A Secured Mobile Money Transaction Using Data Masking and Enhanced Base64 Algorithm

https://doi.org/10.3991/ijes.v9i1.17803

Abolore Muhamin Logunleko (✉)
Gateway ICT Polytechnic, Sapaade, Ogun State, Nigeria
abolore.logunleko@gaposa.edu.ng

Kolawole Bariu Logunleko, Opeoluwa Olanrewaju Lawal, Onyinyechi Ogochukwu Doris Ezugwu, Olorunsesan Sunday Akinyemi
DS Adegbenro ICT Polytechnic, Eruku-Itori, Nigeria

Abstract—There is always a need to transfer money from one user to another for either payment of services or settlement of business transactions and so on. Research has shown that traditional money transaction systems are prone to attacks through falsified deposit slips and drafts, theft of debit cards, forgery of signatures, use of false cheques and so on. Electronic money transaction is a payment performed from an electronic device which enables users to have access to their money anywhere and at any time with the aid of a network but not adequately secured. This application offers a platform independent of securing and transferring money using data masking and an enhanced base64 algorithm from one account to another. The study improves on existing money transfer and transaction systems by achieving a secured mobile money transaction system with masked and encrypted financial details both on the mobile application and also on the short message service application (Text Message Notification) sent to user's platform which makes it difficult for third party to intercept and understand.

Keywords—Masking, Enhanced Base64 Algorithm EB64, Short Message Service SMS, Cipher, Encryption, Mobile Application

1 Introduction

Sending or receiving money for either payment of services, settlement of business transactions, payment of utility bills, or for family support is common both for businesses and individuals because there always be a necessity to transfer money from one user to another. It requires efficient, reliable and affordable money transfer services whereby money can be deposited in one location and withdrawn in another in both urban and rural areas.

Electronic money transfer is a controlled payment service via internet that allows individual to gain access to their money at any point in time without the need to go to a bank for such services. Money is changed into electronic money (e-money) and kept electronically so that individual can make use of it for payment of utility bills, digital payment, and so on [1].

More Nigerians have been found to own gadgets that can connect them to the internet than bank accounts, thereby demonstrating the great potential of online money transfer in Nigeria. However, since its inception, online money transfer has been reported to make very little impact in the country. But with the policy put in place by the Central Bank of Nigeria (CBN) on cashless Nigeria the future of money transfer in the country lies in the hands-on electronic transfer [2].

Nigeria's primary aim of electronic money transfer is to promote a cashless society by providing financial inclusion for the over 80 million Nigerians who do not own bank accounts. 77% of adults in Nigeria are unbanked while there is well over 54% mobile penetration rates. This is especially significant because of the fact that 57% of Nigerians live in the rural areas where financial institutions find it commercially unviable to operate; thus, emphasizing the immense potential of electronic money transfer services in Nigeria [3].

Research has proven that traditional money transfer systems are prone to attacks through falsified deposit slips and drafts, forgery of signatures, use of false cheques. And also, there will be a greater need in the society to transfer money (especially in large amounts) through an electronic platform. This would help to solve the inability to withdraw physical cash (over N500, 000) and give it to another individual or organization. A lot of transactions which are required to take place during the weekend or after banking hours cannot happen because banks do not open on weekends and do not attend to customers after hours. Furthermore, modern money transfer needs a very strong and adequate security during the process of money transfer and transaction. Therefore, this study offers a secured platform independent way to transact money from one place to another using an enhanced base64 algorithm and data masking at any time and on every day of the week. The study aimed at improving on existing mobile money transaction systems thereby offers a data hidden and secured means of money transaction.

The rest of the paper is arranged as follows: Section 2 provides existing literature and some related works. Section 3 focuses on the methodologies. Section 4 presents the results and discussions, section 5 concludes the paper, Section 6 is the references and Section 7 is the authors.

2 Literature Review

2.1 Theoretical frame work

Money is anything that is widely used and accepted in transactions involving the transfer of goods and services from one person to another [4]. Mobile money is the use of a mobile phone in order to transfer funds between banks or accounts, deposit or withdraw funds, or pay bills. This term is also used for the broader realm of electronic commerce; it can refer to the use of a mobile device to purchase items, whether physical or electronic [5].

Money Transfer Systems offers a quick and easy way to transfer electronic funds which can be used by both individuals and businesses with internet-based devices. Electronic money is broadly defined as an electronic store of monetary value on a technical device that may be widely used for making payments to undertakings other than the issuer without necessarily involving bank accounts in the transactions, but acting as a prepaid bearer instrument. Money Transfer Systems are essential in the future of Nigeria with the cashless policy that has been put in place by the Nigerian government [2].

Data that can be read and understood without any special measures called a plaintext. The method of disguising plaintext in such a way as to hide its substance is called encryption. Encrypting plaintext results in unreadable gibberish called cipher text. The process of reverting cipher-text to its original plaintext is called decryption [6].

