

A New Model for Enhancing ATM Security in Nigeria Using Second Level Authentication Process

Muhammad-Bello, B.L.

Ganiyu, S. O.

Alhassan, M. E.

Information and Media Technology Department
School of Information and Communications Technology
Federal University of Technology Minna
Nigeria

bilkisu_bello@futminna.edu.ng

shefiu.ganiyu@futminna.edu.ng

m.alhassan@futminna.edu.ng

Abstract— There are certain standards that must be met by banks in order to ensure the safety and security of their banking environments. The security measures been put in place by banks are of huge importance because they often prevent the incidence of fraud on customers and banks alike. However, on certain occasions these security measures could be awkward, thereby causing inconveniences and dissatisfaction to the customers. A recent directive was issued by the Central Bank of Nigeria (CBN) directing all banks to destroy trapped ATM cards by perforation before forwarding the cards to the issuers. This study focuses on the problem of confiscated Automated Teller Machine (ATM) cards in the Nigerian banking industry, with intent to reduce the incidence of trapped ATM debit cards. The second level authentication technique was adopted for the proposed system which was used to authenticate the user to the bank system in an incidence where an incorrect Personal Identification Number (PIN) has been entered trice. The proposed system was built on the existing system and it was able to reduce the number of incidents in which ATM cards were confiscated.

Keywords- *Second Level Authentication, ATM Security, Automated Teller Machine, Trapped ATM cards.*

I. INTRODUCTION

The Automated Teller Machine (ATM) is a computerized mechanical device that is linked to the accounts and records of a banking institution [1]. It is used by banks and financial institutions to enable customers carry out banking transactions such as withdrawal, deposits, balance enquiries, top-up purchases, account to account transfers, mini statements etc. All over the world, banks have continued to increase the number of services available via the ATM terminal to further improve on the convenience of banking through the ATM channel. This has been attributed to the fact that bank customers are not willing to join the long queues or wait for too long in order to be attended to by bank officials [2]. This has also been the trend in Nigeria where the number of ATM card holders has continued to grow due to the increasing e-payment awareness and the policies been put in place by the Central Bank of Nigeria (CBN). In Nigeria, 80-90% of all e-banking transactions are carried out via the ATM channel [3].

In an ironic manner, the activities of fraudsters have also been on the increase in Nigeria. ATM fraud has become a nationwide issue affecting both the banks and customers [4]. Card theft, shoulder surfing, Personal Identification Number (PIN) interception via text messages and emails are some of the common approaches been used by fraudsters. In the context of banking fraud via the ATM, this is only possible if both the card and PIN are in the possession of the attacker or fraudster. This implies that even in an event where a card has been stolen or missing, withdrawal via the ATM is not possible unless the PIN is also stolen or correctly guessed. The ATM confiscates ATM cards after entry of an incorrect PIN three times in order to prevent further guessing which might lead to fraud. Therefore, the confiscation of ATM cards is a security measure that is put in place by the bank to prevent fraud and also ensure the safety and security of the account holder. However, this security measure often inconveniences some bank customers. This is because often times, customers tend to forget their PIN and as such, their ATM card gets confiscated by the ATM. One major factor responsible for this trend is because ATM card users have to face the challenge of choosing a PIN that is easy to remember (usability requirement) but hard to guess (security requirement). The users who are aligned with the security requirement as against the usability requirement are more likely to forget their PIN thus more likely to get their ATM cards confiscated. Another major factor that could be attributed to this problem is the literacy level of some of the ATM users. The threat of ATM frauds in Nigeria can be attributed to the indiscriminate issue of ATM card without regard to the literacy level of the customers. In a study conducted by the National Bureau of Statistics [5], the adult literacy level in Nigeria was estimated to be 57.9% as at 2010. A similar study by UNICEF [6] revealed the total adult literacy rate to be 51.1% as at 2012. Therefore, many bank customers who are illiterates or semi-literates in Nigeria and other developing countries are completely unfamiliar with the ATM concept and are unlikely to memorize and remember a PIN for use on the ATM terminal [2]. This implies that not all cases of the entry of incorrect PIN is due to fraud attempt on the card. There are cases whereby legitimate card owners tend to forget their PIN and end up getting their ATM cards confiscated by the bank ATM machine. A recent study by [2] also suggests

that people who live in today's high tech society constantly have to deal with so many numbers such as computer passcodes, phone lock codes, social security number, credit card number etc. Therefore, they sometimes get confused and have difficulty in remembering such PINs and passwords which could also lead to ATM cards being retained at an ATM. This study therefore aims to apply second level authentication process to improve ATM security and operations by minimizing the incidence of ATM cards getting trapped in the ATM as a result of the entry of incorrect PIN three times.

