International Journal of Computer (IJC)
ISSN 2307-4523 (Print & Online)

http://ijcjournal.org/

Development of a Secure Mobile E-Banking System

Raphael Olufemi Akinyede[a]*, Odoseiye Aidohelen Esese[b]

[a,b]*Department of Computer Science, The Federal University of Technology, Akure. Ondo State, Nigeria*

[a]*Email: roakinyede@futa.edu.ng*

[b]*Email: greatestodose@gmail.com*

Abstract

Mobile banking refers to the usage of a telephone or different cellular device to carry out on-line banking responsibilities. Those responsibilities encompass account balance enquiry, funds transfer, bill payment, finding an ATM, etc. Considering the excessive fee of adoption of this technology, quite a few concerns are raised as regards user authentication, data confidentiality, non-repudiation, data integrity and service availability. This research, therefore, introduces a more advantageous comfortable model to help conquer challenges mentioned earlier. In other to attain the set goals, the proposed model uses a popular salted Secure Hash Algorithm (SHA-512) Cryptographic Hash Algorithm to hash personal information, which include account information, and passwords. Advanced Encryption Standard (AES) approach was used for encryption and decryption, One Time Password (OTP) also turned into used to beef up user authentication. The design was carried out using Hypertext Preprocessor (PHP), JavaScript, CSS and MySQL database. Cain and Abel that is a password recovery tool that allows smooth recovery of various passwords by sniffing the network, cracking encrypted password using dictionary, brute-force and cryptanalysis attacks, revealing password bins, uncovering cached passwords and analyzing routing protocols was used to envision the validity and dependability of the model and also to obtain result. Results obtained suggests that the model is viable as data encrypted and hashed could not be decrypted by an attacker compared to other existing models.

Keywords: mobile banking; security; cryptography; encryption; decryption.

---

* Corresponding author.

1. Introduction

Technology has reduced the world to a global village and nearly the entirety are been accomplished by means of technology. The development that has taken place so far in information technology (IT) is transforming into a critical factor in the future advancement industries round the world. The traditional method of banking is logically making ready for contemporary method of banking within the twenty first century. Conventional methods of banking has been in existence for a long time now and it is the greatest commonplace method of donning out banking transactions in particular areas –countries, both developed and developing [1]. Nowadays, marketplace center orientation has moved to consumer orientation. Advances in IT essentially and the developing utilization of the Net for business transactions have found significant outcomes at the banking enterprise. With adequate know-how of the noteworthiness of synchronous utilization of different channels of banking, premium is currently typically centered around mobile banking (m-banking), particularly as to keeping relationship with customers [2]. The term m-banking intends to deal with managing an account transactions from mobile devices, for example, iPhones, notebooks or tablets (e.g. iPad). You may get to your e-banking facility from browsers; novel applications empowering you to see your account balance, send remittances, set up status orders and perform distinctive capacities that are accessible from your standard e-banking facility. In Nigeria, banking industry and citizens all incur unnecessary overheads in the utilization of physical cash. Mobile and wireless technology are being used in various areas, for example, voyaging, tutoring, stock purchasing and selling, military, package delivery, disaster recuperation, banking, clinical emergency care, and numerous others [3]; but emphasis in this work will be placed on m-banking. The increase of m-commerce takes after the undeniably well-known proprietorship and utilization of mobile personal, programmable communication devices, together with mobile phones and Personal Digital Assistants (PDAs). These devices are intense for approving and dealing with payment and banking transactions, offering security and solace favors in contrast with on-line payment through personal computer frameworks (PCs). Figure 1 showing the relationship of mobile banking with other electronic transactions. With identity theft on the upward push, m-banking system need to consider information wellbeing important. There are more than one ways that banks can verify customers—that is, guarantee they are who they are saying they are. Those methods range from Usernames and Passwords, PIN (Personal Identification Number), Identifiable Image, USB Token, One Time Password (OTP), Graphical Passwords, Biometrics and so forth. With cryptographic algorithms utilized as a part of m-banking being broken, data is absolutely vulnerable when intercepted. Most cases, some of regions ordinarily vulnerable for attacks are at the customer end, in the communication channels, and at the server side [4]. These vulnerabilities can be outlined as the shortage of end-to-end security for data being transmitted, vulnerabilities in the authentication systems, and vulnerabilities in the application server security administration rules. Authentication issues incorporate the PIN characters now not being covered while typed on the mobile phone making it possible for someone to eavesdrop over one's shoulder; and the PIN is most effective four digits long constituted with numbers handiest, consequently becoming prone for a brute force attack. Confidentiality is likewise missing in light of the fact that less encryption is done to the data transmitted between the customer and server. Besides, the security guidelines inside the software servers define a couple of vulnerabilities that can be exploited. In this work, we have a trendy Salted SHA-512 Cryptographic Hash Algorithm to hash private information along with account information, passwords and so on, with a specific end goal to hold their integrity

and validity. An Advanced Encryption Standard (AES) technique turned out to be broadly used for encryption and decryption so as to ensure information are transported as secure and protected as could be expected under the circumstances. These will help in gaining confidentiality, non-repudiation, security and different necessities for a secured m-banking system. One Time Password (OTP) transformed into used to further bolster consumer authentication. AES is the cutting-edge information security standard adopted in most public and private sector for secure data communication and information storage functions [5]. The AES algorithm is symmetric key type institutionalized by the National Institute of Science and Technology (NIST). AES is a non-Feistel cipher that encrypts and decrypts a data block of 128 bits and it utilizes 10, 12, or 14 rounds. The key size, which may be 128, 192, or 256, 512 bits depends at the range of rounds [5]. Finally, banking specifically in developing nations is characterized by lengthy queues, long distance travels and time wastes that adversely affect business activities and in the long run monetary improvement. Strong security for an m-banking system will help assist in gaining confidence and trust of the customers and in this manner increase its adoption.