[7] [8] discussed that cryptography is the science of secret writing with the goal of hiding the meaning of a message. The main aim of these cryptographic techniques is to forestall snooping and to reduce the chance of an attacker detecting the cryptosystem. This method is highly recommended when there is a need for the transmission of the data among people [9]. They classified the concept of cryptography into two classes, symmetric or asymmetric, depending only on whether the keys at the sender and receiver are easily computed from each other. In asymmetric cryptography, a different key is used for encryption and decryption while in the symmetric cryptography, sender and receiver share the same key (K), which is unknown to the attacker, and uses it to encrypt and decrypt their communications channel.

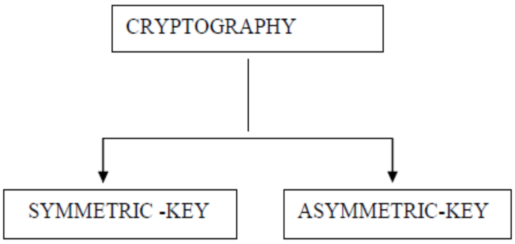


Fig. 1. Concept of Cryptography

Symmetric key cryptography: In symmetric-key cryptography, the same key is used by both parties. The sender uses this key and an encryption algorithm to encrypt data; the receiver uses the same key and the corresponding decryption algorithm to decrypt the data as shown in figure2.

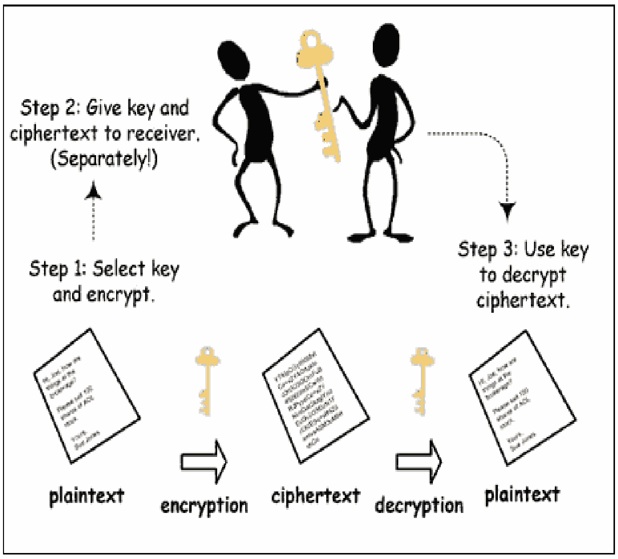

Step 2: Give key and ciphertext to receiver. (Separately!)
Step 1: Select key and encrypt.
Step 3: Use key to decrypt ciphertext.
plaintext
encryption
ciphertext
decryption
plaintext

Fig. 2. Symmetric-key Cryptography

Asymmetric-key cryptography: In asymmetric or public-key cryptography, there are two keys: a private key and a public key. The private key is kept by the receiver. The public key is announced to the public. This is shown in figure3.

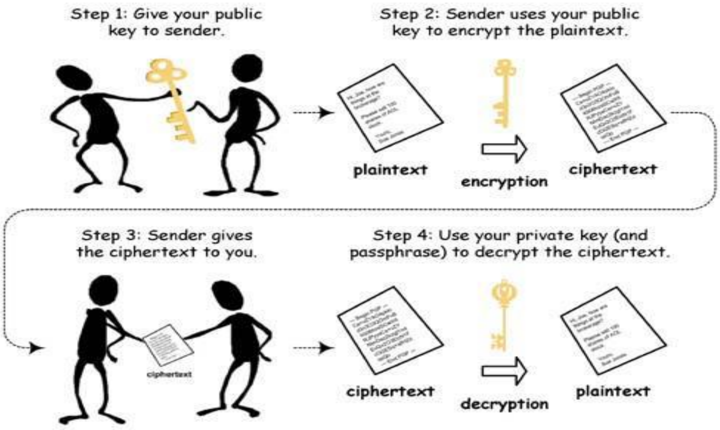

Step 1: Give your public key to sender.
Step 2: Sender uses your public key to encrypt the plaintext.
plaintext
encryption
ciphertext
Step 3: Sender gives the ciphertext to you.
ciphertext
Step 4: Use your private key (and passphrase) to decrypt the ciphertext.
ciphertext
decryption
plaintext

Fig. 3. Asymmetric-key Cryptography

2.2 Conceptual frame work

Cryptographic model: There are two conceptual models which are as follows: Symmetric model and Asymmetric model. In symmetric model, encryption key is the decryption key and in asymmetric model, encryption key is not the decryption key. Thus, Symmetric encryption uses Symmetric key or private key and Asymmetric encryption uses a public key. In Symmetric encryption only one key is used for communication while in Asymmetric encryption two different keys are used for communication. This paper uses the concept of symmetric model for it model.