A lot of past researches have focused on enhancing the security and operations of the ATM. However, little or no work has focused on the operation of the ATM from the perspective of ATM cards being trapped in the ATM.

II. RELATED WORK

Majority of the researches that were conducted in the past focused on enhancing ATM security via biometric means. A few of such works are as follows: A biometric strategy using finger print measure was designed by [2] for enhancing ATM security in Indian E-banking system. In a recent study by [7] proposed using the Iris Recognition and Palm Vein (IRPV) recognition technology to prevent card duplication and crimes via the ATM. The Advanced Encryption Standard (AES) algorithm was adopted in [8] to improve the security level of ATM Banking Systems. Finger print recognition in digital image processing was adopted in [9] for a proposed new business model which would enhance ATM security. In [10] however, the existing security of the ATM system was enhanced by incorporating the fingerprints of users into the bank's database as a means for another authentication process. ATM based fingerprint verification was developed and simulated for ATM operations in order to reduce frauds associated with the use of ATM. A recent study conducted by [11] enhanced the security of the ATM using a combination of fingerprint and GSM technology. The fingerprint recognition technology and PIN verification was embedded into a GSM modem which was connected to a microcontroller to generate 4 digits one-time passcode which is to be sent to a user's mobile number whenever the user tries to enroll the finger print image on the banking system. A similar study in [3] also developed a prototype of an enhanced ATM authentication system using Short Message Service (SMS) verification and also conducted a usability testing of the proposed system. A system which incorporates facial recognition technology into the identity verification process used in ATMs was proposed in [12]. The proposed ATM model developed using facial recognition software was more reliable in providing security. A Novel Hybrid Technology in ATM Security Using Biometrics was proposed in [13]. The proposed algorithm adopted in the study provided two phases of security using both biometric and GSM technology. In addition to the PIN provided, a second level authentication using fingerprint was required. In an event whereby the fingerprint authentication fails, a one-time passcodes is to be sent as an SMS to the pre-registered mobile number which would be used as a second level authentication.

III. EXISTING ATM SYSTEM IN NIGERIA

The rapid development in Information and Communications Technology has transformed the way and manner in which banking operations are carried out. The ATM system has been revolutionary in the banking industry and has been widely accepted worldwide. The ATM system in Nigeria enables bank customers to access several services such as cash withdrawal, cash deposits, money transfer, top-up purchases, utility bills payment, balance enquiries etc. ATM cards in Nigeria are chip-based cards as the Magnetic stripe cards have been phased out few years ago. The ATM system requires chip-based cards and a valid PIN for all valid transactions. The ATM system compares the PIN code entered against a stored list of authorized PIN for the ATM users. If the PIN code entered is correct, the system authenticates the user and grants access to all the services available via the ATM. However, if the user fails to authenticate to the system by entering an incorrect PIN three times, the system blocks the card and the ATM also retains the card at the ATM.

As a rule, ATMs give users three tries to authenticate to the bank system. In an event where the user fails to authenticate to the bank system, the bank card will typically be blocked. In Nigeria however, in addition to the ATM card being blocked or locked, the card also gets confiscated by the bank ATM. If the user were to be a fraudster, confiscating the bank card is the ultimate security measure that would prevent the fraudster from further guessing the correct PIN and subsequently withdrawing from the card owner's account via the ATM. However, if the user happens to be the legitimate card owner who has forgotten his/her PIN, confiscating the card is a problem. This is because in Nigeria, confiscated cards are withheld by banks for at least 24 hours before they are released to card owners that are customers of the bank. Cards belonging to customers of other banks are processed and forwarded to the nearest branch of the customer's bank for onward delivery to the card owner. This process tends to be inconvenient some customers because having to wait for 24 hours or going to the nearest branch of a bank is not the ultimate solution to the problem and customers tend to get frustrated or dissatisfied with this system.

