An Enhanced ATM Security System using Second-Level Authentication

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

Alhassan M.E.
Information and Media Technology Department
School of Information and Communications Technology
Federal University of Technology Minna
Nigeria

Ganiyu, S.O.
Information and Media Technology Department
School of Information and Communications Technology
Federal University of Technology Minna
Nigeria

ABSTRACT
The increase of automated teller machine (ATM) frauds has actuated the development of new authentication mechanisms that can overcome the security problems associated with the personal identification numbers (PIN). The traditional PIN entry system has stood the test of time mainly because of its speed and memorability which are part of the metrics used to access the ATM authentication system. The third metric, which is security has often been compromised thence the need for a more secured authentication system for ATM operations. This paper therefore proposes an enhanced ATM security system using second level authentication process. The method adopted for this research is to develop an enhancement of the existing system by building an additional security mechanism on the existing system's security mechanism. The proposed system was found to be realistic and cost effective when compared to other proposed authentication mechanism for ATM transactions.

General Terms
ATM Security.

Keywords
Authentication, ATM Security, Second-Level Authentication, ATM.

1. INTRODUCTION
The ancient and traditional society lacked any monetary instruments, thence the entire exchange of goods and merchandise was managed by the "barter system" [1]. The modern society however started using monetary instruments as a unit of exchange which now replaced the barter system. Thus, money in various denominations was now used as the sole purchasing power as against the barter system. The contemporary era has replaced these traditional monetary instruments from a paper and metal based currency to "plastic money" in the form of credit cards, debit cards, etc [2]. This has resulted in the increasing use of Automated Teller Machine (ATM) all over the world.

The numbers of ATM card holders continue to grow daily as result of e-payment awareness and deployment of more ATM cash points by banks all around the world. Ironically, activities of card fraudsters and 'intelligent' criminals appear to be on the increase. Many banks have continued to warn ATM card users against disclosing their ATM card details to a second party in order to enforce the security of ATM usage.

Common approaches used by fraudsters to perpetuate ATM fraud include, outright card theft, shoulder surfing of users at ATM points, use of fake PIN Pad overlay and PIN interception via emails and text messages.

The problem of ATM fraud does not affect only the banks, rather, it is a big threat to all parties involved and it requires a coordinated and cooperative action on the part of the bank, bank customers and the law enforcement agencies [3], [4]. ATM frauds do not just cause financial loss to banks but they also undermine customers' confidence in the use of ATMs [5]. This would discourage a greater use of ATM for monetary transactions. More so, ATM services are highly profitable for banks and many banks especially in Nigeria aggressively market the use of ATM cards [6]. It is therefore in the interest of banks to prevent ATM frauds. Thus, precautionary and insurance measures that gives greater protection to the ATMs need to put in place.

To ensure the safety and integrity of domestic online payments, various banks have introduced a second level authentication process to authenticate online transactions. This technology was first used by Google to enhance the security of electronic mail account holders. Second level authentication also known as two factor authentication or two-step verification was used by Google to add an extra layer of security to users' Google Apps accounts by requiring them to enter a verification code in addition to their username and password, when signing in to their account [7]. Second level authentication is a security process that can be accomplished by utilizing either a mobile phone (SMS) or token device which provides a one-time password for transaction authentication.

This authentication process helps to protect users' accounts from unauthorized access. Therefore, should an un-authorized user manage to obtain a user's password/ PIN, or even if a password is cracked, guessed, or otherwise stolen, the attacker will not be able to authenticate to the system without access to the user's verification codes, which only the user can obtain via their own mobile phone or token device.

Objectives
The aim of this study is to attain a higher level security in ATM transactions and operations through second level authentication process. The objectives of this study are as follows:

i. To propose a second-level authentication system on the existing ATM process for withdrawal, after entry of correct a PIN.

ii. To propose second-level authentication system in a scenario where a customer-specified withdrawal limit is attained.

