Development of Second-Level Authentication Process for a Higher Level Security in ATM Transactions

J. K. Alhassan
Department of Computer Science
Federal University of Technology
Minna, Nigeria
E-mail: jkalhassan@futminna.edu.ng

A. Ochoche
Statistics Department,
Central Bank of Nigeria,
Headquarters, Abuja, Nigeria
oabraham@cbn.gov.ng

A. M. Enagi,
Department of Information and Media Technology,
Federal University of Technology,
Minna, Nigeria

G. O. Shefiu
Department of Information and Media Technology,
Federal University of Technology, Minna, Nigeria

B. L. Muhammad-Bello
Department of Information and Media Technology,
Federal University of Technology, Minna, Nigeria

***Abstract*— The increase of automated teller machine (ATM) frauds has actuated the development of new authentication mechanisms to overcome security problems of personal identification numbers (PIN). As a rule, ATMs give users three tries for authentication to the bank server. In an event where the user fails to authenticate to the bank server, the ATM card will typically be blocked and also confiscated by the ATM. In this research, a model to provide second-level authentication for ATM transactions was proposed and implemented using Visual Studio and MySQL. To operate this system, the user is to insert the ATM card into the machine, provide the PIN and then set the withdrawal limit. Any amount above this limit will request the user to enter the second level authentication code which is sent to the user's mobile phone by the bank server. The application was tested and found to solve the problem of cards confiscation and stressful existing process of retrieving such cards. It is recommended for implementation by banks and other financial institutions.**

Keywords- authentication; security; transaction; automated teller machine

I. INTRODUCTION

The earliest and old-fashioned society lacked to some extent monetary tools, therefore, the whole give-and-take of goods and commodities was accomplished by the "barter system" (1). The contemporary society though started using monetary tools as a unit of give-and-take which now substituted the barter system. Therefore, money in numerous values were now used as the solitary buying power as contrary to the barter system. The modern age has substituted these old-style financial tools from a paper and metal centered money to "plastic money" in the form of credit cards, debit cards, and so on (2). This has caused in the cumulative usage of Automated Teller Machine (ATM) all over the world. The statistics of ATM card owners has persistent to raise as consequence of e-payment consciousness and the placement of extra ATM cash points by banks all everywhere the world. In Nigeria, 80-90% of all e-banking dealings are conceded out via the ATM channel (1). Paradoxically, actions of card impostors and 'intelligent' criminals seem to be on the rise. ATM scam has developed a countrywide subject touching together the banks and customers (3). Numerous banks have sustained to caution ATM card operators against revealing their ATM card particulars to a second party in order to impose the safety of ATM usage. Common approaches used by cheats to propagate ATM scam comprise, absolute card robbery, shoulder surfing of operators at ATM points, usage of false personal identification number (PIN) Pad overlap and PIN interference via emails and text messages.

The difficult of ATM scam does not touch only the banks, somewhat, it is a large risk to all parties involved and it needs a synchronized and supportive action on the part of the bank, bank clients and the law implementation organizations (4), (5). ATM scams do not just cause economic harm to banks but they likewise demoralize clients' self-assurance in the usage of ATMs (6). This would dampen a larger usage of ATM for financial dealings. Further so, ATM facilities are extremely

This research was funded by Tertiary Education Trust Fund institution-based research intervention fund (TETFUND/FUTMINNA/2014/47) through Federal University of Technology, Minna, Nigeria.

lucrative for banks and numerous banks particularly in Nigeria violently market the usage of ATM cards (7). It is consequently in the importance of banks to avert ATM scams. Therefore, safety and insurance actions that provides better defense to the ATMs must to be put in place.

To guarantee the protection and honesty of internal online payments, many banks have presented a second level authentication method to confirm online dealings, (8) and (9). This technology was first used by Google to improve the safety of electronic mail account holders. Second level authentication also known as two factor authentication or two-step confirmation was used by Google to add an additional cover of safety to operators' Google Apps accounts by demanding them to enter a verification code in addition to their username and password, while signing in to their account (10), (11), (12) and (13). Second level authentication is a security procedure that can be consummate by applying either a mobile phone (SMS) or token device which offers a one-time password for transaction authentication.

This authentication procedure aids to guard operators' accounts from illegal admittance. Consequently, should an illegal operator manage to get a operator's password/ PIN, or even if a password is broken, predicted, or else taken, the invader will not be capable to validate to the system without admittance to the operator's confirmation encryptions, which only the operator can get via their own mobile phone or token device. Consequently, this study is on the usage of second level authentication and extra security features for ATM deal. The continuing parts of this study comprises literature review, methodology, results, discussion and findings.