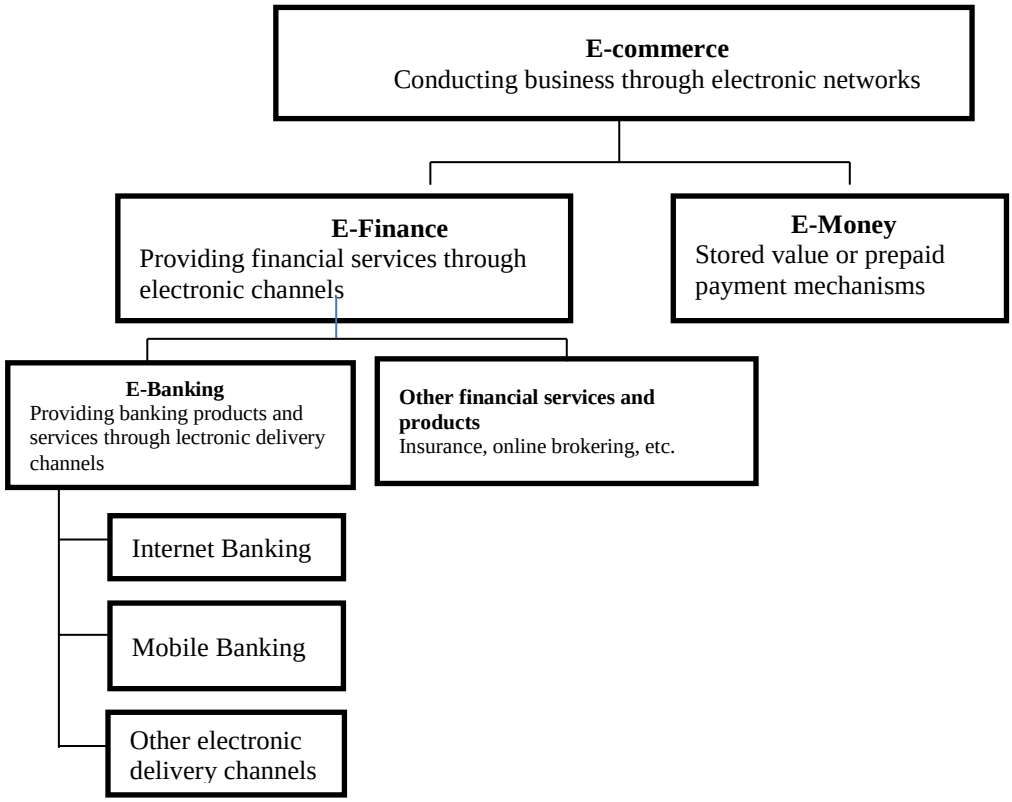


Figure 1: Showing the relationship of M-banking with other electronic transactions. (Source: [6]).

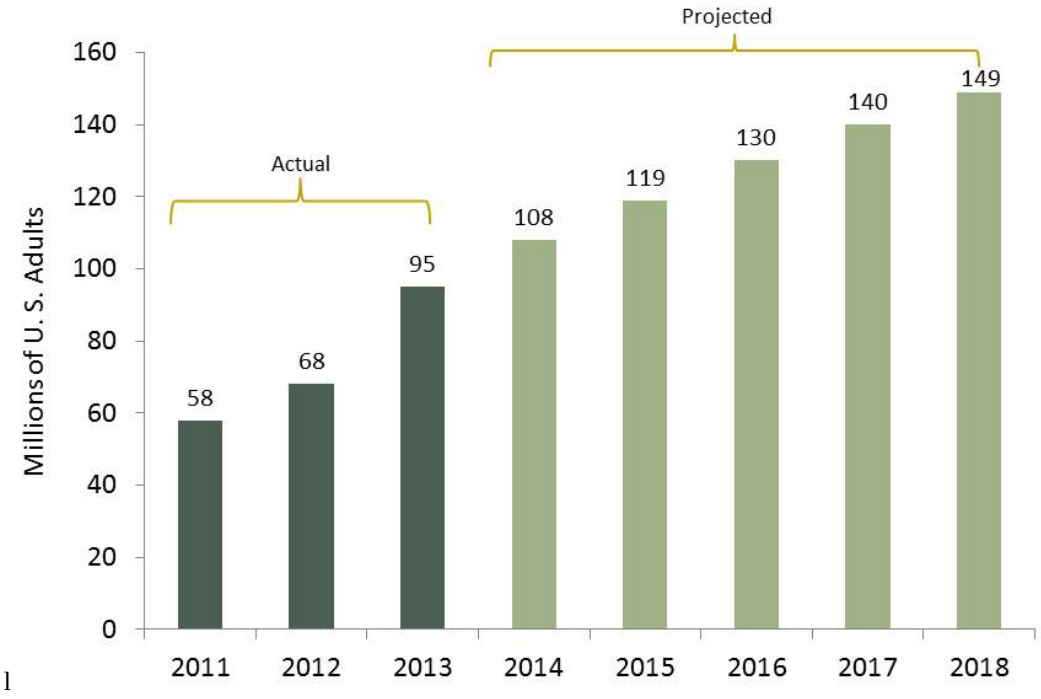
2. Overview of Mobile Banking

Nowadays, the banking industry has been experiencing radical change by means of information technology (IT) system and that is surfacing in all parts of the baking areas. IT is utilized by banks to reduce turn-around time and enhance business in general. The advent of mobile technology and its devices have introduced effectiveness in the way in which commercial and commercial enterprise activities are been achieved [7]. Among this

technological advancement is the coming of mobile telephony, which serves as a platform for jump starting out innovative mobile smartphone applications and services. Utilizing mobile technology for industrial for industrial cause has brought about the idea of m-commerce. M-banking is an application of m-commerce which enables customers to bank at any convenient time and place. There has been evidence of increment in the wide variety of people subscribing for mobile smartphone in developed and developing nations. Presently, the fastest growing global marketplace is the mobile industry.

2.1 Mobile banking market

The introduction of m-banking to the banking sector has added efficiency within the way banking business and business exercises are being accomplished [7]. In accordance with [8], year 2013 saw a significant inundation of customers rushing to m-banking, with 74,000 new people joining m-banking on daily basis. In [8]'s report as referred to in [9], m-banking, tablet and smartphone forecast 2013-2018 as shown in figure 2, smart device adoption drives m-banking boom, which outlines a 5-yr forecast of m-banking and mobile smartphone and tablet adoption calculating for key drivers and potential roadblocks. [9]'s report on survey completed in the US in 2014, it was discovered that among m-bankers, 17%-18% utilize their phones to check balances and statement of account more than 20 times each month. He additionally included that the rate of generation Y (18-34) m-bankers that check their balances and transactions more than 20 occasions a month is twice that of Toddler Boomers (48-68). As a result, it became concluded that financial institutions (FIs) can drive the prominence of m-banking further by not continually requiring logins to view transactions like checking of balances and reviewing recent transactions, likewise that consumers must be discouraged from the use of features like mobile P2P or bank charge pay. Lots of researches ought to be done in other to ease the use of m-banking [9].



l

Figure 2: Mobile banking adoption and related financial services in US 2011-2018. (Source: [9]).

2.2 Consumer behaviour towards m-banking

Customer behaviour is the demonstrations of decision-making which directly include the getting and the utilization of satisfying products and services, which consolidates the decision-making procedure which precedes and determines these acts [10,11]. A customer is a man or business enterprise that uses economic services or commodities. He/she is the person who can pay to expend products and enterprises created. In that capacity, he/she plays an indispensable position in the financial system of a nation. Without consumer request, manufacturers might lack one of the key motivation of produce: to sell to consumers [12]. Personal and enterprise (organizational) consumers are two types of consumers [13]. Individual consumers are those people who buy items and services for their own intake while businesses are the individuals who purchase equipment, products, services, and so on, just to facilitate their business. Individual acceptance of recent innovation or technology has been found to be one of the numerous predetermining factors that have an impact on consumer mindset towards m-banking [11]. Masses of on-line bank customers need to consider the issue of information protection in connection to adoption of e-banking; this and numerous others have been observed to be obstacles confronting the adoption of on-line bank by customers.