2. LITERATURE REVIEW

2.1 Research Background

PThe increase of automated teller machine (ATM) frauds has actuated the development of new authentication mechanisms to overcome security problems of personal identification numbers (PIN). These authentication mechanisms are usually assessed based on speed, security, and memorability in comparison with traditional PIN entry systems [8]. The biometric authentication technique seems to be the most popular emerging alternative mechanism as against PIN-based ATM authentication. This authentication technique however has its own flaws. Fingerprints, for example, are unique but they are not secrets. We leave them everywhere with everything we touch, therefore, they can easily be forged with a film [9]. The fingerprints on a person can get damaged and also, it changes with age [10]. In addition to this, another serious flaw with the fingerprints is that the theft of a person's biometric leads to some serious issues as reenrolment is not possible unlike the resetting or changing of PIN.

The use of second level authentication can help ensure the security of ATM operations. Second level authentication process involves the use of two authentication techniques. It is commonly used for online transactions by many financial institutions. The purpose of the second level authentication technique is to validate that the individual logging in is the correct one. The second level authentication technique uses the first two out of the three commonly accepted types of user authentication outlined below [9]:

i. Something you know – For example passwords or PIN.

ii. Something you have – For example token devices, smart cards, digital certificates, and keys.

iii. Something you are – A biometric or biological trait such as finger prints, palm vein image, iris image or voice

The third option above is mainly used by authentication techniques that use biometrics. With second level authentication in place, an impostor or a fraudster would not only need to steal the PIN, but would also have to know the onetime password/code as well.

As a rule, the 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 and also confiscated by the ATM. If the user were to be a fraudster, confiscating the bank card would prevent the fraudster from further guessing the correct PIN and subsequently withdrawing from the card owner's account via the ATM. However, in a situation whereby the fraudster is in possession of both the bank card and correct PIN, there is no way of preventing such withdrawals via the ATM machine. Thus, this paper proposes the second-level authentication mechanism as a means to improve the security of ATM usage and operations

2.2 Related Work

Many recent studies have focused on using biometric techniques in enhancing the security of the ATM. However, a few studies have also exploited the use of GSM Technology, while some have adopted a combination of both techniques. Table 1 summarizes some of the related studies, the techniques they adopted, the contribution and limitations of the studies.

Table 1. Summary of past related studies

AUTHORS	TECHNIQUE ADOPTED	CONTRIBUTION	LIMITATIONS
Oko S. and Oruh, J. (2012) [11]	Finger print biometric token.	Developed an ATM based fingerprint verification and simulated it for ATM operations by incorporating the fingerprints of users into the bank's database.	1. The system developed was inefficient because there was no finger print matching algorithm. 2. The system developed was not built as an enhancement of the existing system.
Ravikumar et al. (2013) [12]	Finger print recognition in digital image processing using both primary and reference fingerprint to authenticate users instead of the traditional pin number	A new business model which would enhance ATM security was proposed.	1. Another reference fingerprint belonging to a nominee or a close family member was adopted which could also lead to a security breech, thus compromising the security of the account owner. 2. The proposed system was not built on the existing system.
Padmapriya V. and Prakasam S. (2013) [13]	A combination of fingerprint biometric token and GSM technology	Proposed a system architecture that incorporates both the finger print and GSM technology into the existing PIN-based authentication process.	1. A nominee or third party's finger print was incorporated in the architecture. 2. There is a discord between the main user and the nominee user in the

			proposed system architecture
Jimoh R.G. and Babatunde A. N. (2014). [1]	Short Message Service (SMS) verification.	Developed an algorithm for enhancing ATM authentication system using Short Message Service (SMS) verification. 2.Conducted a usability testing of the proposed system	1. The developed algorithm only considered a minimum withdrawal amount.
Das, S.S. and Debbarma S.J. (2011) [14]	Finger print biometrics	Developed a system for the withdrawal interface of the ATM while incorporating the finger print biometric in the authentication process	1. A nominee or third party's finger print was incorporated in the design.
Santhi B. and Ram Kumar K. (2012) [15]	Finger print biometric and GSM technology	Proposed an algorithm that provides two phases of security using both biometric and GSM technology as alternatives.	
Prithika M. and Rajalakshmi P. (2013) [16]	Iris Recognition and Palm Vein (IRPV) recognition technology	Proposed using the Iris Recognition and Palm Vein (IRPV) recognition technology to prevent card duplication and crimes via the ATM	1. The proposed system was not built as an improvement on the existing system
Okereke E. Ihekweaba G. and Okpara F.K. (2013) [17]	Facial recognition technology	A system which incorporates facial recognition technology into the identity verification process used in ATMs was proposed	1. The proposed system was not built as an improvement on the existing system. 2. The study relied on open-source facial recognition program and did not discuss the local features that will be analyzed for the facial verification process.
Ibidapo et. al. (2010) [18]	Fingerprint biometrics	A fingerprint mechanism as a biometric measure to enhance the security features of the ATM was developed	
Selvaraju N. & Sekar G. (2010) [19]	Advanced Encryption Standard (AES) algorithm	The Advanced Encryption Standard (AES) algorithm was adopted to improve the security level of ATM Banking Systems.	

