ENHANCING ATM CARD SECURITY USING 2-FACTOR AUTHENTICATION BY HASHING CUSTOMERS DEVICE ATTRIBUTES

Faki Ageebee Silas[5], Ibrahim Yakubu Aliyu, and Babatunde Jacob Peter

ABSTRACT

The proliferation of ATM cards for financial services along with the inevitable rise in identity theft and related card frauds is making card security to be a top priority of financial institutions. For decades, institutions have relied on Personal Identification Number (PIN) and One Time Password (OTP) for authentication and validation of customer's cards. Due to technological advancement, this single-use of digits or alphanumeric characters is becoming obsolete, unsecured and vulnerable. To be ahead of fraudsters, banks must employ reliable authentication models that give the customer a leave to feel secured. This study therefore proposed a 2-factor authentication model that secured customers authentication. The model combines the PIN system and customer mobile device data that are already saved in bank database. To enhance the security of customers, the model is able to hashed distinct attributes from customer's registered device in to a cryptographic code. The code is then sent to customers registered device for authentication within shortest possible time. This system makes it impossible for fraudsters to break through since interception of the code renders it unworkable without the registered device.

[5] Author's Address: Faki Ageebee Silas[5], Ibrahim Yakubu Aliyu, and Babatunde Jacob Peter, Department of Computer Science. Bingham University, PMB 005, Karu Nasarawa State-Nigeria faki.silas@binghamuni.edu.ng, talktoibro80@yahoo.com, and tundejacob@binghamuni.edu.ng

"Permission to make digital or hard copies of part or all of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than IJCIR must be honored. Abstracting with credit is permitted. To copy otherwise, to republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee."
© International Journal of Computing and ICT Research 2008.

International Journal of Computing and ICT Research, ISSN 1818-1139 (Print), ISSN 1996-1065 (Online), Vol.11, Issue 2, pp. 53 - 64, December 2017.

Keywords: ATM, cryptographic hash function, fingerprint, OTP, two-factor authentication.

IJCIR Reference Format:

Faki Ageebee Silas[6]' Ibrahim Yakubu Aliyu, and Babatunde Jacob Peter. "Enhancing ATM Card Security Using 2-Factor Authentication by Hashing Customers Device Attributes", Vol. 11, Issue.2 pp 53 - 64. http://www.ijcir.org/volume 11-issue 2/article 4.pdf.

INTRODUCTION

In recent time, the use of technology in financial industrial is on the increase across the globe. This is due to the fast changing technological innovations that permeate the financial market and increase in strong competition. Therefore, efficiency and security of customers that necessitates the use of information technology to speed up transactions becomes mandatory. (Foresight, 2012). This leads to financial organization deploying card processing machines at strategic places like shopping malls, school campuses, places of worships, cinema halls, airport etc. A card processing machine could be an Automatic Teller Machine (ATM), a Point of Sale terminal (POS). The slim operational difference between ATM and POS is that while an ATM is a self-servicing machine which handles cash withdrawer, deposit, balance enquiries, transfer and bills payment, a POS could be a portable machine that handles consumer payment for goods and services.

Recent improvement in technology has actually closed the gap between POS and ATM allowing most of their functionalities to overlap. Though, the most important thing to note here is all of them use card system and both has security challenges in a similar fashion. ATM being a

[6] Author's Address: Faki Ageebee Silas[6]' Ibrahim Yakubu Aliyu, and Babatunde Jacob Peter, Department of Computer Science. Bingham University, PMB 005, Karu Nasarawa State-Nigeria faki.silas@binghamuni.edu.ng, talktoibro80@yahoo.com, and tundejacob@binghamuni.edu.ng

"Permission to make digital or hard copies of part or all of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than IJCIR must be honored. Abstracting with credit is permitted. To copy otherwise, to republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee."
© International Journal of Computing and ICT Research 2008.

International Journal of Computing and ICT Research, ISSN 1818-1139 (Print), ISSN 1996-1065 (Online), Vol.11, Issue 2, pp. 49 - 60, December 2017.

self-servicing machine has more security challenges because of the popular Personal Identification Number PIN authentication system (Richard, 2017). In Africa and Nigeria to be precise, all ATM uses four digits (PIN) for authentication. This leaves the card owner vulnerable due to the one factor authentication and ease of breaking digits PIN system. To improve the protection of card users, this study therefore, modeled card authentication system to include a cryptographic hash function which uses algorithm that get inputs from the distinct variables of customers registered device, (International Mobile Equipment identity (IMEI), serial and mobile number) to compliment the serial four digit PIN authentication.