3. Related Works

Numerous researchers have worked on e-banking and its related areas with a specific goal to provide higher models to accomplishing security, improving integrity of data and appraisal of various components which affect the use of e-banking. The following researches are considered as follows:

Reference [14]'s work was on modelling, design and analysis of secure m-payment systems. He was motivated by means of the lack of enough security in the present m-payments systems, particularly because of unsuitable protocol design and deployment of lightweight cryptographic operations which led to the lack of crucial transaction security properties. Having examined the issues of existing m-payment system, the research developed a payment framework which is suitable for wireless environments that increases transaction performance whilst making use of it to m-payment protocol. In spite this, the proposed accountability logic can only analyse m-payment protocols and not typically e-commerce protocols.

In [15], a SMSSec: an end-to-end protocol for secure SMS was developed to attend to confidentiality and integrity of message content in SMS. The work proposed a protocol referred to as SMSec that was totally based on public key cryptography that can be used to secure SMS communication send by Java's wireless messaging API. Be that as it may be, the work did not consider other mobile services, for example, multimedia messaging service and HTTP connections.

Reference [16] worked on securing m-payment systems: using personal identification number (PIN) method. However, in light of the need for sufficient security for online financial transactions, the system was designed to focus on the security issues in m-payment for m-commerce with emphasis on personal identification number (PIN). The work proposed a way and framework for securing a payment transaction model, which comprises of Customer (C), Merchant (M), Acquirer (A), Issuer (I), Payment Gateway (PG). 3DES encryption algorithm becomes proposed to take care of encryption and decryption of data. At the end, they were able to provide an

improved model for securing m-payment systems; but because same key was used for encryption and decryption of data, the two parties have to work based on trust and if the trust is betrayed, the safety of the system may be compromised.

Reference [17], designed and implemented an m-payment scheme based on WPKI and WAP technology. [17] built a J2ME m-payment scheme based totally on WPKI (Wireless Public Key Infrastructure) that performs mutual authentication on constrained memory space like mobile phones, PDA, and many others. He analysed identification technology within the presently existing m-payment system and put forward a J2ME m-payment system primarily based on WPKI performing mutual authentication. The work enhanced m-payment, between m-payment user and bank gateway, but, the system was built only for Java enabled systems.

Reference [18], worked on analysis of e-commerce and m-commerce: advantages, limitations and security issues. Having reviewed present literatures, he was able to present an evaluation of e-commerce and m-commerce; stated the advantages, obstacles and security issues but he did not present suggestions on how to improve on the limitations and security issues identified within the research.

4. The Proposed System Analysis and Design Model

4.1 System design

The design of the proposed system stresses functions rather than physical implementation –that is what things need to be done or considered in developing the secure payment system. In this paper, we describe the components of the system model in detail i.e. hashing using Salted SHA 512, authentication using OTPs, encryption and decryption using AES.

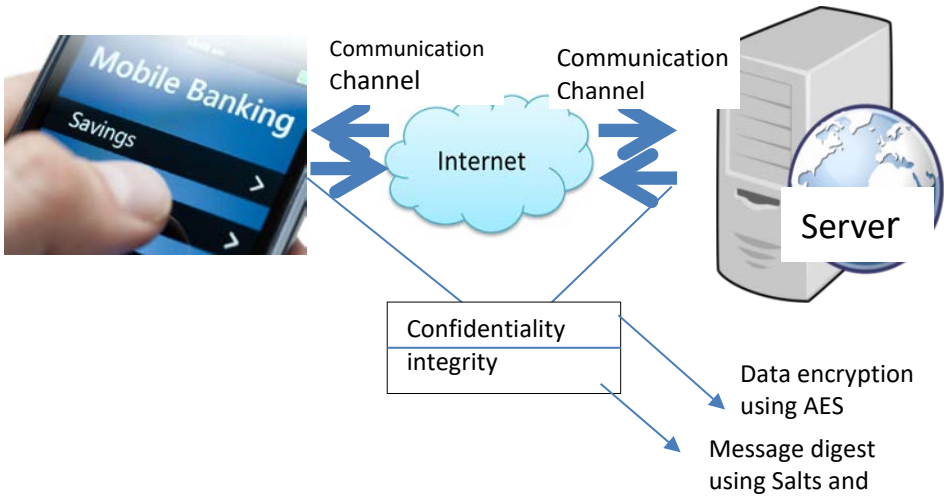


Figure 3: Architecture of the proposed system (Adapted from [4])

The proposed model tried to address the problems of [4]. The draw-back in the choice of hashing algorithm used. It is hereby discussed

1. SHA-1 is appeared as more secure than MD5, in which collisions had been located in 2004 year by some of those who reported the latest discovery. In the same manner, collisions had been located in SHA-0 by a French group. The US National Institute of Standard and Technology (NIST) has since for long endorsed that government phase out SHA-1 in favour of SHA-256 and SHA-512. Later, in 2010, SHA-1 was completely driven away by NIST to give way for more secure hashing algorithms in SHA-2 class consisting of SHA-256, SHA-512 [19].
2. We have used a Wireless Application Protocol (WAP) based solution in our model to address the problems raised in present systems. The application is divided into client module developed using HTML and CSS and the server developed using MySql, Personal Home Page (PHP) serves as the server side scripting languages. As shown in figure 3, the client software is capable of performing basic m-banking operations which consist of funds transfer, viewing of statement of account and other enquiry services. The server application is able to fetching requests from the customer and storing his/her information for next usage. System architecture is a generic discipline to address objects (existing or to be created) called "systems", in a manner that helps reasoning about the structural properties of these objects. It is a response to the conceptual and practical problems of the description and the design of complex systems.
3. Based totally on the vulnerabilities identified in the literature reviewed and [4], we developed a model with greater security controls which deal with the subsequent:-

    a. Data confidentiality: data confidentiality is whether the data stored on a system is blanketed towards unintended or unauthorized access. In other to protect our data, message encryption can be used to make sure cease-to-cease security and ensure that data can best be accessed via, authorized parties [4].
    b. Data integrity: data integrity is the reverse of data corruption (a form of data loss). Data integrity is ensured with the aid of the use of message digests which are obtained by hashing message contents being transmitted across the network. The message digest is attached within the sent message. At the receiving end, another digest is generated from the acquired contents and compared with the attached message digest. If the two digests do not match, the receiver will know that the message integrity has been compromised [4].
    c. Data authentication: on communication exchange channel, data authentication is supposed to confirm customers' identities through preventing unauthorized people from using the system resources by claiming to be persons they are not. It nonetheless relies on three universally recognized authentication factors: what you know (e.g. passwords), what you have (e.g. ATM card, tokens or mobile device), and what you are (e.g. biometrics). Current work has been done in trying alternative factors such as a fourth factors, e.g. somebody you know, which is primarily based on the notion of vouching [20,21,22, 23]. Different measures sometimes called knowledge-based authentication (or "challenge-response") regularly require a user to answer additional questions.