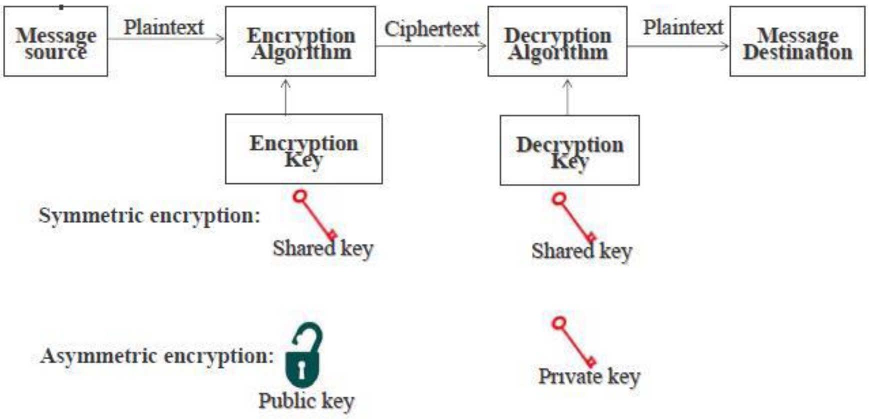


Fig. 4. Cryptographic Model

2.3 Empirical frame work

Different authors have proposed various techniques to give security to mobile money transactions. Grabianowski, et al. [10] revealed that Paypal allows people to make financial transactions online by granting the ability to transfer funds electronically between individuals and businesses. It allows customers to send, receive, and hold funds in 26 currencies and also to donate to charity, buy items online, etc. EWP (encrypted website payments) EWP is a paypal payments standard feature that uses public and private keys to encrypt the payment button code used on merchant websites. The encryption hides the payment details so they cannot be seen by anyone viewing the website source code in browser.

Brandom, R. [11] discussed Two-tier security mechanism, is an extra layer of security that requires not only a password and username but also something that only, and only, that user has on them, i.e., a piece of information only they should know or have immediately to hand-such as a physical token

Logunleko, et al. [12] carried out a research that produces a technical technique of the differential computation of the encryption algorithms. The aim to be considered is the security of the encrypted data against pattern recognition attack. The research therefore filled the gap of security threat in EB64 pseudo code as compared with the newly proposed EHB64 pseudo code. In addition, this newly concept introduced generates a symmetric key by shuffling the original key with the textual data, thus making the transformation of each character of the data better each time it is shuffled. Thus the final output of the key-based pseudo code will be stronger than the pseudo code of EB64. Therefore, the developed concept secures the data more adequately than the existing one because of the designed pattern and confusion created during the process.

Logunleko, et al. [13] carried out a study on security assurance framework for intelligible information using a customized base64 encryption algorithm to develop a framework for information security model for both encryption and decryption process. The authors used the developed framework to transform the inputted characters to limited characters as compared to others encryption algorithms without the use of key being introduced in the algorithmic process. Thus, the algorithm could be standardized using key mechanism like others standardized key-based encryption and decryption algorithms.

Robbi, R. [14] conducted a study titled combination Base64 Algorithm and End-Of-File (EOF) Technique for Steganography. Steganography consists of a set of methods and techniques to embed the data into another media so that the contents are unreadable to anyone who does not have the authority to read these data. The authors discussed steganography and encoding techniques using base64, which is encoding scheme that converts the same binary data to the form of a series of ASCII code. Also, the EoF technique is used to embed encoding text performed by Base64. The authors further explained that the usage of the two methods together will definitely increase the security level for protecting such data. Hence, the research aimed to secure many types of files in a particular media with a good security and not to damage the stored files and coverage media being used.

Bamasak, O. [15] carried out study in Saudi Arabia found that there is a bright future for m-payment. Security of mobile payment transactions and the unauthorized use of mobile phones to make a payment were found to be of great concerns to the mobile phone users. Security and privacy were the major concerns for the consumers.

Motawie, et al. [16] revealed how Base64 algorithm was implemented to encode the JAR file for securing data from unauthorised users. The proposed work gives benefits of log files, and these log files send to Administrators periodically. The Administrators nullify the user and prohibited them from further access to data. The approach demonstrates accountability in a highly distributed manner.

3 Methodology

The model is developed to secure mobile money transaction using enhanced base64 algorithm and data masking which are the tools that ensure the security of users' messages at both user ends. The enhanced base64 algorithm was used to encode and decode large amount of textual data using concatenation of syntax on both side of the text while data masking added more security features to the model.

3.1 Data masking

Data masking is the method of hiding original data with modified content. The main reason for applying masking to a data is to protect sensitive data from unauthorised individual. Data masking is necessary in a numerous way such as protection of data from third-party vendors and operator error.

3.2 Description of the enhanced base64 algorithm

The enhanced base64 algorithm is designed to encrypt and decrypt huge amount of textual data using concatenation of <hgmn3>and </hg,3>on both side of the text, thereby giving it a different result. The scheme uses a concept of modern encryption algorithms. It is typically used when there is a need to encode binary data that needs to be stored and transferred through media designed to deal with textual data. This is to ensure that the data remains intact without modification during shipping. The scheme can be used commonly in multiple applications including email through MIME and storage of complex data in XML.