3. THE EXISTING SYSTEMS

The existing ATM system authenticates transactions via the card and PIN-based system. Thereafter, it grants access to bank customers to several services such as cash withdrawal and deposits, account to account transfers, balance enquiry, top-up purchases and utility bills payment. The ATM system compares the PIN entered against the stored authorization PIN for every ATM users. If there is a match, the system authenticates the user and grants access to all the services available via the ATM. If there is a mismatch on the other hand, the user authentication process fails and the user is given two more opportunities to enter a correct PIN. If an incorrect PIN is entered for the third time, the card gets blocked and retained by the ATM.

An instance of cash withdrawal on the existing ATM system is depicted in the transition diagram in Figure. 1. Entry of a correct PIN is adequate to authenticate a user to the bank system and thereafter grant access to the system for withdrawal as depicted in Figure 1 .The existing system also retains ATM cards after entry on an incorrect PIN thrice thereby eliminating further attempts to gain unauthorized access.

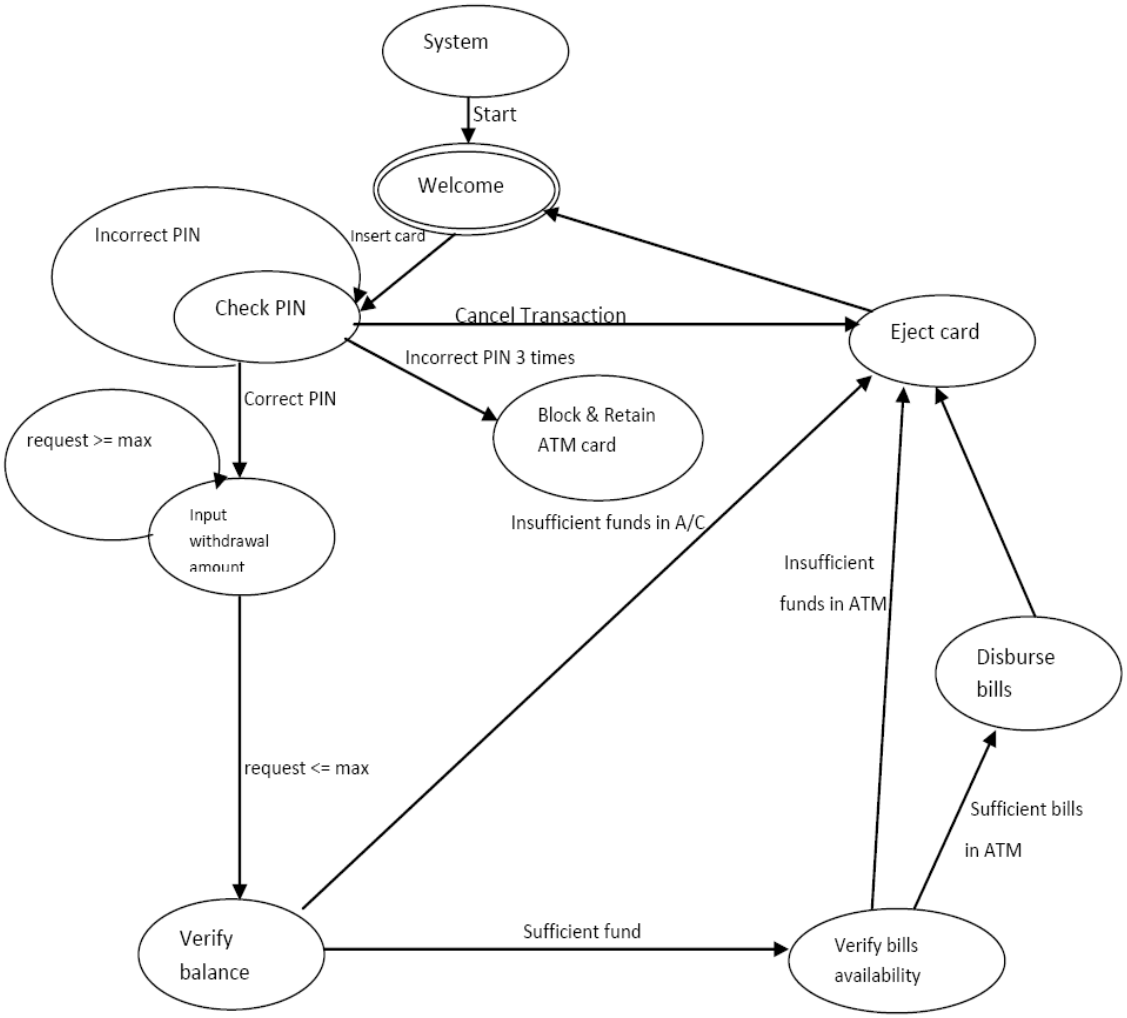

Figure 1: Transition diagram of the existing system

4. THE PROPOSED SYSTEM

The proposed system is an enhancement of the existing system, and, it is built upon the existing card and PIN-based system. The proposed system is in two different modes; the first will improve the security of the ATM by applying second level authentication on the existing ATM process for withdrawal, after entry of correct a PIN, while the second will apply second level authentication in a scenario where a customer-specified withdrawal limit is attained.