RELATED WORKS

Automatic Teller Machine (ATM) as is mostly called is known by other names as cash machine, cash dispenser, the hole in the wall has become popular in the world with its role to complement the traditional financial activities that require the physical presence of workers and customers. This fast moving technology create a system that bring unrestricted access to cash and break physical boundaries between financial institutions and customers (Dirk, Youngsho & Peter, 2012). Due to isolated and non-secured locations of most ATM machine, vulnerable to attack either by physical robbery or fraudulent activities by fraudsters to defraud customers of their money is becoming a norm. Therefore, there is a need to urgently improved security for ATM machines and card holders. A customer with an ATM Card can visit any of the ATM machine (especially those on the same network) to be able to withdraw cash, deposit cash, transfer cash, check cash balance, pay bills and top up airtime. Most ATM card uses a combination of Personal Identification Number (PIN) which is formed from a combination of digits (0 to 9) for authentication and security (Rini, Sreedavi & Vidhya, 2017). The digits are combined in four, five or six numbers depending on the country. The target of fraudsters is either communication link of ATM networks, ATM terminal or customers card PIN.

In developing countries like Nigeria, many holders of ATM cards are not literate or lack basic ICT skills to conveniently operate the ATM machine leaving them with no choice than to either send relatives or request for help on the queue (which in most cases from strangers) for transactions thereby exposing their PIN to person(s) who in turn take advantage to defraud them. In recent times, many researchers are exploring the use of biometrics to increase the security of card holders. According to Jaswinder and Jaswinder (2015) model, ATM PIN can be shared with others while a secured security system based on finger print and voice recognition is proposed. The model provides secured ATM security as well as be of benefits to illiterate and blind customers. This model has a 3-step authentication, removes the hidden cost most banks charge on ATM card maintenance but consumes time based on the three steps authentication. Also voice recognition systems are always prone to error due to variation in voice input.

Mohammed (2016) adds a second level of security in addition to PIN by either generating a One-Time Password (OTP) or fingerprint biometric. The OTP is generated in fixed digits using cryptographic hash functions with an option of using finger print biometric if so desired. This model provides another level of card security but incurs additional cost of hardware purchase which is the finger print scanner and also OTP are no guarantee to attacks. Majority of researchers proposed ATM card security enhancement by use of finger print (Frimpong, Kofi & Michael,2016; Padmapriya, & Prakasam, 2013; Awotunde, James & Fatimoh, 2014), these models provide a secured system but incur overhead in database by saving large images of fingerprint and introduction of finger print scanner. Also shouting finger prints are evitable because of the agrarian nature of developing countries customers. In order to prevent identity theft and enhance privacy, Swathy and Rasmi (2015) introduces a user-centric biometric model using BioCapsule. This model securely enables users data fused with biometric system thereby providing a robust authentication. The model is user friendly and therefore does not require user's former training but require the use of robust hardware for biometrics capture..

1.1.Cryptographic Hash Functions

Cryptographic hash function is a function that computes and condenses an arbitrary massage of varying length into a massage of fixed size in length which is called a digest, fingerprint or a hash. Hash, massage authentication code (MAC) and one way functions are basic cryptographic security used in most systems (Heung & Moti, 2010). Major properties that make a hash functions secured is that none of the massages will have same hash value and no corresponding massage can be retrieve from its hash value. There exist a thin line between practical and theory of hash functions. This is because, in practice, cryptographic hash functions are fixed mapping from input bits strings of variable length to a fixed length of an output string while in theory they are defined as keyed mapping (Ozgul, 2012). A hash function can be represented as

$$Hf = \{0,1\}^* - - - \rightarrow \{0,1\}^n \qquad (1)$$

where n is the string length and * the arbitrary length of input.

Basically, a cryptographic hash function is viewed as an instance of a family of functions. For instance,

Let

$$H : \{0,1\}k \times \{0,1\} * \to \{0,1\}n \qquad (2)$$

be a family of functions.