3.3 Pseudocode for enhanced base64 algorithm (Eb64)

This is as follows:

1. Add **<hgmn3>**and **</hg,3>**as prefix and suffix respectively to the plain text.
2. Get the ASCII code of each plain text.
3. Change each ASCII number to 8 bits Binary String
4. Merge the 8 bits to form 24 bits.
5. Then, split a 24 bit earlier to 6 bits.
6. Each 6 bit is changed into a decimal equivalent.
7. Finally, use the decimal equivalent to choose a character in Base64 character table

3.4 System architecture

As demonstrated in figure5, the model ensures the security of users’ transactions at both ends. It deals with a secured money transactions and a secured SMS notification via a non-server architecture network. The users initial the secured transaction via non-server architecture network which shall be authenticated by administrator (bank) before it gets to the receiver. The receivers received the secured transaction and decode it. The model secures mobile SMS end-to-end encryption (E2EE) method of communication. E2EE means that the senders or initiators are responsible to encrypt data (message) and all encrypted data (messages) transferred between different users of the system, the contents is only readable to the users who have the authority. In the architecture, the mobile carrier SMS Centre (SMSC) does the destination findings, and then sends the message to destination devices (cell phone).

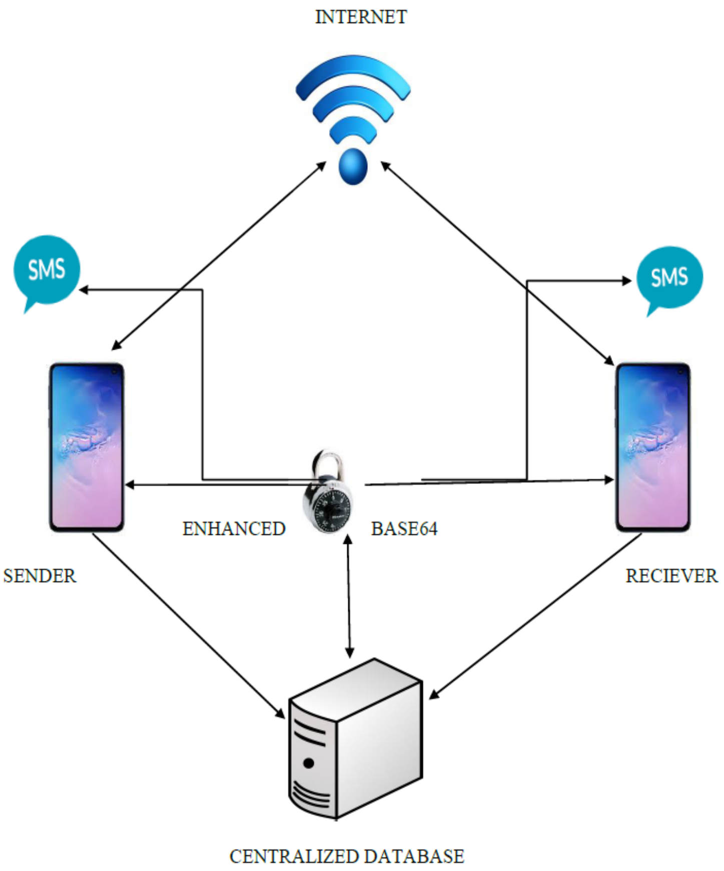


Fig. 5. System Architecture

3.5 System flow chart design

This section gives a detailed description of the system flow chart design as shown in figure6. After successful registration, the username and password are supplied through the login interface and MySQLi query statement search for the corresponding username and password in the "username" table and "password" table in the database.

If the login is correct, it disposes the login form and opens the interface for user to perform operations else it goes back to login