5. The Proposed System Model

The System model is represented with the schematic representation as we have it in figure 3 above. In this section, we shall be explaining the system components one after the other.

5.1 Cryptography

Here, the original form of a message is usually known as plaintext, and the encrypted form is called ciphertext. The set of all the plaintext messages is denoted by Mp; similarly, the set of all the ciphertext is denoted by Mc and f is a mapping from the variables in Mp into the set Mc. P and C represent plaintext and ciphertext respectively. Both of them are transited into binary data and they are represented as follows:

5.2 Cryptography mathematical model

$$C = f(P) \quad (1)$$

In the reverse process, the decryption function f^{-1}operates on C to obtain plaintext

$$P = f^{-1}(C) \quad (2)$$

where $P \in Mp$, $C \in$ Mc; and f is viewed as the encryption algorithm (function) and f^{-1} denotes e decryption algorithm. Since the encryption and decryption are inverse functions of each other, the following formula must be true:

$$P = f^{-1}(f(P)) \quad (3)$$

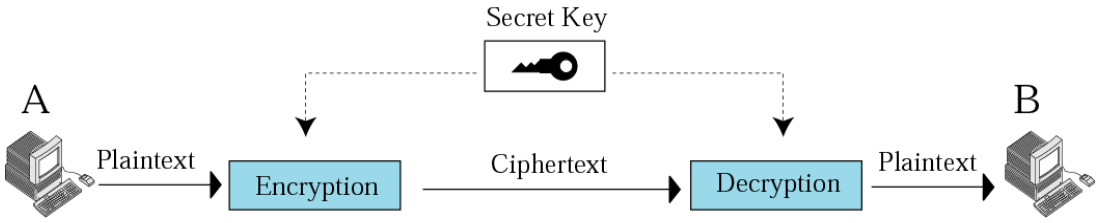


Figure 4: Encryption model (Source: [24]).

When using this form of encryption, it is essential that the sender and receiver have a way to exchange secret keys in a secure manner. As shown in figure 4, encryption scheme has five major parts:

1. Plaintext – it is far the unique text message from “A” to which an algorithm is implemented.
2. Encryption algorithm– mathematical operations to conduct substitutions and transformations to “A”s plaintext will be implemented.
3. Secret key - the key dictates the encrypted final results, and made available to the receiver “B” by the sender “A”.
4. Cipher textual content - that is the encrypted or scrambled message produced by way of applying the algorithm to “A”s plaintext message via the usage of the secret key.
5. Decryption Algorithm– it is far the encryption algorithm in reverse. It uses the ciphertext, and the secret key to derive the plaintext message for “B”.

5.3 Advanced encryption standard (AES)

Here, we give detail explanations of what transcends in the model above. Each of the process involved and how they affect the Encryption and Decryption process. AES is regarded as the most secure symmetric algorithm in the world. It is an iterated block cipher with a fixed block length of 128 and a variable key length. The distinctive transformations operate at the intermediate results, called *state*. The *state* is a rectangular array of bytes and since the block size is 128 bits that is 16 bytes, the rectangular array is of dimensions 4x4. The number of rounds depends on the chosen key length [25], reported on Rijndael model with variable block size. It became stated that the row length is fixed to 4 and the number of columns vary. The *state* consists of (cipher key is in addition pictured as a rectangular array with 4 rows) 4 rows of bytes, each containing *Nb* bytes, in which *Nb* is the block length divided by 32 [25].

Algorithm 1: AES Algorithm (Source: adopted from [26])

```
 begin
 byte state[4,Nb]
state = in
AddRoundKey(state, w[0, Nb-1])
for round = 1 step 1 to Nr--1
 SubBytes(state)
 ShiftRows(state)
 MixColumns(state)
 AddRoundKey(state, w[round*Nb, (round+1)*Nb-1])
 end for
 SubBytes(state)
 ShiftRows(state)
 AddRoundKey(state, w[Nr*Nb, (Nr+1)*Nb-1])
out = state
 end
```

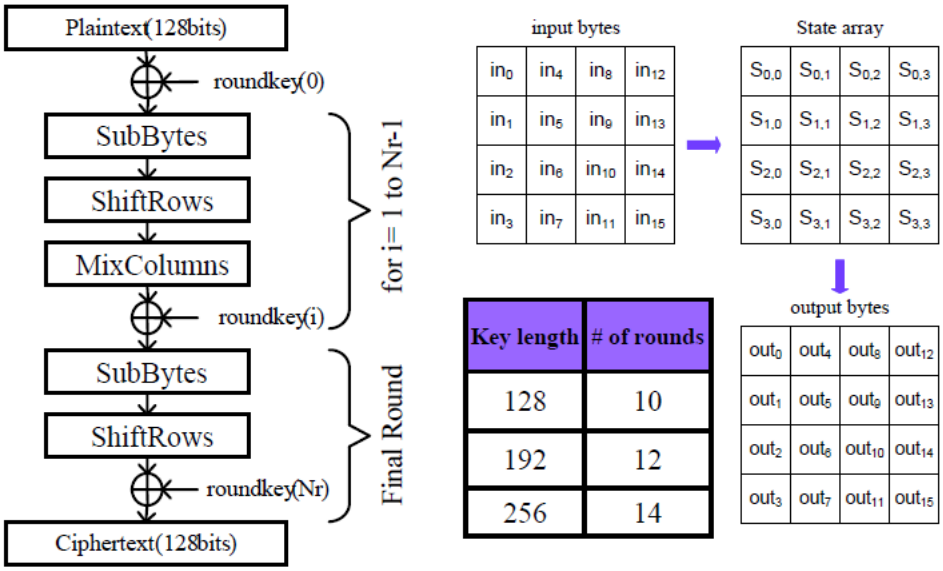


Figure 5: Showing the operations for encryption in AES Algorithm (Source: [27])