Figure 2 depicts an instance of withdrawal on the ATM for the proposed system which is an enhancement of the existing system. The entry of a correct PIN is inadequate to authenticate to the bank system. This is because an additional level has been incorporated for the authentication process which requires the customer to enter a valid code which will be sent to the customer's pre-registered mobile device via SMS gateway. If a correct code is supplied the customer gets authenticated and is granted access for withdrawal. However, if an incorrect code is supplied even after the entry of a correct PIN, the authentication process fails and the customer is denied access for withdrawal.

The second mode depicted in Figure 3 is also an instance of withdrawal on the ATM. This mode gives the customer the opportunity to choose the second level authentication process as an additional level of authentication for withdrawal in order to guarantee the security of the account owner. With this mode, a customer-specified withdrawal limit must be attained before the system prompts for entry of a valid code. If a valid code is supplied, the authentication process is complete and the customer is granted access for withdrawal. On the other hand, if an invalid code is supplied, the authentication process fails and the customer is denied access for withdrawal. It is imperative to note that if a customer-specified withdrawal limit is not in place, the entry of a valid PIN will be sufficient to authenticate the customer to the system and thereafter grant access for withdrawal. This implies that the second level authentication process would not be applied in such instances.

In addition, the entry of an incorrect PIN still guarantees maximum security in the proposed system because the bank card gets blocked and retained by the ATM in such instances.