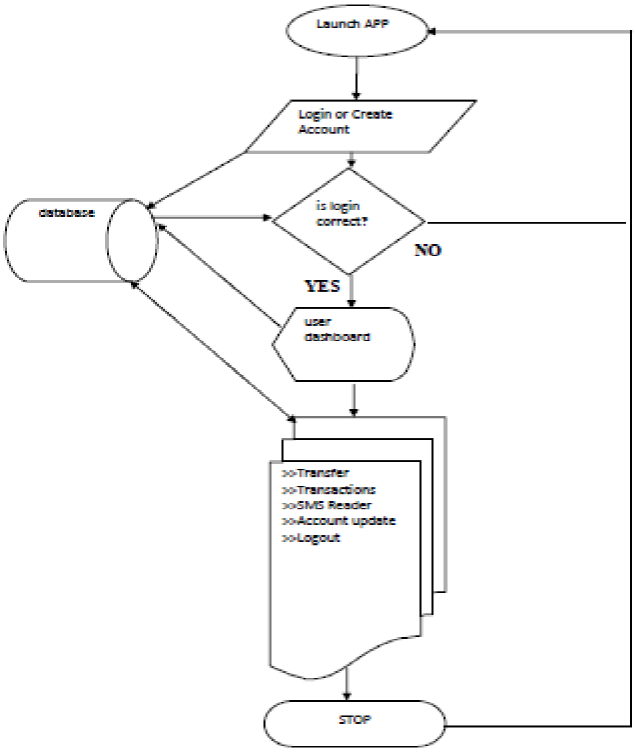


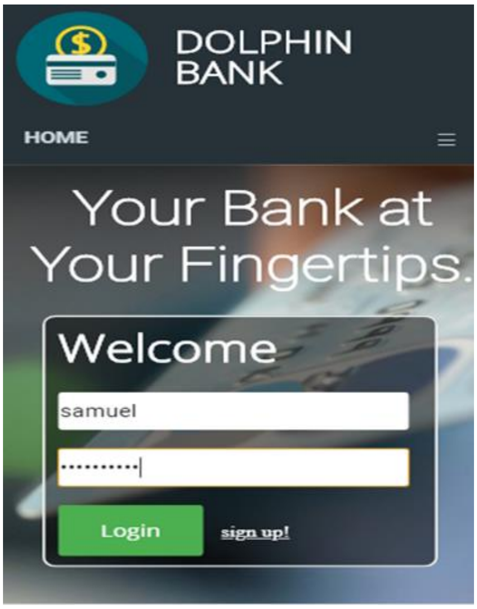
Fig. 6. System Flow chart Design

4 Results and Discussions

The algorithmic model was integrated into the mobile money transaction App or Application. The proposed Application 'Dolphin Bank Mobile' is a secured mobile money transaction application using data masking and an enhanced base64 algorithm. The Application was developed with the use of PHP, HTML5, CSS, JavaScript and Mysqli as database. The developed system hides some notable content of the transaction and this can only be unhidden by the authorised users. The developed system was tested on this system configuration:

Model:	TECNO LA6
Android version:	8.1
Device Name:	TECNO Pouvior 2
Processor:	ARM Cortex-A53, 1.3 GHz
RAM:	2.00GB
Phone storage:	16.00GB

The first interface of "Dolphin Mobile Banking" is a login interface and sign up interface that shows username and password input fields, just beside the form is a text link to create new account as shown in figure 7.



DOLPHIN BANK

HOME

Your Bank at Your Fingertips.

Welcome

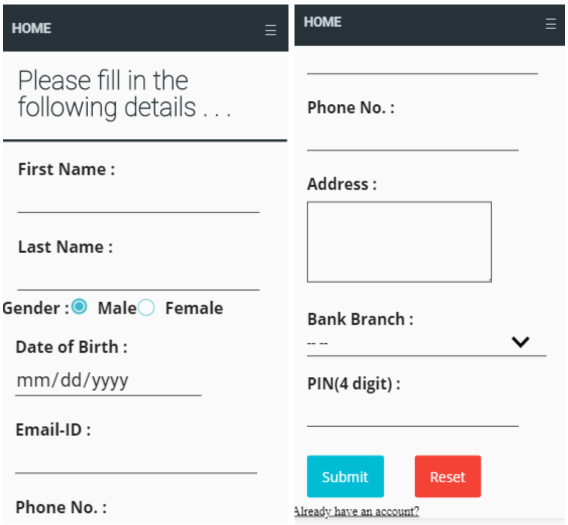
samuel

••••••••••

Login sign up!

Fig. 7. Login Page

On the sign-up page, there are request information such as name, gender, date of birth, email address, phone number, home address, nearest branch and 4-digit transaction pin as shown in figure 8.



HOME

Please fill in the following details . . .

First Name :

Last Name :

Gender : ● Male ○ Female

Date of Birth :

mm/dd/yyyy

Email-ID :

Phone No. :

HOME

Phone No. :

Address :

Bank Branch :

-- --

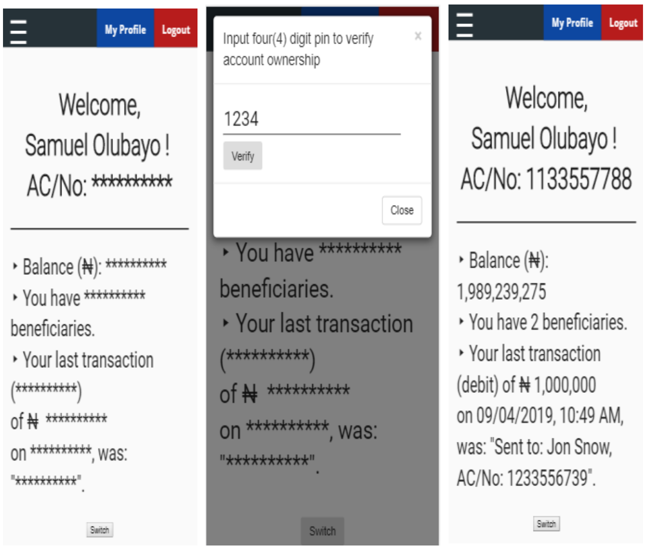
PIN(4 digit) :

Submit Reset

Already have an account?

Fig. 8. Sign up Page

Successful login user will be redirected to dashboard showing his/her account balance, number of beneficiaries, last transaction details and account number, all in encoded format which can be toggled back to plain text with the permission of the user by using personal identification number when click on switch button at the bottom of the page as shown in figure 9.



Welcome, Samuel Olubayo ! AC/No: **********

- Balance (₦): **********
- You have ********** beneficiaries.
- Your last transaction (**********) of ₦ ********** on **********, was: "**********".