In a recent development, the CBN has directed all banks in Nigeria to henceforth destroy ATM cards trapped in their ATM terminal by perforating them and subsequently forward the cards to the issuers by the next working day [14]. The new policy is to be applied to both the issuing banks' ATM cards and other banks' ATM cards. This directive has actuated a lot of debate and controversy because the burden of re-issuing the ATM card is to be borne solely by the card owner [15]. This seems to be unjust to the customers because cards trapped can sometimes be as a result of a faulty ATM or a legitimate card owner could forget his PIN and this would result in the card getting trapped.

Fig. 1 shows the transition diagram of the existing ATM banking transaction system for an instance of withdrawal. In general, entry of the correct PIN is sufficient to authenticate to the bank system and protect against fraud. Thus the user is granted access to the system and allowed access for withdrawal as depicted in Figure 1 above. The system also effectively eliminates most of the common attempts to gain unauthorized access by retaining ATM

cards after the entry of an incorrect PIN three times. It however creates another problem for legitimate card owners

who cannot remember their PIN and also for cases where cards get trapped as a result of a faulty ATM.

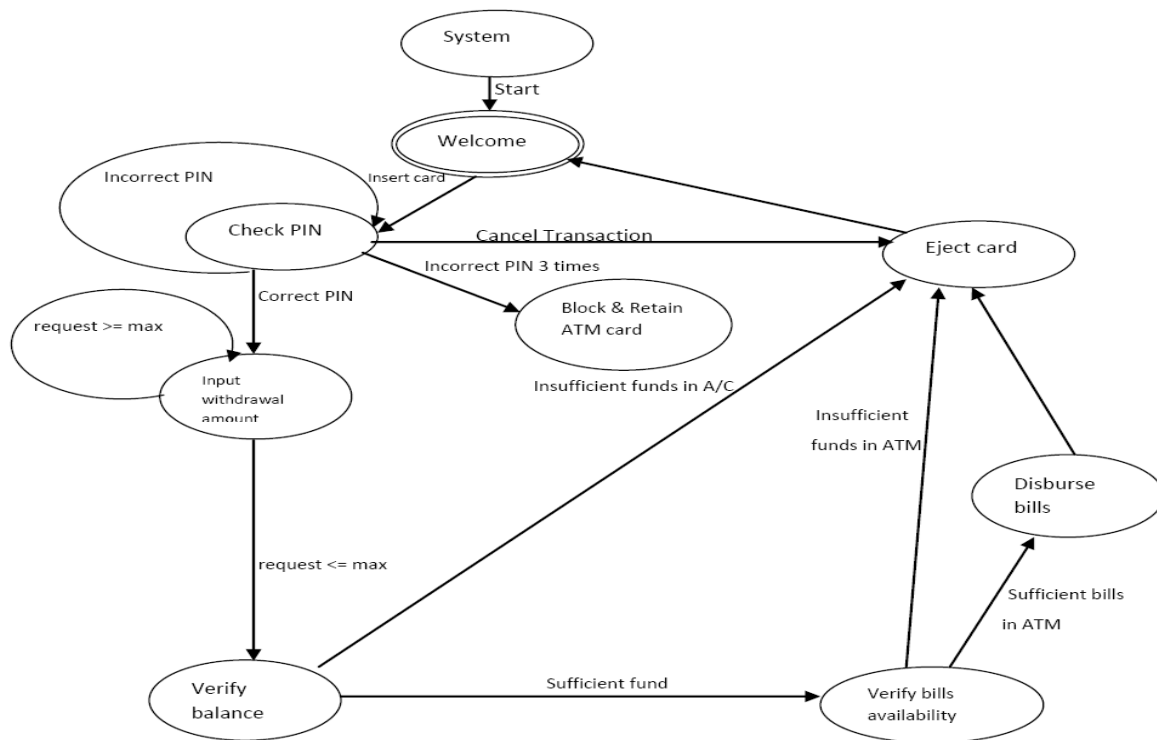


Figure 1. Transition Diagram for the Existing System

IV. THE PROPOSED SYSTEM

The ATM is a networked system connected to a centralized computer (server) which is responsible for the ATM operations. The use of second level authentication via SMS is possible and realistic at the ATM. The proposed system is an enhancement of the existing system which would help reduce the incidence of confiscated cards in the ATM.

