user and requested to select the option that contains the last three (3) digits of the user's chosen PIN, as shown in Figure 5. It is important to note that the user's chosen PIN used in this design is 5 digits; this means that the digit in the middle will appear twice in the first and second stages. After a successful PIN entry, the user will be presented with a soft biometric question. If the response is correct, the transaction goes successfully, else it terminates. Merging soft biometrics with PIN will result in higher security (Garg et al., 2018).

Algorithms 1: PIN Randomization Obfuscation

Algorithm 1 shows how users' PIN will be concealed from an attacker using the randomization obfuscation method. To conceal the PIN from the shoulder surfer, the user-defined function, *insertreal1()*, inserts randomly the first three digits of users chosen PIN in left-to-right (LTR) order. 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 IV shows how one of the 8 generated wrong arrays (options) will be picked and the first 3 digits of users PIN will be randomly injected in the right order. This means that each correct digit PIN will replace any existing digit at the random position selected. This process is repeated for the last 3 digits of the PIN.

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 to array with 10 entries***

Article DOI: 10.52589/AJENSR-DPCGWN0X
DOI URL: https://doi.org/10.52589/AJENSR-DPCGWN0X

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 another number***

iv. **Get set of digits:** numset = array();

for ($x = 0; $x<=7; $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(0,8); ***//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 8 set of numbers:** numshow = shuffle(numset); ***// shuffle them and output as***

a set (8 groups of 10 digits with only one

vii. **Return array: numshow ; *//Return vii to the USSD interface for use***

Figures 4 and 5 show both the queries presented to the user of which only one option contains the users' PIN in the right order and also the response given by the user. From both figures, users' responses were 4 and 7. This means that the options with the identifiers 4 and 7 contain

Article DOI: 10.52589/AJENSR-DPCGWN0X
DOI URL: https://doi.org/10.52589/AJENSR-DPCGWN0X

the first 3 and last 3 digits of the users' 5-digit PIN respectively, in the right order. The identifiers are what a shoulder surfer will see without being able to capture the exact PIN digits represented by these identifiers. These identifiers are not constant but change with each transaction.

Figure 4: 1st 3-digit PIN of a user

Article DOI: 10.52589/AJENSR-DPCGWN0X
DOI URL: https://doi.org/10.52589/AJENSR-DPCGWN0X

African Journal of Environment and Natural Science Research
ISSN: 2689-9434
Volume 7, Issue 1, 2024 (pp. 13-27)