Input four(4) digit pin to verify account ownership

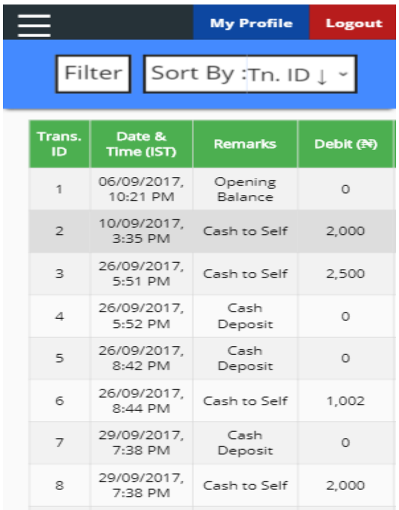
1234

Welcome, Samuel Olubayo ! AC/No: 1133557788

- Balance (₦): 1,989,239,275
- You have 2 beneficiaries.
- Your last transaction (debit) of ₦ 1,000,000 on 09/04/2019, 10:49 AM, was: "Sent to: Jon Snow, AC/No: 1233556739".

Fig. 9. Account Details Page

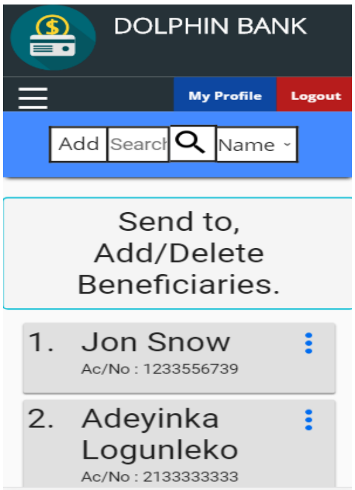
In figure 10, this screen holds and show previous records of money transfer (credit and debit) with each respective time and third-party sender when necessary.



Trans. ID	Date & Time (IST)	Remarks	Debit (₦)
1	06/09/2017, 10:21 PM	Opening Balance	0
2	10/09/2017, 3:35 PM	Cash to Self	2,000
3	26/09/2017, 5:51 PM	Cash to Self	2,500
4	26/09/2017, 5:52 PM	Cash Deposit	0
5	26/09/2017, 8:42 PM	Cash Deposit	0
6	26/09/2017, 8:44 PM	Cash to Self	1,002
7	29/09/2017, 7:38 PM	Cash Deposit	0
8	29/09/2017, 7:38 PM	Cash to Self	2,000

Fig. 10. User's Transaction Page

To transfer money from one user to another, the system will require the current user (sender) to add or select from previously registered beneficiaries, this screen appears immediately before input transfer details such as amount and transaction pin. This is shown in figure 11.



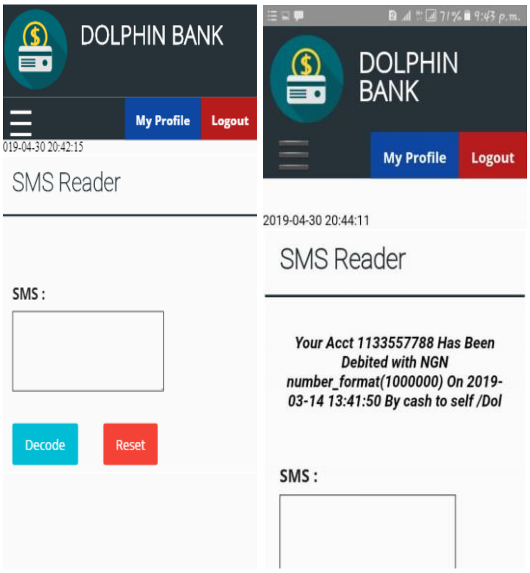
Send to, Add/Delete Beneficiaries.

1. Jon Snow
Ac/No : 1233556739

2. Adeyinka Logunleko
Ac/No : 2133333333

Fig. 11. List of Beneficiary Page

After each transaction, both the receiver and sender will be notified via Base64 encoded SMS. Figure 12 and 13 show the SMS notification.

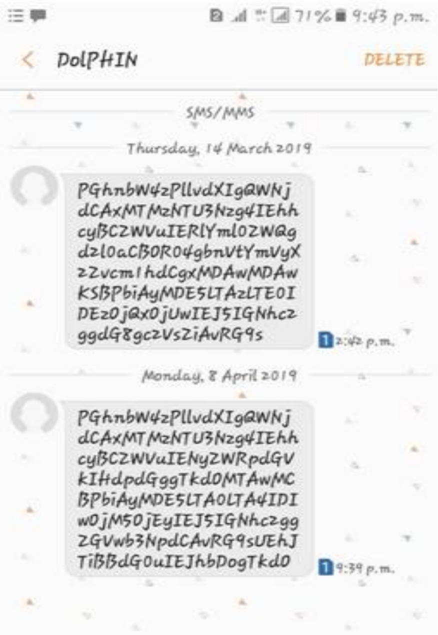


019-04-30 20:42:15

2019-04-30 20:44:11

Your Acct 1133557788 Has Been Debited with NGN number_format(1000000) On 2019-03-14 13:41:50 By cash to self /Dol

Fig. 12.SMS Encoder and Decoder



Thursday, 14 March 2019

PGhnbW4zPllvdXIgQWNj
dCAxMTMzNTU3Nzg4IEhh
cyBCZWVuIERlYml0ZWQg
dzl0aCB0R04gbnVtYmVyX
zZvcm1hdCgxMDAwMDAw
KSBPbiAyMDE5LTAzLTE0I
DEz0jQx0jUwIEJ5IGNhcz
ggdG8gczVsZiAvRG9s

2:42 p.m.