Second level authentication can help minimize the number of confiscated bank cards in an ATM. Second level authentication could be used to ensure that only stolen cards get confiscated by the ATM. This is because if the user is the genuine owner of the card who has forgotten his PIN thus failed to authenticate to the bank system after three trials, the second level authentication process will provide another opportunity for the user to authenticate to the banks system. Even though the bank card gets blocked after the entry of an incorrect PIN thrice, this technology will prevent the card from getting trapped in the ATM.

Fig. 2 shows the transition diagram of the proposed ATM banking transaction system for an instance of withdrawal.

Entry of a correct PIN is still sufficient to authenticate to the bank system and protect against fraud. However, if an incorrect PIN is entered, the card still gets blocked but an authentication code is sent from the bank server to customer's pre-registered mobile number via SMS gateway. Thus the user is given another opportunity to authenticate to the bank system. If the user is able to provide the correct authentication code, the blocked card is ejected from the ATM. If however, the user was unable to provide the correct authentication code, then it is more likely to be a fraud attempt and the blocked ATM card gets retained by the ATM.

It is imperative to note that in any case, the entry of an incorrect PIN thrice still guarantees the blocking of the ATM card. Therefore the safety and security of the account holder is not compromised with the proposed system. The proposed system is only effective in solving the problem of ATM cards getting retained as a result of cases of false positives.

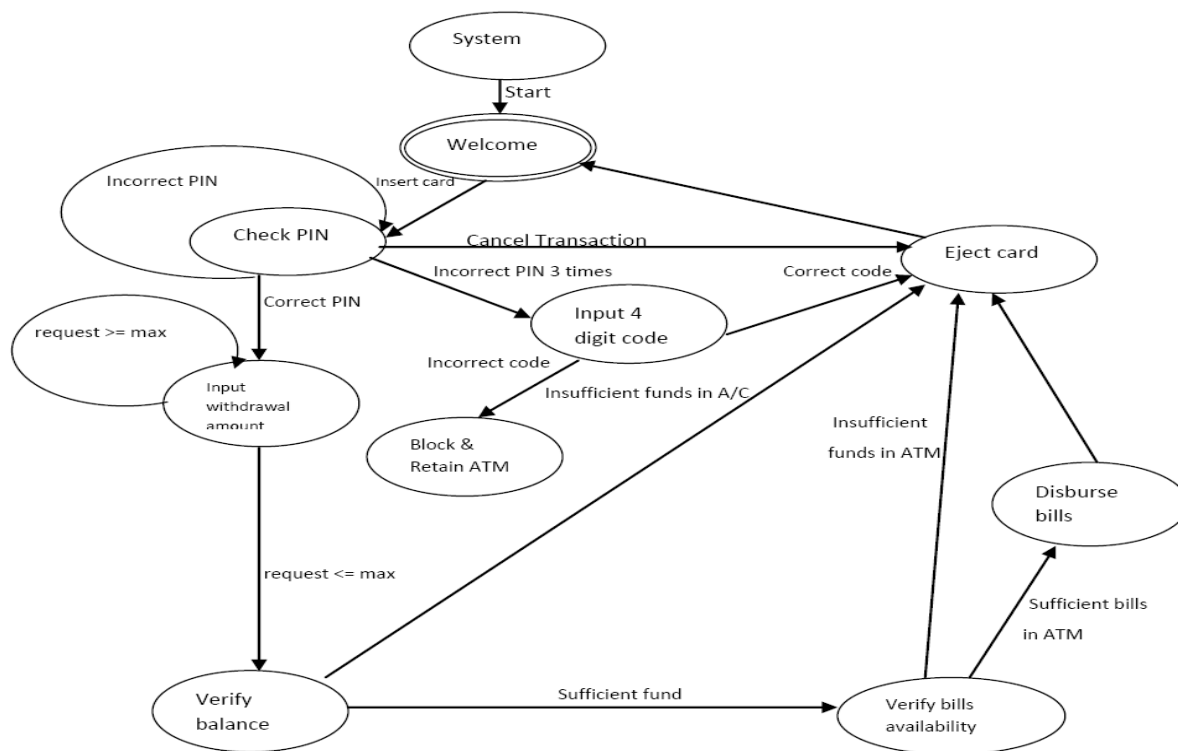


Figure 2. Transition Diagram for the Proposed System

V. THE ALGORITHM

The algorithm for the proposed system is summarized as follows:

START

STEP 1: Insert card into the ATM Machine

STEP 2: Enter PIN

STEP 3: If PIN is Valid

GOTO STEP 10

ELSE

GOTO STEP 4

STEP 4: Block ATM card

STEP 5: Generate authentication code and send to user's pre-registered mobile phone number

STEP 6: Enter authentication code

STEP 7: If authentication code is correct

GOTO STEP 8

ELSE

GOTO STEP 9

STEP 8: Eject blocked ATM card

GOTO STOP

STEP 9: Retain ATM card

GOTO STOP

STEP 10: Grant access to all ATM services

STOP

VI. DISCUSSION

The proposed system will reduce the time taken for customers to retrieve their confiscated ATM cards from the bank and also reduces the number of trapped cards that needs to be processed by bank officials. When cards get trapped on an ATM, most banks in Nigeria do not release the trapped cards to their own customers until after at least 24 hours of the cards getting trapped. ATM cards from other banks are not released to the owners but rather sent to the nearest branch of the customer's bank for onward delivery to the card owner.

With the proposed system, another opportunity will be provided for card owners to provide an authentication code which would be sent to their pre-registered mobile phones in order to authenticate to the bank system and prevent their bank cards from getting confiscated by the ATM after entering an in-correct PIN thrice.

VII. CONCLUSION

The banking industry in Nigeria has been positively impacted with the adoption of the ATM as an e-banking channel. About 80-90% of transactions conducted through the e-payment channels have been attributed to the ATM alone. The success of the ATM in the Nigerian e-banking industry is mainly because of its effectiveness and convenience for customers. The recent CBN directive on trapped ATM cards is however not in the best interest of the bank customers. The system proposed in this study uses second level authentication process to minimize the incidence of confiscated ATM cards in the Nigerian e-banking sector which will further encourage users to patronize the ATM as an e-banking channel because it will translate to good and quality services to the customers. This

is because it will reduce the time taken for customers to retrieve their confiscated ATM cards from the bank and also reduces the number of trapped cards that needs to be processed by bank officials. Considering the recent CBN directive, it will also reduce the number of cards that will have to be destroyed by the banks and also save legitimate card owners the cost of having their ATM cards reissued.

ACKNOWLEDGMENT

The authors wish to gratefully acknowledge the encouragements of Dr. Abraham Ochoche at the inception of this research.