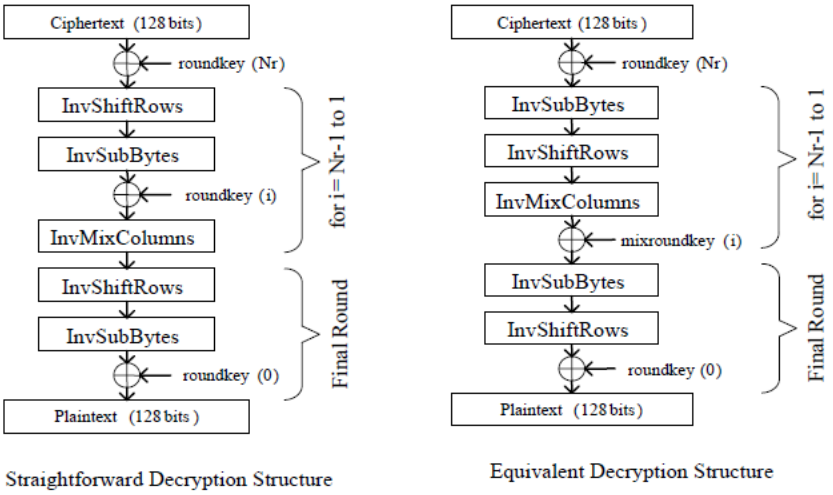


Figure 6: Showing the operations for decryption in AES Algorithm (Source: [27])

5.4 Algorithm parameters, symbols, and functions

The following algorithm parameters, symbols, and functions are used throughout this standard [27], see figures 5 and 6:

AddRoundKey() Transformation in the Cipher and Inverse Cipher wherein a Round Key is added to the *State* using an XOR operation. The length of a Round Key equals the size of the *State*, that is, for *Nb* = 4 (number of columns), the Round Key length equals 128 bits/16 bytes and derived from the Rijndael key schedule,

ShiftRows() Transformation in the Cipher that processes the *State* by cyclically shifting the last three rows of

the State by using one-of-a-kind offsets.

SubBytes() Transformation within the Cipher that processes the *State* using a nonlinear byte substitution table (S-box) that operates on each of the *State* bytes independently.

$$S'_{i,j}=M\times S^{-1}_{i,j}+b \qquad 4$$

MixColumns() Transformation inside the Cipher that takes all of the columns of the *State* and mixes their data (independently of one another) to generate new columns.

Nb Number of columns (32-bit words) comprising the *State*. For this standard, ***Nb*** = 4.

Nk Number of 32-bit words comprising the Cipher Key. For this standard, ***Nk*** = 4, 6, or 8.

Nr Number of rounds, which is a function of ***Nk*** and ***Nb*** (that is fixed). For this standard, ***Nr*** = 10, 12, or 14.

InvMixColumns()Transformation within the Inverse Cipher this is the inverse of MixColumns().

InvMixColumns (State XOR roundkey) = InvMixColumns (State) XOR InvMixColumns (roundkey)

InvShiftRows() Transformation inside the Inverse Cipher that is the inverse of ShiftRows().

$$S'_{i,j}=(M^{-1}\times(S_{i,j}+b)) \qquad 5$$

InvSubBytes() Transformation inside the Inverse Cipher that is the inverse of SubBytes()

Salient features:

1. The cipher key extended into a bigger key, which is later used for the actual operations
2. The round key is introduced to the *state* before beginning the with loop
3. For the duration of each round, any other a part of the expanded key is used for the operations
4. The expanded key shall usually be derived from the Cipher Key and in no way be distinctive at once

6. System Implementation

This is the implementation of the proposed model and can be divided into three sections as follows:

6.1 Interface design

The Interface design allows the user to have easy access to the system without bothering much about codes or memorization of some keywords to communicate with the system. It helps in retrieving and sending of

information between the user and computer. This research has basically eight (8) interfaces which include: Signup page 1 and 2, Login/Sign in page, View profile, Balance enquiry, Transfer funds, Transfer authentication, Transaction history.

6.2 Registration interface/Signup page (new user)

Figures 7(a) and (b) show the registration interface of the System. Included are the username, password, phone security question, answer to security question, account name, account number, and account type. This completes the registration of a new user.

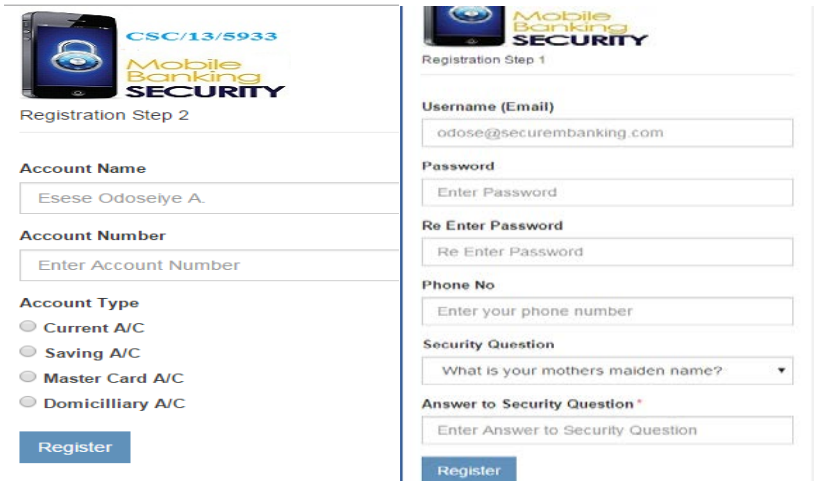


Figure 7: (a) Signup page/ Registration (b)

6.3 Sign in/Login page (Existing user)

Figures 8 shows the Log-in interface of the System. This enables the user to gain access to the system by inputting their username and password

Figure 8: Shows the Log-in interface of the System.

6.4 Encryption code for the user information

Figures 9(a) shows the encryption code for the user information while figure 19(b) shows the login page code. The hash of the password inputted by the user is compared with the hashed value in the database. This determines if user is authentic or not

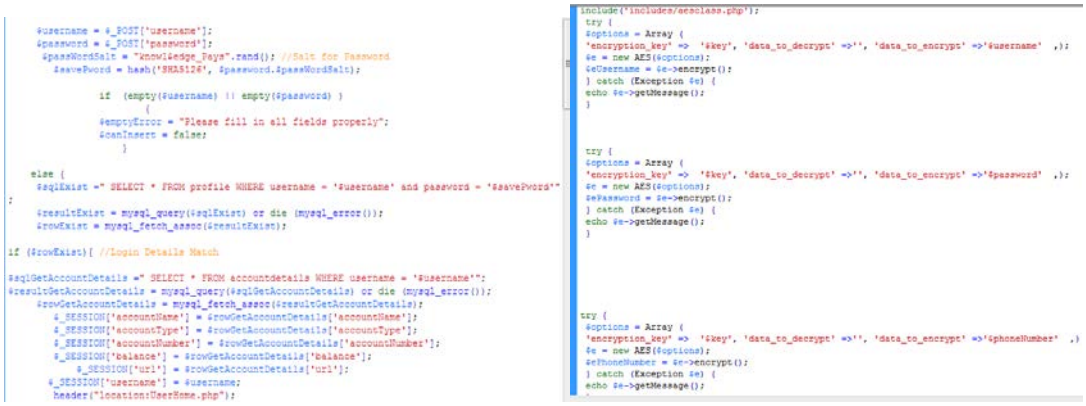


Figure 9: (a) Shows user encryption code (b) Shows the login page code.