Monday, 8 April 2019

PGhnbW4zPllvdXIgQWNj
dCAxMTMzNTU3Nzg4IEhh
cyBCZWVuIENyZWRpdGV
kIHdpdGggTkd0MTAwMC
BPbiAyMDE5LTA0LTA4IDI
w0jM50jEyIEJ5IGNhczgg
ZGVwb3NpdCAvRG9sUEhJ
TiBBdG0uIEJhbDogTkd0

9:39 p.m.

Fig. 13.SMS Notification

4.1 Comparison

Based on the review of the exiting studies and the features of the proposed system, a comparative study between the Existing System, ES and the Proposed System, PS is demonstrated in the Table 1 using the following factors:

Table 1. Comparison between ES and PS

Factors	ES	PS
Encryption	Not Applicable	Applicable and Fast
Decryption	Not Applicable	Applicable and Fast
Speed	Fast	Faster
Layer of Security	Two	More than two
Security	Secure	Highly and Adequately Secure
Mask	Partially used on account number.	Fully used on account number, account balance and so on
Internet	Required	Required

5 Conclusion

The paper presented the use of data masking and enhanced base64 algorithm to hide and secure money transaction on mobile application. The application is implemented and designed on android phone which runs on a mobile phone and does not require any additional encryption devices. With the increasing use of SMS for alert notification, communication and information exchange, care should be taken when sensitive information is transmitted using SMS. Users should be aware that SMS messages might be subject to interception. Solutions such as encrypted SMS should be considered if there is a need to send sensitive information via SMS. Hence, SMS is an integral part of mobile communication and SMS security is undoubtedly useful and interesting. In general, the proposed model improves the existing system by adding more security features via the use of data masking and cryptography.

6 References

[1] Odior (2012): "Cashless Banking in Nigeria: Challenges, Benefits and Policy Implications" Retrieved from http://eujournal.org/index.php/esj/article/view/192.pdf

[2] CBN (2012): "Cash-less Nigeria" Retrieved from http://www.cenbank.org/cashless

[3] Yaqub, Bello, Adenuga, Ogundeji (2013) "The Cashless Policy in Nigeria: Prospects and Challenges" http://www.ijhssnet.com/journals/Vol_3_No_3_February_2013/20.pdf

[4] Mishkin, Frederic S. (2007) "The Economics of Money, Banking, and Financial Markets (Alternate Edition)." Boston: Addison Wesley. p. 8.ISBN 0-321-42177-9.

[5] Merrit Cynthia (2010) Mobile Money Transfer Services: "Mobile money Transfer Services: "The Next Phase in the Evolution in Person-to-Person Payments" Retrieved from https://frbatlanta.org/media/Documents/rprf/rprf_resources/wp0810.pdf?la=en

[6] Agoyi, M. & Seral, D. (2012) "SMS security: an asymmetric encryption Approach" Proc.6th International Conference on Wireles and Mobile Communication, 2012. https://doi.org/10.1109/icwmc.2010.87

[7] Rolf Oppliger, (2005) "Contemporary cryptography". Artech House computer security series, ISBN 1-58053-642-5

[8] Michael, N., Kelley, D., & Pillitteri, V.Y, (2017) "An Introduction to Information Security" https://doi.org/10.6028/NIST.SP.800-12r1

[9] Sheshadri, H.S, Shivaputra and Lokesha, V, (2015). "A Naïve Visual Cryptographic Algorithm for the transfer of a compressed Medical Images". International Journal of Recent Contributions from Engineering, Science & IT (iJES), Volume 3, Issue 4, Pp26-36. http://dx.doi.org/10.3991/ijes.v3i4.5190 https://doi.org/10.3991/ijes.v3i4.5190

[10] Grabianowski,Ed;Crawford, Stephanie (2014) "How Paypal Works" How stuff works.

[11] Brandom, R. (2017) "Study of Hidden Markov Model in Credit Card Fraudulent Detection." International Journal of Computer Applications, (0975 –8887), Volume 20–No.5. https://doi.org/10.5120/2428-3263

[12] Logunleko, A.M., Logunleko K.B., Odufowora M.Y. and Gbolagade K.A (2020) "A Differential Computational Encryption Modeling Technique on Textual Data" International Journal of Scientific Research in Computer Science and Engineering Vol.8, Issue.1, pp.81-86, E-ISSN: 2320-7639

[13] Logunleko K. B, Logunleko A. M, Akinwunmi O. O. & Lawal O. O. (2019) "Security Assurance Framework for Intelligible Information Using a Customized Base64 Encryption Algorithm" Proceedings of the 17th iSTEAMS Multidisciplinary Research Nexus Conference, D.S. Adegbenro ICT Polytechnic, Itori- Ewekoro, Ogun State, Nigeria, 21st – 23rd July, 2019.Pp 85-93. www.isteams.net - DOI Affix - https://doi.org/10.22624/AIMS/iSTEAMS-2019/V17N2P10 https://doi.org/10.5120/ijca2020920669

[14] Robbi, R. (2018) "Combination Base64 Algorithm and EOF Technique for Steganography" International Conference on Information and Communication Technology (IconICT): Journal of Physics: Conf. Series 1007.