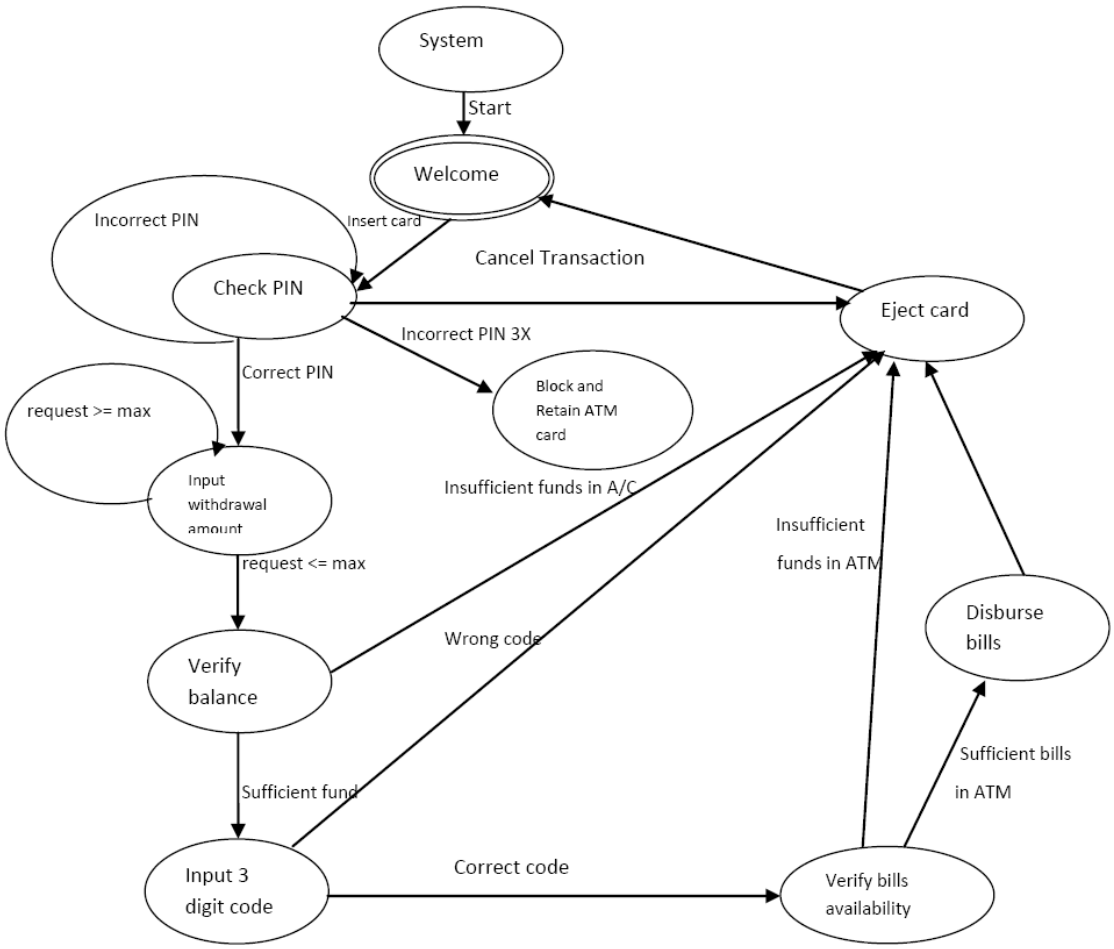

Figure 2: Transition Diagram for the Proposed System without customer specified limits

4.1 The Algorithms

The algorithms for the proposed system are described below. Algorithm A describes the proposed system without customer specified limits while Algorithm B describes the proposed system for the scenario where a customer specified limit is in place.

4.1.1 Algorithm A

START

STEP 1: Insert card into the ATM Machine

STEP 2: Enter PIN

STEP 3: If PIN is Valid

GOTO STEP 7

ELSE

STEP 4: Verify if Incorrect PIN has been entered trice

STEP 5: If incorrect PIN entered trice

GOTO STEP 6

ELSE

GOTO STEP 2

STEP 6: Block and Retain ATM card

GOTO STEP 17

STEP 7: Input withdrawal amount

STEP 8: If withdrawal amount > maximum allowed

GOTO STEP 7

STEP 9: Verify account balance

STEP 10: If balance is sufficient

GOTO STEP 11

ELSE

GOTO STEP 17

STEP 11: Generate authentication code and send to the customer's pre-registered mobile phone number