II. Literature Review

Numerous earlier researches connected to the safety and operation of the ATM dedicated on improving ATM safety through biometric method. Though, very tiny or no effort has engrossed on the procedure of the ATM from the viewpoint of ATM cards being confined in the ATM. A biometric policy by finger print measure was planned by Das and Debbarma, (14), for improving ATM safety in Indian E-banking structure. In a latest study by Prithika and Rajalakshmi, (15) proposed using the Iris Recognition and Palm Vein (IRPV) recognition technology to avoid card replication and crimes via the ATM. The Advanced Encryption Standard (AES) algorithm was accepted in (16) to increase the safety level of ATM Banking Systems. Finger print recognition in digital image processing was implemented in (17) for a suggested new business model which would improve ATM safety. In (18) nevertheless, the standing safety of the ATM system was improved by joining the fingerprints of operators into the bank's database as a means for additional authentication procedure. ATM based fingerprint confirmation was established and simulated for ATM procedures in imperative to lessening cheats connected with the use of ATM. A latest study piloted by (19) improved the safety of the ATM by a mixture of fingerprint and GSM technology. The fingerprint recognition technology and PIN verification was implanted into a GSM modem which was linked to a microcontroller to produce 4 digits one-time passcode which is to be directed to a operator's mobile number every time the operator tries to register the finger print image on the banking system. A alike study in (20) also established a sample of an improved ATM verification system by Short Message Service (SMS) confirmation and also piloted a usability trying of the offered system. A system which combines facial recognition technology into the individuality confirmation procedure used in ATMs was offered in (20). The offered ATM model established using facial recognition software was more dependable in providing safety. A Novel Hybrid Technology in ATM Security Using Biometrics was suggested in (21). The suggested algorithm embraced in the study provided two stages of safety by together biometric and GSM technology. In adding to the PIN delivered, a second level authentication by fingerprint was compulsory. In an occasion whereby the fingerprint verification 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 verification. A current study in (22) suggested a new model for improving ATM Security in Nigeria using Second-Level Authentication.

III. Methodology

The ATM second-level authentication research is simulated by a designed model encompassing of hardware and software modules to copycat a complete ATM operation as showed in Figure 1.

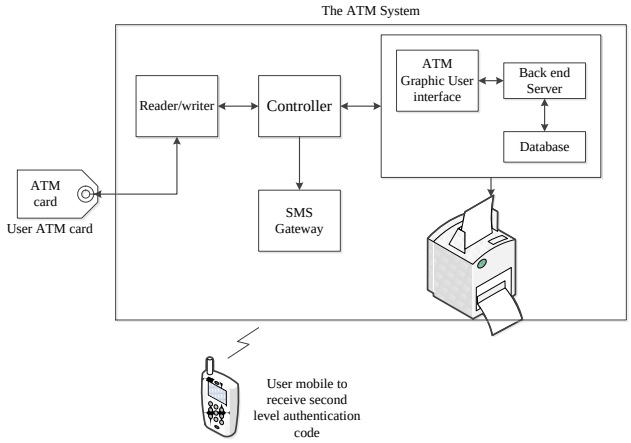

Figure 1: System Flow Diagram

The ATM card unit includes the usage of a smart card. The card can also joins to a reader with direct physical connection or with a remote contactless radio frequency interface. In this research, the physical connection card is used since unbroken communication is obligatory among the card and the reader through the operation procedure.

The card in the instance of this research is programmed via a smart card reader/writer. The smart card reader/writer can read from the card and can write to it as well. An I2C communication protocol was used to communicate with the card via the card reader. Each user details such as: account name, account number, pin number, and phone number, were written to the card for each of the user. These information are

also stored on the database for verification each time the user inserts the ATM smart card.

Smart card reader are used to read/write on smart cards. The control unit was programmed to manage the operation of the smart card reader/writer. The central control unit interfaces between the database and the user interface end. This control unit is divided into two: the software part which was implemented using Microsoft Visual studio and runs on a windows 8 All-in-One PC, the second part involves a hardware programing which runs on an Atmel microcontroller. The microcontroller monitors the user's ATM cards through a smart card reader and communicate card details to the central control unit. The microcontroller used in this research is a low-power CMOS 8-bit microcontroller based on the AVR RISC architecture.