For a particular key $K \in \{0, 1\}k$,

$$HK : \{0,1\} * \to \{0,1\}n \qquad (3)$$

is defined for every m ∈ {0, 1}∗ by HK(m) = H(K,m).

A hash function of this nature with k as a secret key is called a massage authentication code (MAC). Because of the wide range of inputs accepted by hash functions, collision is rare but not completely inevitable. To avoid collision, many authors employed open hashing which is hashing with chaining and closed hashing which could be either linear or quadratic probing. Either of open or closed hashing techniques can resolves collision but on the other hand add overhead to the hash function. There are many flavors of hashing method such as MD-2, MD-4, MD-5, MD-6 and the SHA's which could be SHA-1, SHA-224, SHA-256, SHA-384 and SHA-512 (Smriti & Sandeep, 2015). Each of these flavors have their pro and cons but the fundamental issues lies in the fact that security design in here is the ability to provide changes to algorithms and codes that protect the user transparently.

PROBLEM STATEMENT

The statement of the problem is formulated based on the fact that most card holders make use of repeated digits or frequently used digits like 1234, 1010, 1111, date of births or carelessly keep or expose their cards pins. Also, frequent unsolicited scam emails sent from fraudsters to bank customers with the intent of collecting their bank details especially the PIN and account numbers.

1.2. Sample unsolicited scam email to a customer from a fraudster

Dear Customer
According to our records this month, your registration for our XYZ bank Customer Digest monthly bulletin has been processed and this comes with a monthly charge of ₦16, 550:00.
As your opinion is important to us, we would like you to confirm your registration
https://ibank.xyzbank.com/ ibank3/confirm_customer_ digest_monthly_bulletin/
7c2c01489b275ea11cc991931e4098 6e75621e473c3c7012ee6b2b514176 57692482fd1cd1db3394e0d67d9756
5a449e9e94e4bce0e9b91ef0f16702 6a138480
If you wish to reject the registration request, follow the cancel reference below
https://ibank.xyzbank.com/ ibank3/cancel_customer_digest_ monthly_bulletin_request/
5172b0044fe84408661228b4131d2d 8cd39a8bce71a09622777922f1d764 7d1ecf7ecf6faa966c3cd0480ef447
44d1235fcecedf9753bb7a012f808f 7d9210de?cancel=1
Thank you for choosing XYZ Bank plc

These types of emails are frequently sent by scammers to customers disguising as bank staff. This leads to many customers falling victims of fraudulent acts especially those that are not careful enough to understand the nitty- gritty of social engineering. A customer who unknowingly sends details of ATM card through the link provided by the fraudster which in most cases are temporary or hijack site will only end up getting withdrawer or other transaction notices that cannot be traced. In most cases the target of the scammer is nothing more than the ATM PIN which they use in cloning a new ATM card that is used carrying out nefarious bank transactions. With all this happenings couple with the fact that there is no end in sight of such fraudulent activities, banks have no option but need proactive measures to enable ATM PIN to use 2-factors authentication system using customers registration profile and device details.

The present ATM system work as follows;

Step 1: User enters card in ATM.

Step 2: ATM reads cards information and sends them to the bank server and request for PIN.

Step 3: User Enter PIN,

Step 4. If PIN is correct according to server, User will be allowed further access for transactions.

Else new options are given to enter PIN again or Exit

PROPOSED MODEL

The proposed model uses 2-tier authentication which is based on what a customer have and what is known for. This authentication model is customer friendly and provides customer more security and convenience of use.

Pre-condition for operation

Customer's profile (in customer database) must include among other data phone number, international mobile equipment identity (IMEI) and serial number of phone, mobile phone number.

1.3.Model Description

To avoid a man-in-the-middle attack (MITM), this study proposed a two factor authentication model which involves the use PIN and cryptographic hash function from customer's data. In this model, the PIN is used for profile authentication or confirmation of account holder but cannot provide access to carry out detail transactions. This means that the PIN can be made public since no real bank transaction process can be authorized by it apart from customer profile verification. The cryptographic hash function is created with an algorithm which combine IMEI, serial, mobile phone number and registered named on the phone to create a function that send a simple massage to customer's phone. The answer to the massage is given in few second on a registered customer phone. The flowchart of the model is shown in Figure 1.