STEP 12: Enter authentication code

STEP 13: If authentication code is correct

GOTO STEP 14

ELSE

GOTO STEP 17

STEP 14: Verify bills availability

STEP 15: IF sufficient bills

GOTO STEP 16

ELSE

GOTO STEP 17

STEP 16: Disburse bills

STEP 17: Eject Cards

STOP

4.1.2 Algorithm B

START

STEP 1: Insert card into the ATM Machine

STEP 2: Enter PIN

STEP 3: If PIN is Valid

GOTO STEP 7

ELSE

STEP 4: Verify if Incorrect PIN has been entered trice

STEP 5: If incorrect PIN entered trice

GOTO STEP 6

ELSE

GOTO STEP 2

STEP 6: Block and Retain ATM card

GOTO STEP 21

STEP 7: Input withdrawal amount

STEP 8: If withdrawal amount > maximum allowed

GOTO STEP 7

STEP 9: Verify account balance

STEP 10: If balance is sufficient

GOTO STEP 11

ELSE

GOTO STEP 21

STEP 11: Verify customer-specified limit exists

STEP 12 IF customer-specified limit exists

GOTO STEP 13

ELSE

GOTO STEP 18

STEP 13: Verify if withdrawal amount > withdrawal limit

STEP 14: If withdrawal amount > withdrawal limit

GOTO STEP 15

STEP 15: Generate authentication code and send to customer's pre-registered mobile phone number

STEP 16: Enter authentication code

STEP 17: If authentication code is correct

GOTO STEP 18

ELSE

GOTO STEP 21

STEP 18: Verify bills availability

STEP 19: If sufficient bills

GOTO STEP 20

ELSE

GOTO STEP 21

STEP 20: Disburse bills

STEP 21: Eject Cards

STOP

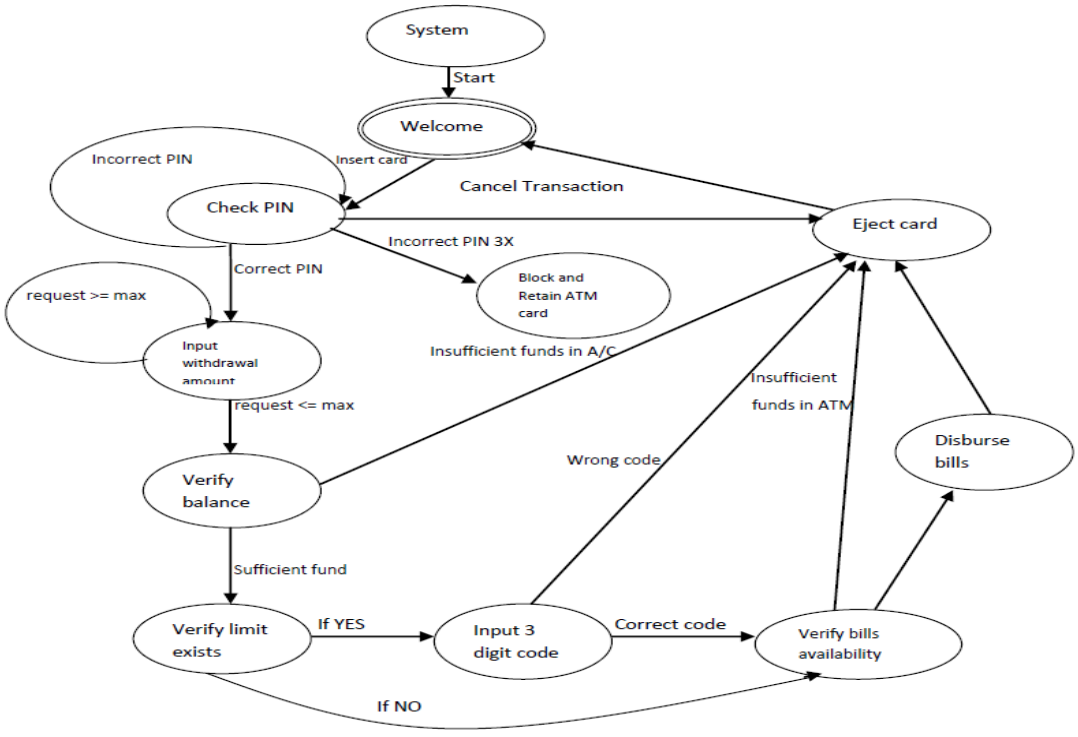

Figure 3: Transition Diagram for the proposed system with customer specified limit