In this research, an ultra-compact and reliable wireless module was used to achieve the SMS gateway. It has a complete Dual-band GSM/GPRS solution in a Surface Mount Technology (SMT) module which is embedded in the ATM machine system making the entire system to have a small dimensions and eventually a cost-effective solutions. Figure 2 shows the SMS gateway module connected to the database central application.

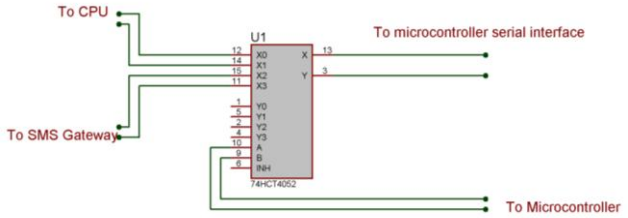

Figure 2: SMS gateway interface to CPU

The database was created using the Microsoft Access database engine. The database created is automatically stored as an SQL database hence requiring MySQL query language to access the data. A connection string is required to connect to the database. The connection string identifies a managed provider named Microsoft.ACE.OLEDB.12.0, which is an underlying database components that understands how to connect to a database and extract data from it. SQL server is one of the two most popular providers available in Visual Studio. The database contains field such as: account name, account number, account balance, and phone number etc. The frontend of the ATM App connect to the database to verify and update user account information.

The flow chart in Figure 3 shows the working operation of the system.

IV. Result and Discussion

The USB cable of the hardware unit was connected to the USB port of the computer, it was turned on and the software was lunched. If the software is launched before the hardware unit is powered on, the user receives a message "Hardware Not Connected". A green LED light comes ON to indicate that the hardware is ready. It goes OFF once a card insertion is detected. The reset button from the side of the hardware unit was pressed, then ATM application was lunched.

ATM card was inserted and a message prompted to enter the secret number, after which transactions were displayed to make a choice. Sensitive transactions involve the user to enter a second level authentication code which will be sent to user's mobile phone. A red LED flashes immediately after the SMS is sent. This totally prevent a holder of a stolen card from performing sensitive transactions such as Cash withdrawer, Changing phone number, Password change, and Setting user withdrawer limit.

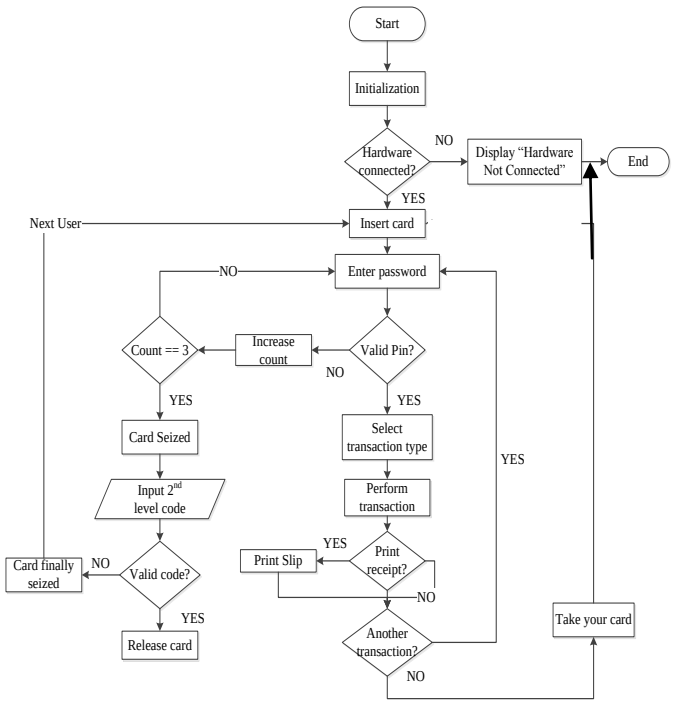

Figure 3: Operation flow chart

A. Findings

In this research, a more secured and fast way for retrieving ceased ATM card by user is proposed. After the user enters the wrong password for up to three times, the card is retained and a second level authentication code is sent to the user mobile phone. If the user is the rightful owner of the card, the card is release immediately the user key in the authentication code; otherwise, the card is finally seized. This new approach save the user the stressful process of retrieving the card using

the existing approach. This is recommended for implementation by financial institutions.

Acknowledgment

The authors acknowledge Tertiary Education Trust Fund institution-based research intervention fund (TETFUND/FUTMINNA/2014/47) through Federal University of Technology, Minna, Nigeria for sponsoring this research.