6.5 Home page/Transfer funds

Figure 10(a) shows the Home page. This serves as a navigation menu for the user. It shows the basic operations in the m-banking system and users can perform these operations by clicking on any of them. Figure 10(b) is the interface that allows an authenticated user to transfer funds from his/her account to another. For the transfer, the user inputs the account number and amount he/she wish to transfer.

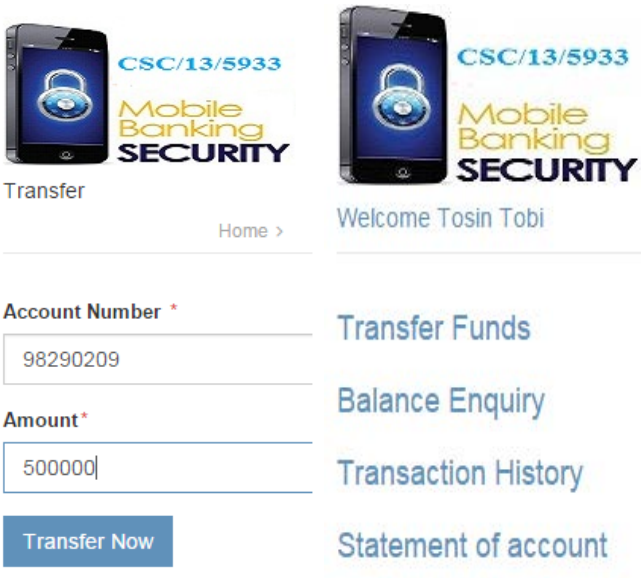


Figure 10: (a) Showing the Home Page. (b) Showing the funds transfer page.

After inputting relevant details in the funds transfer page, an enhanced token is sent in the form of OTP to the

user phone via SMS. This gives the correct user a One Time Password which will be required for authenticating this transfer see figure 11 (a). At the delivery of the SMS, the user receives the message, which includes his OTP which will be used for authenticating the transaction see also figure 11 (b).

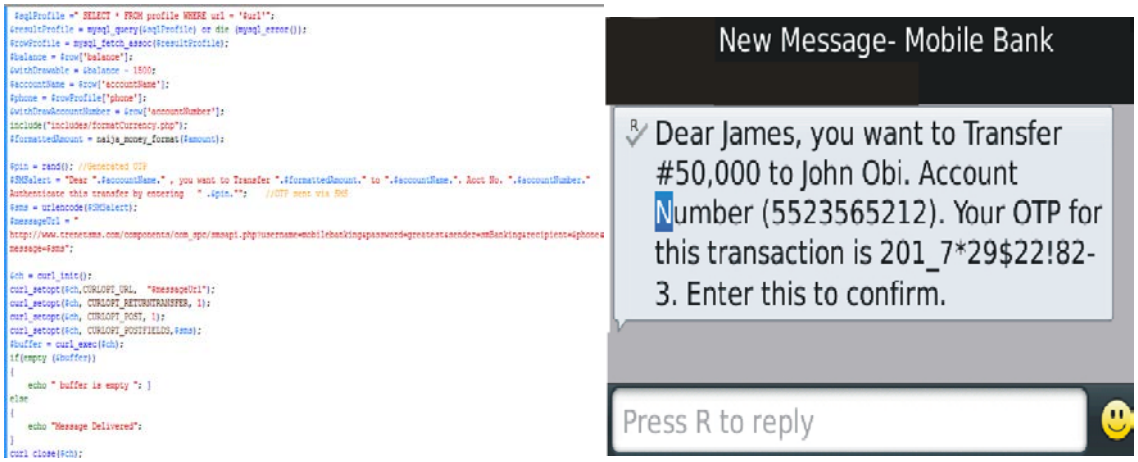


Figure 11: (a) Sending OTP code to user phone (b) Screen shot of SMS received by user which includes the OTP and details of the transfer.

6.6 Transfer authentication

As shown in figure 12(a), the interface allows the user who has initiated a transfer to input the answer to security question; and OTP sends to his phone. This allows the prohibition of a non-genuine user for carrying out transfers on the behalf of a genuine user without approval. When the OTP and answer to security question are verified to be correct, the transfer is authenticated and user gets a notification to this effect. The parties involved are credited and debited respectively see figure 12b.

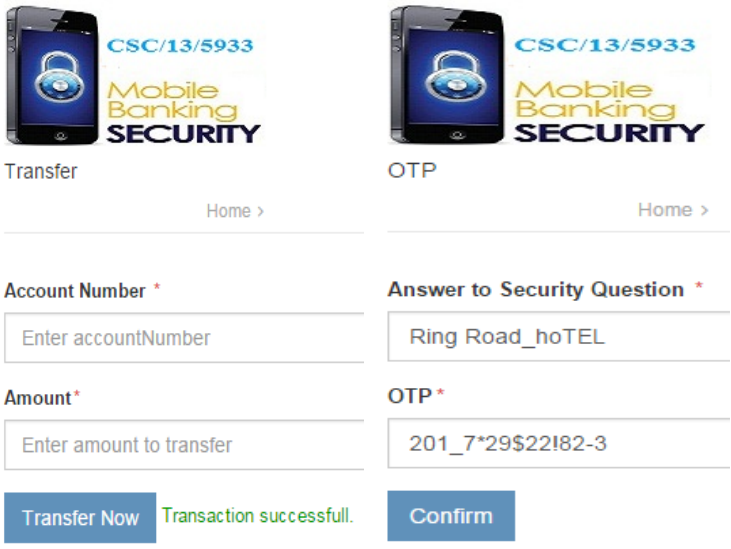


Figure 12: (a) Transfer Authentication Page (b) Transaction success notification

However, if the OTP or answer to security question inputted is not correct (figure 13a), the transfer is prohibited and user is notified to have supplied invalid details. As in figure 13b, if the user does not have sufficient funds to make transfer, the user is notified also and transfer prohibited.