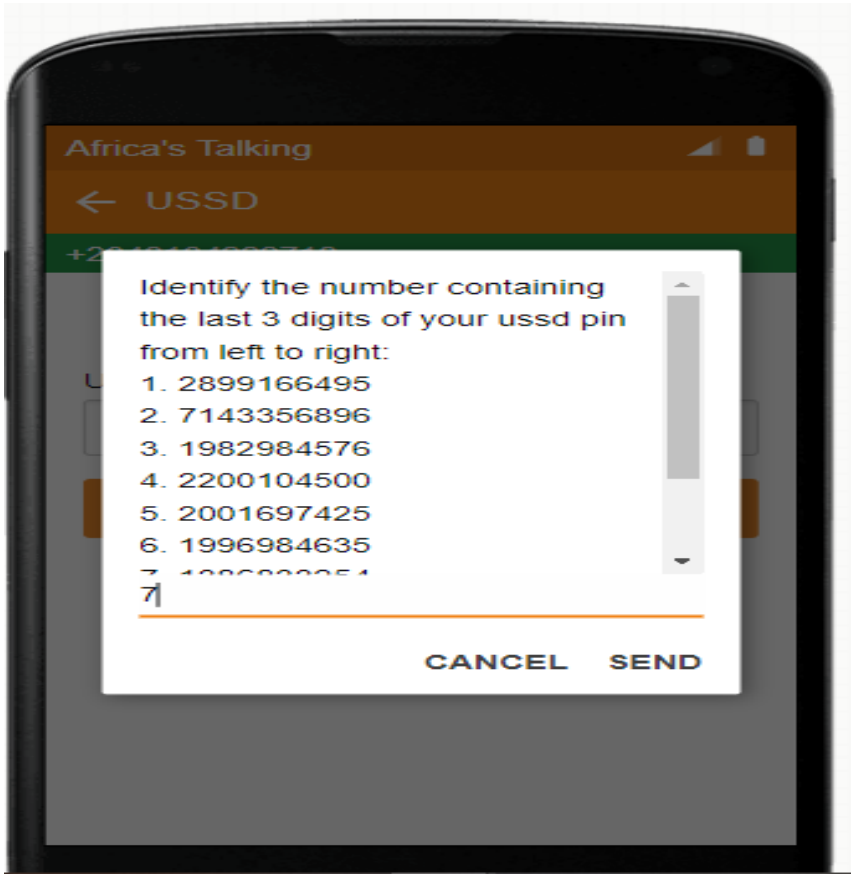

Figure 5: Last 3-digit PIN

Algorithm 2: PIN Validation

User responses to system-generated queries/requests will be validated and verified against the existing data to enable secured user authentication. Algorithm 2 shows how the model validates the response submitted by the user during the USSD transaction. Algorithm 2ii shows that the system will first search for the order of the PIN submitted and then as algorithm 2iii shows, the order of the PIN submitted will be checked against the stored users' PIN. If it matches, the transaction continues, else, an error message will be displayed.

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

Article DOI: 10.52589/AJENSR-DPCGWN0X
DOI URL: https://doi.org/10.52589/AJENSR-DPCGWN0X

```
} else{
return false //ERROR MESSAGE
}
```

DISCUSSION AND FINDINGS

The research revealed that the PIN entered for user authentication during a USSD transaction appears in plain text on a mobile interface because the USSD channel accepts data in plain text only. This means that any authentication model to be implemented in the USSD channel against shoulder surfing must be in plain text. These findings led to the design of a new authentication model.

CONCLUSION

The designed model uses randomization obfuscation method to conceal the user's PIN from a human shoulder surfer as against the existing direct PIN entry method where the user enters only the PIN in plain text. Additional security requires the user to enter a one-time password (OTP) and BoSB details. These three details will be required from the user before any transaction is authorized. The implementation of the new system will provide the non-existing security at the mobile interface in USSD transactions against human shoulder surfers and this makes USSD a safer technology in African environs where it is mostly used.

REFERENCES

1. Africa's talking (2021). Powering communications solutions across Africa. Retrieved from africastalking.com on June 15th, 2021.
2. Al-Husainy, M. A.F. and Uliyan, D.A. (2018). A smooth textual password authentication against shoulder surfing attack. *Journal of Theoretical and Applied Information Technology*, 96(09), 2546-2556.
3. Almuairfi, S., Veeraraghavan, P. and Chilamkurti, N. (2013). A novel image-based implicit password authentication system (IPAS) for mobile and non-mobile devices. Mathematical and Computer Modelling, 58(1–2), 108–116.
4. Baken, D.E., Parameswaren, R., Blough, D.M., Franz, A.A., & Palmer, T.J. (2004). Data obfuscation: anonymity and desensitization of usable data sets. IEEE security and privacy, 2(6) Pp. 34-41.
5. 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.

Article DOI: 10.52589/AJENSR-DPCGWN0X
DOI URL: https://doi.org/10.52589/AJENSR-DPCGWN0X