On confirmation from the bank server that the answered massage is from the registered customer's phone, access is given to the customer to carry out bank transaction. The model allows three trials of both the PIN and hash code sent to phone. Wrong PIN on fourth trial leads to the Card to be retained in the ATM while fourth hash code from a strange device other than the registered one leads to blocking of account from the customer.

1.4.Add another device

A customer is allowed to add a new device with the permission of the bank staff. Else, a device can be added online with the use of a token and secret question created for online transaction. The new device mobile number registration must be done with customer's name and bank verification carries out before usage is allowed. This is to block intruders from registering their device on a customer's account.

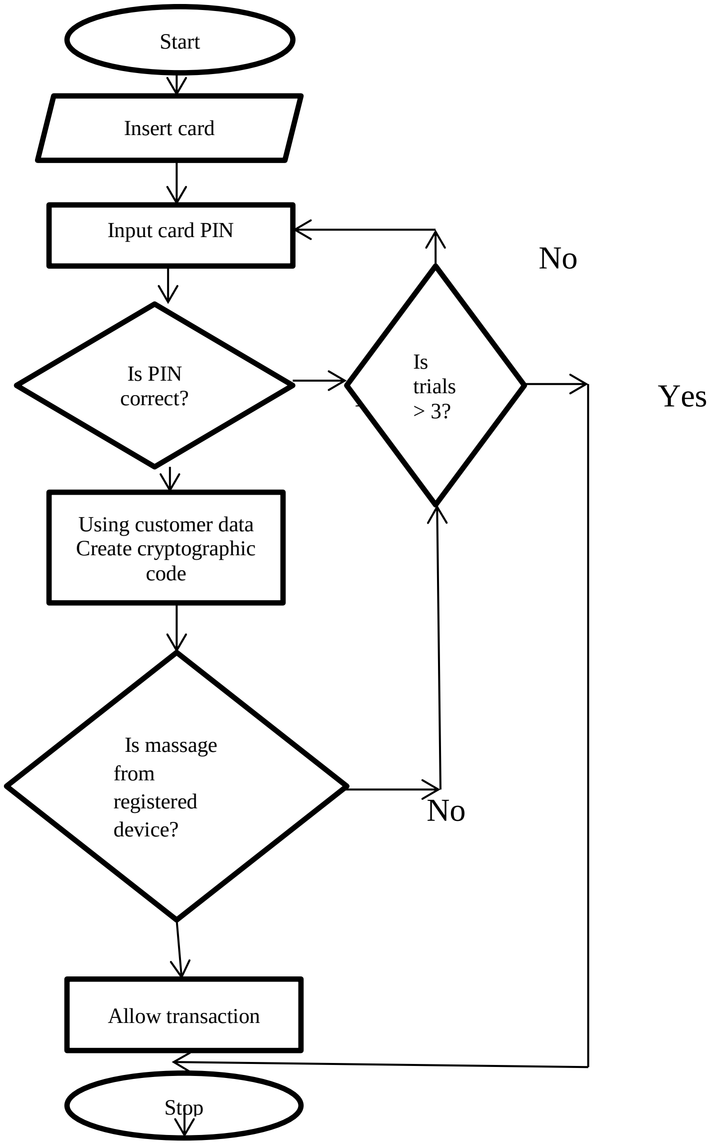

Fig. 1. Flow chart of the proposed 2-factor model using customer registered device

To evaluate the performance of the study’s model, a simulation is carried out. A bank customer database was created with customers profile and registered device attributes stored in. These profile and device attributes were called up by writing codes in C++ language as depicted in the pseudo code that follow.

```
.Step 1: Create str1 customer_name;
                       str2   imei_no_0f_ device;
                      str3  device_ serial_no;
                      str4  mobile_no;
Step 2:  At random, create a substring of length two from each of the variable;
Step 3: check: if str  out of bound, start from index 0;
 Step 4: concat all str to length 8;
Step 5:  eight str code is our digest.
```

From each of the selected string from the customer database, a substring of length two is form. The substrings are further concatenated to form a string of length eight with alphanumeric characters. The eight characters form the cryptographic code or digest which is sent to a registered customer device for authentication.