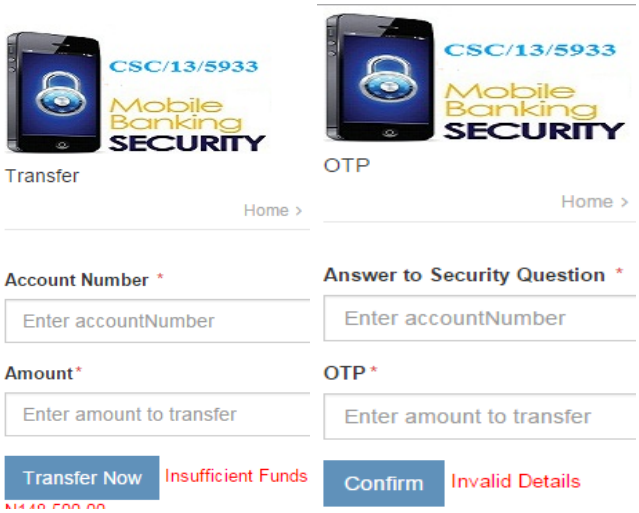


Figure 13: (a) Invalid details notification (b) Insufficient Funds notification

6.7 Enquiry

This interface (figure 14a) allows viewing of account details and user information. These information are in cypher format and a user will need to enter his/her secret key to be able to decrypt this information (see figure 14b).

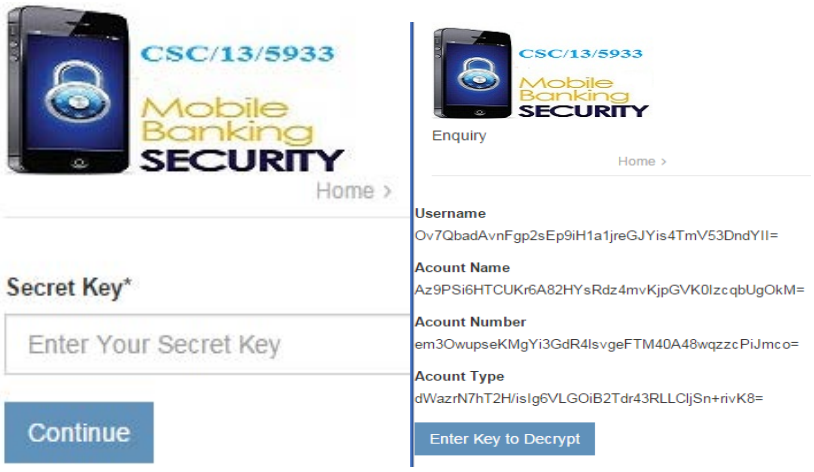


Figure 14: (a) Showing cyphered Enquiry. (b) User enters decryption key

6.8 Decryption/ Decrypted enquiry and integrity status/ Statement of account

After inputting key, the cypher message is decrypted and a hash is computed for all the values and compared with the existing hash value in the database. This helps to know the integrity status of the information (see

figures 15a). This interface allows a user to view a history of all transactions he/she has performed with the system (see figure 15b).

Figure 15: (a) Showing the Decrypted Enquiry and Integrity Status. (b) Showing the Transaction history page

7. Results and Discussion

7.1 Cain and Abel

Cain and Abel is a password recuperation device. It permits easy recuperation of various forms of passwords by means of sniffing the network, cracking encrypted password using dictionary, brute-force and cryptanalysis attacks, recording VoIP conversations, decoding scrambled passwords, recording wireless network keys, revealing password boxes, uncovering cached passwords and analysing routing protocols and for several particular authentication, password/hash calculators. Users' information stored inside the database as Salted. SHA512 hash functions had been run on Cain and Abel to verify the possibility of been cracked. Figures 18 (a), (b) and (c) below show the outcomes of the check.

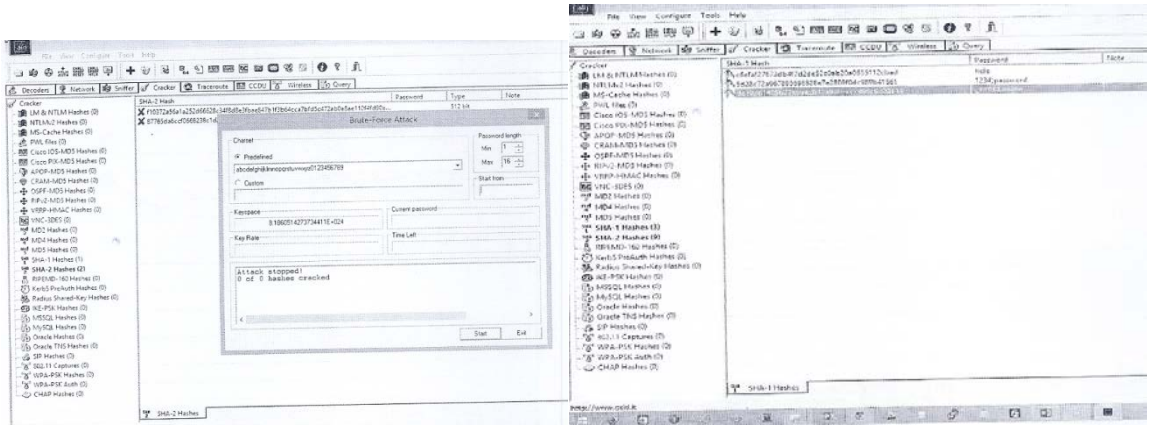


Figure 18: (a) Choice of attack been selected in Cain and Abel. This allows the hacker to select the choice of attack. either brute force or dictionary) (b) Attack successful on SHA 1. (Passwords retrieved successfully). On selecting attack choice, passwords hashed with SHA 1 are seen to be revealed by the Cain and Abel hacking tool.

(c) Attack Successful on SHA 256 but not successful on SHA 512. The password column on Cain and Abel reveals the plain text of data hashed with SHA 1 but for data hashed with SHA 512, the password column is blank (Attack on SHA 512 unsuccessful)

7.2 Security analysis of the proposed model

The primary attention of our design goals for the model was to conform to the standards of secure service. These are user authenticity, confidentiality of data, non-repudiation, data integrity, and availability of service. We give a brief description below of how these services are addressed in our model.

User authentication

The user is authenticated to the system using a pre-selected password, auto-generated random token which a user must supply while performing any transaction on the system. Hashing these authentication mediums using SHA-512 facilitates save brute-pressure attack and different attacks. This guarantees that only the authorized user can perform a transaction

Data confidentiality

Symmetric key ciphers are used to encrypt message contents so as to ensure data confidentiality. Since the keys used are known by the customer and bank only, the communications between them will remain exclusively confidential as long as the keys remain a secret.

Non-repudiation

The key used for encryption/decryption is uniquely associated with most effective one subscriber. Since only this key can encrypt messages that will be successfully decrypted by the server, neither of the parties can deny its involvement in any transaction. Only the customer and bank ought to have information of the key; all successful transactions, therefore, must have originated from a consumer with a correct key. As a consequence, the encryption can be used to hold a customer accountable for transactions done on his/her account.

Integrity

Message digests are used to ensure message integrity where hashes of message contents are calculated at both

ends and then compared. If the digest calculated by sender differs from that generated with the receiver; the recipient will detect a compromise within the message integrity.