[15] Bamasak, O. (2011) Exploring consumers' acceptance of mobile payments-an empirical Study. International Journal of Information Technology, Communications and Convergence 1: 173-185. https://doi.org/10.1504/ijitcc.2011.039284

[16] Motawie, R., El-Khouly, M.M & Samir Abou El-Seoud M. 2016. Security Problems in Cloud Computing. International Journal of Recent Contributions from Engineering, Science & IT (iJES), Volume 4, Issue 4, pp36-40. https://doi.org/10.3991/ijes.v4i4.6538

7 Authors

Logunleko Abolore Muhamin MCPN, MNCS, CiTP, MAITP, MITSSP, MNITPCS, GNIM is a Lecturer at the Department of Computer Science, School of Science and Technology, Gateway ICT Polytechnic, Saapade, Ogun State Nigeria. He bagged B.Sc (Hons) Degree in Mathematical Sciences (Computer Science Option) at Federal University of Agriculture, Abeokuta, Ogun State, Nigeria and Master of Science Degree in Computer Science at prestigious Premier University, University of Ibadan, Oyo State, Nigeria. He is a PhD Student of the Department of Computer Science, Kwara State University, Malete, Ilorin, Kwara State, Nigeria and a Chartered Information Technology Professional with 13 years teaching experience. He has published papers in both local and international reputable journals and conferences. He is an active member of Computer Professionals (Registration Council of Nigeria)**,** an active member of Nigeria Computer Society and active Member Academia in Information Technology Professional among many others. His research interest areas are: Computer Arithmetic, Bioinformatics, Cryptography, Information Security, Computer Networks and Security, Database Management, Data Communication, Software Engineering, Web Technology and Computer Information System among others. **Email:** abolore.logunleko@gaposa.edu.ng

Logunleko Kolawole Bariu MCPN, MNCS, CITP, MAITP is a Lecturer at Computer Science & Statistics Department, Faculty of Science and Engineering, D.S Adegbenro ICT Polytechnic Eruku-Itori, Ewekoro, Ogun State Nigeria. He bagged B.Sc (Hons) Degree in Mathematical Sciences (Computer Science Option) with Second Class Upper Division at Federal University of Agriculture, Abeokuta, Ogun State, Nigeria and Master Degree in Computer Science at prestigious Premier University, University of Ibadan, Oyo State, Nigeria. Besides, Logunleko, K.B is a Chartered Information Technology Professional with over 13 years teaching and lecturing experience and publications in both local and international journals and conferences. He is an active member Computer Professionals (Registration Council of Nigeria)**,** an active member of Nigeria Computer Society and active Member Academia in information Technology among many others. His research interest areas are: Computer Networks and Security, Cryptography, Data Communication, Computer Numerical Analysis, Knowledge Based System, Information Security, Software Engineering, Computer Information System among others. **Email:** logunleko.kolawole@dsadegbenropoly.edu.ng

Lawal Opeoluwa Olanrewaju is a Computer Science Lecturer at D.S Adegbenro ICT Polytechnic, Itori, Ogun State, Nigeria. He has a Bachelor of Science in Computer Science from Ambrose Alli University, Ekpoma and Master of Science in Computer Science from Ajayi Crowther University, Oyo, Nigeria. He is married and blessed with children. He has several published papers/articles to his credit. **Email:** opepolawal@gmail.com

Ezugwu Onyinyechi Ogochukwu Doris is a senior technologist at the department of computer science, D.S Adegbenro ICT Polytechnic Itori, Ewekoro, Ogun State, Nigeria. She has over eight (8) years of experience in teaching. Ezugwu completed her PGD at Federal University Abeokuta and currently running her Master of Science Degree. Her research interest lies on area of computer security. She has many collaborated activities with researchers in several other areas of computer science. Ezugwu has served two conferences program committee. She is happily married to Engr. Ezugwu Joseph with children. **Email:** ogochukwudoris@yahoo.com

Akinyemi Olorunsesan Sunday holds Master Degree in Computer Science from Ajayi Crowther University, Oyo, Nigeria and Bachelor Degree in Computer Science from Crescent University Abeokuta, Nigeria. He also bagged Higher National Diploma (HND) in Electrical / Electronics Engineering from Osun State College of Technology, Osun State, Nigeria and Post Graduate Diploma in Electronics/Computer Engineering from Lagos State University, Lagos, Nigeria. Besides, he has many publications with more than twelve (12) years of versatile professional work experience both in Lecturing and as a Technologist at D.S Adegbenro ICT Polytechnic, Itori Ewekoro, Ogun State, Nigeria. **Email:** sessygee_m@yahoo.com

Article submitted 2020-08-15. Resubmitted 2020-10-28. Final acceptance 2020-10-29. Final version published as submitted by the authors.