Disclaimer:

Dr. A. Ochoche is a staff of Statistics Department, Central Bank of Nigeria Head Office. The opinions expressed in this paper are those of the authors and do not necessarily reflect the position of the Central Bank of Nigeria

References

[1] R. G Jimoh, and A. N. Babatunde, "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, Vol.8 No.1 pp. 14-17, 2014.

[2] S. A. Adepoju, and M. E. Alhassan, "Challenges of automated Teller Machine (ATM) usage and fraud occurrences in Nigeria – A case study of selected banks in Minna metropolis," Journal of Internet Banking and Commerce, Vol. 15, No. 2, pp. 1-10, 2010, Available online at: http://www.arraydev.com/commerce/JIBC/2010-08/Solomon.pdf.

[3] B. Richard, and M. Alemayehu, "Developing e-banking capabilities in a Ghanaian bank: preliminary lessons," Journal of Internet Banking and Commerce, Vol. 11, No.2, August 2006, Available online at: http://www.arraydev.com/commerce/jibc/ Accessed on: 15 September, 2014.

[4] M. I. Siddique, and S. Rehman, "Impact of Electronic crime in Indian banking sector – An Overview," International Journal of Business & Information Technology, Vol. 1, No. 2, September 2011, pp.159-164.

[5] H. B. Leow, "New Distribution Channels in banking Services," Banker's Journal Malaysia, No.110, June 1999, pp.48-56.

[6] A. A. Aliyu, and R. B. Tasmin, "Information and Communication Technology in Nigerian Banks: Analysis of Services and Consumer Reactions," In proceedings of 3rd International Conference in Business and Economic Research (3rd ICBER 2012), March 2012, pp. 150-164.

[7] O. Shoewu, and F. O. Edeko, "Outgoing call quality evaluation of GSM network services in Epe, Lagos State," American journal of scientific and industrial research, Vol. 2, No.3, 2011, pp. 409-417.

[8] S. Rosenblatt, "Two-factor authentication: What you need to know," Retrieved from: http://www.cnet.com/news/two-factor-authentication-what-you-need-to-know-faq/ Last updated on April 14, 2014. Accessed on November 23, 2014.

[9] 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.

[10] O. Chima "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.

[11] A. De Luca, M. Langheinrich, and H. Hussmann, "Towards Understanding ATM Security – A Field Study of Real World ATM Use," Retrieved from: https://cups.cs.cmu.edu/soups/2010/proceedings/a16_deluca.pdfAccessed on November 26, 2014.

[12] C. Kyle, "Biometrics: An In Depth Examination. SANS Institute Information Security Reading Room." SANS Institute 2004, Retrieved from: http://www.sans.org/reading-room/whitepapers/authentication/biometrics-in-depth-examination-1329. Accessed on November 26, 2014.

[13] N. Y. Liu, "Bio Privacy: Privacy Regulations and the Challenge of Biometrics," Taylor & Francis, 2013.

[14] S. S. Das, and S. J. Debbarma, "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 pp. 197-203.

[15] M. Prithika, and P. Rajalakshmi, "Card duplication and crime prevention using biometrics," IOSR Journal of Computer Engineering (IOSR-JCE), Mar. - Apr. 2013, Vol. 10, No. 1 pp. 1-7.

[16] N. Selvaraju, and G. Sekar, "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, pp. 5-10.

[17] S. Ravikumar, S. Vaidyanathan, S. Thamotharan, and S. Ramakrishan, "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.

[18] S. Oko, and J. Oruh, "Enhanced ATM security system using biometrics," IJCSI International Journal of Computer Science Issues, September 2012, Vol. 9, Issue 5, No. 3, pp. 352-357.

[19] V. Padmapriya, and S. Prakasam, "Enhancing ATM security using fingerprint and GSM technology," International Journal of Computer Applications, October 2013, Vol. 80, No. 16, pp. 43-46.

[20] E. Okereke, G. Ihekweaba, and F. K. Okpara, "Facial verification technology for use in ATM transactions," American Journal of Engineering Research (AJER), Vol. 02, No. 5, pp. 188-193.

[21] B. Santhi, and K. Ram Kumar, "Novel hybrid technology in ATM security using biometrics," Journal of Theoretical and Applied Information Technology, March 2012, Vol. 37, No. 2, pp.217-223.

[22] B. L. Muhammad-Bello, S. O. Ganiyu, and M. E. Alhassan, "A New Model for Enhancing ATM Security in Nigeria Using Second Level Authentication. International Journal of Science and Advanced Technology. Vol. 04, No 09, September, 2014. pp. 12-16.