SIMULATION OF RESULTS

Using Intel core i7-4810MQ, 2.8 GHz, 16GBRAM, 1000GB HDD, window Operating system, with variable string as

```
   Str1_name[]="fakiageebee";

  Str2_imei[]="352419066482441";

  Str3_sno[] ="0193810721902256";

  Str4_mobile[] = "+2348066238988";
```

The first and last ten of the cryptographic codes were as follows:

```
19ia6610     41ki+219     06ia6293     66ee2381     35ia0695

13ef+238     66ia8+93     06ia2319     64ge+295     82ge6656

-----------  ------------ -----------  ------------ -------------

-----------  ------------ -----------  -----------  -------------

19fa9048     90fa2319     90ak4821     19ee2321     44ag6601

41be8+56     24eb2307     13ee6690     52ef+281     35i10693
```

From simulated output, 300 customer’s attributes were hashed with output showing no specific pattern. This make it impossible for a fraudster to trap the code and make meaning out of it. Also since the registered device is with the customer, trapping the code is useless for it won’t work on a different device other than the one the inputs came from. Thus, by this model, security of a card holder is squarely in his hands for it is impossible for the card and a registered device to be in the hand of criminals or fraudsters at same time.

CONCLUSION

In this work, a user friendly, more secure am easily operated model using what a customer is known for and what he has is proposed. The proposed model expunges the craziness for ATM card PIN theft because this only allows operations at a customer profile level. The model allows a transaction to occur only when a registered device received a cryptographic code and responds to it therefore making it impossible for fraudster to penetrate the system. The approach is also secured from attached from intercepting cryptographic code since they will be useless without the very device that creates the code. This model is then, a simple approach that is secured and defeat card attacks.

FURTHER STUDIES

The authors in the nearest future intend to implement this model in one of the small community bank to evaluate its security strength.

REFERENCES

Foresight: The Future of Computer Trading in Financial Markets
Final Project Report, The Government Office for Science, London, (2012)

Richard, m.: Staying One Step Ahead in the ATM Security Challenge, Authoritative Analysis on International Banking, International Banker, Wincor Nixdorf UK/I, (2017

Jaswinder S., Jaswinder K..: Proposed Security System to Embed Fingerprinting and Voice Recognition for ATMs, International Journal of Advanced Research in Computer Science and Software Engineering, vol 5, issue 5. (2015).

Dirk, V., Youngsho, C., Peter, S.: The digital challenge to retail banking, Brain and Conpany Inc, USA, (2012).

Rini, J,. Sreedevi, K., vidhya, M.: Multilevel Authentication for ATM Security, International Journal of Advanced Scientific Technologies Engineering and Management Science, Vol.3, Special Issue.1, April, *(2017).*

Mohammed, H. K.: Securing ATM with OTP and Biometric, International Journal on Recent and Innovation Trends in Computing and Communication, Vol. 3, Issue 4, 2041 - 2044, (2016). DOI: 10.17762/ijritcc2321-8169.160460

Frimpong, T,. Kofi, N,. Michael, A.: Improving Security Levels In Automatic Teller Machines (ATM) Using Multifactor Authentication, International Journal of Science and Engineering Applications
Vol. 5, Issue 3, (2016).

Padmapriya, V,. Prakasam, S.: Improving Security Levels In Automatic Teller Machines (ATM) Using Multifactor Authentication, International Journal of Computer Applications Vol 80, No 16, (2013).

Awotunde, J., James, T., Fatimoh, T.: Fingerprint Authentication System: Toward Enhancing ATM Security, International Journal of Applied Information Systems, Foundation of Computer Science FCS, New York, USA, Vol 7, No.7, (2014).

Entersekt: Securing the Mobile Banking Channel, (2014)

Heung, Y., Moti, Y.: Information Security applications, The 10th International Workshop on

Information Security Applications (WISA 2009), Busan, Korea, August 25–27, (2010),

Ozgul, K.: Design and Analysis of Cryptographic hash Functions, Katholieke Universitiet, Leuven, (2012).

Smriti, G., Sandeep, K.: Performance Analysis of Cryptographic Hash Functions, International Journal of Science and Research, Vol 4, issue 8. (2015).