5. THE PROPOSED SYSTEM MODEL

The ATM second-level authentication process for the proposed system will be simulated by designing a model comprising of hardware and software components to mimic a complete ATM transaction as depicted in Figure 4. The model comprises four interacting subsystems namely, ATM machine, bank server, Short Message Application Programming Interface (SMS API) and customer. The software component of the proposed system will be developed using Java and/or C programming languages, MySQL (Standard edition) will serve as the database management system and SMS API will be used to route SMS from the bank server to the customers' mobile device via SMS gateway. The major hardware for the research include: a backend server with high configuration, a terminal with touch screen features to simulate ATM machine, crossover cabling connection and mobile devices. A customer using a pre-configured ATM card containing necessary transaction information will participate in the research.

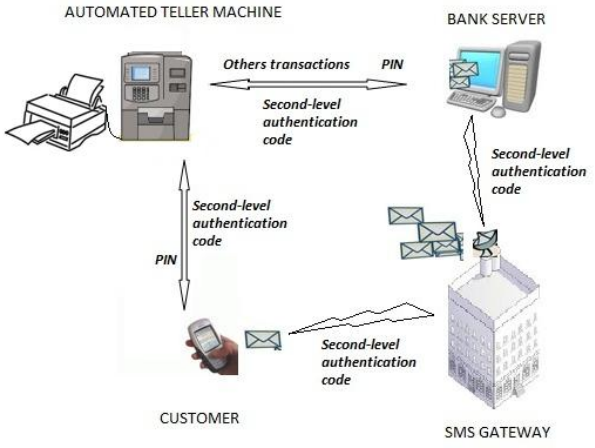

Figure 4: Second-Level Authentication Model for the proposed system

6. CONCLUSION

The adoption of the ATM as an electronic banking channel has positively impacted the banking industry worldwide because it is very effective and convenient for bank customers [20]. The advent of ATM fraud has however been a menace for many banks all over the world and many banks now aim to eradicate fraud costs to the bank. The proposed system can provide a practical and workable solution that addresses the requirements of the regulatory authority of the banks. The adopted technology of the proposed system is also cheaper to deploy than the biometric authentication technique because it utilizes the components of the existing system. The model can also provide for high withdrawal limits to cater for the demands of a cash-focused customer base. In general, it will positively impact the banking industry and the society by reducing the rising levels of crimes that are associated with ATM transactions.

The proposed second level authentication mechanism for ATMs will increase customer satisfaction and also give customers the peace of mind they need considering the high level of security applied to their accounts. Finally, it will limit the financial risks of customers given that they most times take the responsibility for financial loss via ATM rather than being allowed to pass on the risk to the banks.

In the future, we will implement the proposed system using the second-level authentication model discussed in this paper.

7. ACKNOWLEDGMENTS

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

8. REFERENCES

[1] 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

[2] Adepoju, A.S & Alhassan, M.E. (2010). 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. [Online]. Available: http://www.arraydev.com/commerce/JIBC/2010-08/Solomon.pdf

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

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

[5] Aliyu, A.A. & Tasmin, R.B. (2012) 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

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

[7] Rosenblatt, S. (2013). 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.

[8] De Luca, A., Langheinrich, M. & Hussmann, H. (2010). 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.

[9] Kyle, C. (2004). 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.

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

[11] 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, pp. 352-357.

[12] Ravikumar, S., Vaidyanathan, S., Thamotharan, S. & 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

[13] Padmapriya, V. & 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.

[14] Das, S.S. & 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 pp. 197-203.

[15] Santhi, B. & 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.

[16] Prithika, M. & 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.

[17] Okereke, E. Ihekweaba, G. & 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.

[18] Ibidapo, O. A., Omogbadegun, Z. O, & Oyelami, O.M. (2010). Towards Designing a Biometric Measure for Enhancing ATM Security in Nigeria E-Banking System. International Journal of Electrical & Computer Sciences IJECS-IJENS Vol:10 No:06. pp. 63-68

[19] 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

[20] Muhammad-Bello, B. L., Ganiyu S.O, Alhassan M.E. (2014). 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