Service availability

The system's availability will in large part be prompted via the network operator's availability. It will subsequently be down if the operator's network is down. The application is capable of multi-processing as much transactions as the server hardware can manage. Again, the considerable availability of mobile telephones makes the service increasingly to be had.

8. Conclusion

The Net has grown exponentially and it enhances the interaction between two businesses - individuals and businesses. Due to the growth of the Internet, e-commerce has emerged and presented extraordinary market capability for nowadays' businesses. One industry that benefits from this new communication channel is the banking industry. Mobile e-banking is providing customers with an extensive variety of services, customers are able to interact with their banking account in addition to make financial transactions from virtually anywhere without time restrictions with the use of their mobile devices. To further beautify the pleasure that customer derive from mobile e-banking, a more suitable system for overcoming data security threats worries in mobile e-banking transactions had been developed. The system includes greater security controls to be used in securing transactions. The necessities for the system have been identified; it was designed and implemented.

9. Recommendations

Although the techniques used for achieving this security are presently immune to current data security threats and attacks, it should however be noted that hackers and crackers are not always at rest and a "today-secure" system cannot be said to be forever secure. This is because several attacks could arrive in future which the currently applied security technology may not be immune to. As a result, it is recommended that review and modification should be made to these techniques overtime in-order to always keep abreast with the requirements of a secure system. Again, the scope of this system covers mobile devices. It is recommended that these techniques could also be deployed to internet banking on Pcs and other e-Banking platforms.

Acknowledgements

We will like to appreciate the Federal University of Technology, Akure through the Department of Computer Science for making the laboratory available for the design and implementation of this work.

References

[1]. P. Luarn and H. H. Lin, "Towards an understanding of the behavioural intention to use mobile banking". Computers in Human Behaviour, 21, 873-891, 2007

[2]. Z. Liao and M. T. Cheung, "Internet-based E-Banking and Consumer Attitudes: An Empirical Study". Information and Management, Vol. 39, pp. 283–295, 2011

[3]. O. K. Boyinbode and R. O. Akinyede, "Mobile Learning: An Application Of Mobile And Wireless Technologies In Nigerian Learning System". IJCSNS International Journal of Computer Science and Network Security, VOL.8 No.11, November 2008

[4]. W. B. Nyamtiga, S. Anael and L. S. Laizer, "Enhanced Security Model For Mobile Banking Systems In Tanzania". International Journal Of Technology Enhancements And Emerging Engineering Research, Vol 1, Issue 4 4 ISSN 2347-428. 2013

[5]. A. Menezes, P. V. Oorschot and S. Vanstone, "Handbook of Applied Cryptography", CRC Press, New York, 2007, p. 81-83.

[6]. H. El-Gohary, "E-Marketing in Developed and Developing Countries: Emerging Practices". Birminghan City University Business School, 2011

[7]. Tiwari, "Handbook of Security", Foundation of Computer Science FCS, New York, USA, 2007

[8]. CA, San Francisco, "Mobile banking adoption and related financial services in US 2011-2018". https://www.javelinstrategy.com/press-release/mobile-device-boom-led-74000-new-mobile-bankers-day-2014

[9]. Javelin Strategy and Research, "Mobile Banking, Smartphone, and Tablet Forecast." https://www.javelinstrategy.com/coverage-area/2015-mobile-banking-smartphone-and-tablet-forecast, 2015

[10]. C. Lamb, J. Hair, and McDaniel. "Marketing". New York: South – Western College Publishing. 2000

[11]. B. F. Adesinasi, "Mobile Banking Adoption and Consumer Behaviour." M.Sc. Thesis Submitted in support of GLOBAL MARKETING. London School of Business and Finance. 2012

[12]. Wikipedia, "Consumer". https://en.wikipedia.org/wiki/Consumer, 2017

[13]. G. Schiffman, and L. Kanuk, "Consumer Behaviour". New Jersey: Prentice Hall, Inc, 2000.

[14]. S. Kungspisdan, "Modelling, Design, and Analysis of Secure Mobile Payment Systems". 5th International Workshop on Information Security Applications (WISA2004) [KLS05].2005

[15]. L. L. Johnny, B. Judith and J. H. P. Eloff, "SMSSec: An end-to-end protocol for secure SMS", Developing Mobile Java Applications. Upper Saddle River, New Jersey: Prentice Hall, 174-179.2008

[16]. R. O. Akinyede, O. S. Adewale and B. K. Alese, "Securing Mobile Payment Systems: Using Personal

Identification Number (PIN) Method." Proceedings of the International Conference on Software Engineering and Intelligent Systems July 5th-9th, Ota, Nigeria. 2010

[17]. J. Liu, "Design and Implementation of Mobile Payment Scheme based on WPKI and WAP Technology". Journal of Convergence Information Technology(JCIT) Volume8, Number15, October 2013.

[18]. M. Niranjanamurthy, "Analysis of E-Commerce and M-Commerce: Advantages, Limitations and Security issues". International Journal of Advanced Research in Computer and Communication Engineering Vol. 2, Issue 6, June 2013

[19]. S. N. Geeta, S. J. Swati and A. D. Aaradhana, "M-Banking Security – a futuristic improved security approach". IJCSI International Journal of Computer Science Issues, Vol. 7, Issue 1, No. 2, January 2010 www.IJCSI.org.

[20]. N. Mallat, M. Rossi and V. Tuunainen, "Mobile Banking Services", Communications of the ACM, 47(8), 42-46. 2004

[21]. J. Brainard, A, Juels, R. L. Rivest, M. Szydlo and M. Yung, "Fourth-Factor Authentication: Somebody You Know", ACM CCS, 2006, 168-78.

[22]. F. Aloul, S. Zahidi, and W. El-Hajj, "Two Factor Authentication Using Mobile Phones." AICCSA 2009. IEEE/ACS International Conference on Computer Systems and Applications. 2009

[23]. R. O., Akinyede, "Modelling a Secure e-Commerce Payment System for Wireless (Mobile) Network in Nigeria." Ph.D Thesis submitted to The Federal University of Tech. Akure, Nigeria. 2012

[24]. S. Parikshit, "Secure hashing algorithm" http://www.secure-hash-algorithm-md5-sha-1.co.uk/ 2009

[25]. Tutorialpoint, "Advanced Encryption Standard. Simply easy learning". All Rights Reserved. http://www.tutorialspoint.com/cryptography/advanced_encryption_standard.htm, 2016

[26]. K. Czesław, K. Mirosław and S. Marian, "Modern Cryptography Primer: Theoretical Foundations and Practical Applications". Springer Science & Business Media. https://books.google.com.ng/books?isbn=3642413862, 2013

[27]. Federal Information Processing Standards –FIPS, "Advanced Encryption Standard (AES)". Federal Information Processing Standards Publications. http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf, 2001