REFERENCES

- [1] Wan, W.W.N.; Luk, C.L.; and Chow, C.W.C. (2005), Customers adoption of banking channels in Hong Kong, International Journal of Bank Marketing, Vol. 23, No. 3, pp. 255-272.
- [2] Das, S.S. and Debbarma S.J. (2011), Designing a biometric strategy (fingerprint) measure for enhancing ATM security in Indian e-banking system. International Journal of Information and Communication Technology Research. September 2011, Vol 1, no 5 pp197-203.
- [3] Jimoh R.G. and Babatunde A. N. (2014), Enhanced automated teller machine using short message service authentication verification. World Academy of Science, Engineering and Technology. International Journal of Computer, Information Science and Engineering 2014. Vol:8 No:1 pp.14-17
- [4] Richard, B. and Alemayehu, M. (2006), Developing e-banking capabilities in a Ghanaian bank: preliminary lessons. Journal of Internet Banking and Commerce, August 2006, vol. 11, no.2. Available online at: <http://www.arraydev.com/commerce/jibc/> Accessed on: 15 September, 2014.
- [5] National Bureau of Statistics. (2010), National Literacy Survey, 2010 – National Bureau of Statistics. Available online at: <http://www.nigerianstat.gov.ng/pages/download/43> Accessed on: 24 September, 2014.
- [6] UNICEF (2012), At a glance: Nigeria Statistics, Basic Indicators. Available online at: http://www.unicef.org/infobycountry/nigeria_statistics Accessed on: 24 September, 2014.
- [7] Prithika M. and Rajalakshmi P. (2013), Card duplication and crime prevention using biometrics. IOSR Journal of Computer Engineering (IOSR-JCE) Mar. - Apr. 2013, Vol10, No 1 pp 1-7. Available at: www.iosrjournals.org Accessed on: 15 September, 2014.
- [8] Selvaraju N. & Sekar G. (2010), A method to improve the security level of ATM banking systems using AES algorithm, International Journal of Computer Applications. June 2010 Vol 3 No.6.
- [9] Ravikumar S., Vaidyanathan S., Thamocharan S. and Ramakrishan S. (2013), A new business model for ATM transaction security using fingerprint recognition. International Journal of Engineering and Technology (IJET). Jun-Jul 2013 Vol 5 No 3 pp 2041-2047
- [10] Oko S. and Oruh J. (2012): Enhanced ATM security system using biometrics. IJCSI International Journal of Computer Science Issues, September 2012. Vol. 9, Issue 5, No 3, pp352-357. Available online at: <http://www.IJCSI.org> Accessed on: 17 September, 2014.
- [11] Padmapriya V. and Prakasam S. (2013), Enhancing ATM security using fingerprint and GSM technology. International Journal of Computer Applications October 2013 Vol. 80 No. 16 pp. 43-46
- [12] Okereke E. Ihekweaba G. and Okpara F.K. (2013), Facial verification technology for use in ATM transactions. American Journal of Engineering Research (AJER) Vol. 02 No. 5. pp. 188-193. Available online at: <http://www.ajer.us> Accessed on: 20 September, 2014.
- [13] Santhi B. and Ram Kumar K. (2012), Novel hybrid technology in ATM security using biometrics. Journal of Theoretical and Applied Information Technology. March 2012. Vol. 37 No. 2 pp.217-223
- [14] Central Bank of Nigeria (2014), Guidelines for Card Issuance and Usage in Nigeria. Banking and Payments System Department, May 2014. Available Online at: <http://www.cenbank.org> Accessed on: 25 September, 2014.
- [15] Chima O. (2014), CBN Explains Directive on Trapped ATM Cards. ThisDay Live 16 May 2014. Available online at: <http://www.thisdaylive.com/articles/cbn-explains-directive-on-trapped-atm-cards-/178620/>. Accessed on: 25 September, 2014.



Muhammad-Bello, Bilkisu Larai was born in Minna, Niger, Nigeria. She received her bachelor degree (B-Tech) in Mathematics/Computer Science from Federal University of Technology Minna, Niger state, Nigeria in 2006, and her master degree (MSc.) in Advanced Computer Science and Information Technologies Management from the University of Manchester, Lancashire, United Kingdom in 2011.

She joined Intercontinental Bank PLC as a customer service/e-banking officer where she gained a wealth of experience in electronic banking. In June, 2012, she joined the Federal University of Technology Minna, Niger state, Nigeria, as a lecturer in the Information and Media Technology Department. Her current research interests include: Electronic banking, Advanced Database Management Systems, Data Mining, Data and Knowledge Management, Green IT and Cloud computing.

Mrs. Muhammad-Bello is a member of the International Association of Engineers (IAENG).



Ganiyu, Olusegun Shefiu was born in Ibefun, Ogun state, Nigeria. He obtained his bachelor degree in Mathematics/Computer science (B-Tech) from Federal University of Technology Minna, Niger state, Nigeria in 2000, and his master degree in Information Science (M.Inf.Sc.) from the University of Ibadan, Oyo state, Nigeria in 2003.

He is currently an Assistant Lecturer in the Department of Information and Media Technology with wealth of industrial experience and certifications in various aspects of Information Technology among which are information system development (SCJP, SCBCD), Oracle Certified Professional, Sun Certified System Administrator (Solaris 10), CompTIA Project+ and CompTIA.

Mr. Ganiyu is a member of Computer Professional Registration Council of Nigeria (CPN).



Alhassan, Muhammed Enagi was born in Minna, Niger State, Nigeria. He obtained his bachelor degree in Library and Information Technology from Federal University of Technology Minna, Niger, Nigeria in 2007, and his Master degree in Information and Business

Technology from Loughborough University, United Kingdom in 2010.

He is currently a lecturer in Department of Information and Media Technology in Federal University of Technology Minna. He joined the academics in 2011. His research interests include: Enterprise Architecture, Collaborative Technologies, knowledge management, Green IT, cloud computing for enterprise and electronic commerce.