6. 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.*
7. Brooks, R.R, (2005). Disruptive security technologies with mobile code and peer-to-peer networks, CRC Press: Boca Raton, FL, 2005.
8. Brooks, R.R., Yun, S.B and Deng, J. (2012). Cyber-physical security of automotive information technology. Boston: Morgan Kaufmann, 655-676.
9. Briceno, M., Goldberg, I., and Wagner, D. (1999). A pedagogical implementation of A5/1,
Available at: http://www.scard.org/gsm/a51.html
10. Bryan, P. (2021). Back in the u.s.s.d: most smartphones owners-especially women- don't use apps for financial services. Retrieved from, nextbillion.net/ussd-smartphone-women-financial-services/ on January 7th, 2021.
11. 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
12. 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.
13. Chakraborty, N., Randhawa, G., Das, K. and Mondel, S. (2016). Mobsecure: A shoulder surfing safe login approach implemented on mobile device. *6th International Conference on Advances in Computing and communications, ICACC*, Cochin India, 854-861.
14. Choi, M., Lee, J., Kim, S., Jeong, Y.S., and Park, J.H. (2016). Location-based authentication scheme using BLE for a high-performance digital content management system. Neuro computing, 209, 25–38.
15. 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.
16. Garg, R., Arora, A., Singh, S & Saraswat, S. (2018). Biometric Authentication using Soft Biometric Traits. *5th IEEE International Conference on Parallel, Distributed and Grid Computing(PDGC-2018)*, Solan, India, Pp. 259-264.
17. Globitel, (2018). USSD gateway, Available at: www.globitel.com/ussd-gateway/
18. Gupta, P.(2010). *End-to-End USSD System*. Tata Teleservices Ltd, India
19. Handfield, R. (2017). Data collection: electronic or manual? NC State University. Retrieved from scm.ncsu.edu/scm-ar… on 12th June 2018.
20. 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
21. Heroku Sales Force Company (July 7th, 2021). Cleardb mysql. Retrieved from www.devcenter.db.heroku.com/article/cleardb, on 12th July 2021.
22. 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/

Article DOI: 10.52589/AJENSR-DPCGWN0X
DOI URL: https://doi.org/10.52589/AJENSR-DPCGWN0X

23. Jodavi, M., Abadi, M., Parhizkar, E. (2015). Jsobfusdetector: a binary pso based one-class
classifier, ensemble to detect obfuscated javascript code. 2015 IEEE International symposium on Artificial Intelligence and signal Processing (AISP), Mashhad Iran, Pp. 322-327. Retrieved on 15th February 2021 from researchgate.ne/publishers/279861980
24. Kwon, T., Shin, S. and Na, S. (2014). Covert attentional shoulder surfing: human adversaries are more powerful than expected," *IEEE Transactions on System, Man and Cybernetics: System*, 44(6), pp. 716-727.
25. Mekala, S. R (2015). Mobile credit using gsm network, top-up for mobile phone. *MSC thesis*
at Faculty of computing, Blakinge Institute of Technology, Kariskrona, Sweden. Retrieved from, www.divaportal.org on January 14th, 2020.
26. Mtaho, A. B. (2015). Improving Mobile Money Security with Two-Factor Authentication. *International Journal of Computer Applications, 109(*07*)*, 0975 – 8887.
27. 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.
28. Por, L.Y., Ku, C.S. and Ang, T.F. (2019). Preventing shoulder surfing attacks using digraph substitution rules and pass-image output feedback, *Journal of Multidisciplinary Digital Publishing Institute, Symmetry, 11.*
29. 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.
30. Satoricyber.com (2022). The fundamentals of data obfuscation. Retrieved from https://satoricyber.com/data-masking/the-fundamentals-of-data-obfuscation/ on August 12th, 2022.
31. Shinde, P. and Shedge, K. (2018). PassMatrix- An authenticartion system to resist shoulder
surfing attacks. *International Research Journal of Engineering and Technology*, 5(03), 296-299.
32. Shore, J. (24th September,2021). Cloud application. Retrieved from https://searchcloudcomputing.techtarget.com/definition/cloud-application , on December 11th, 2021.
33. Waghmare, P., Longadge, R . and Kapgate, D. (2014). A review on shoulder surfing attack in
authentication technique. International Journal of Computer Science and Network (IJCSN), 3(6), 573-576.
34. 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.

Article DOI: 10.52589/AJENSR-DPCGWN0X
DOI URL: https://doi.org/10.52589/AJENSR-DPCGWN0X