I. J. Computer Network and Information Security, **2017, 10, 50-56**
Published Online October 2017 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijcnis.2017.10.06

Improving Security Using a Three-Tier Authentication for Automated Teller Machine (ATM)

Moses O. Onyesolu
Department of Computer Science, Nnamdi Azikiwe Univerity, Awka, 420001, Nigeria.
E-mail: mo.onyesolu@unizik.edu.ng

Amara C. Okpala
Department of Computer Science, Nnamdi Azikiwe Univerity, Awka, 420001, Nigeria.
E-mail: amaraokpala@yahoo.com

Received: 20 February 2017; Accepted: 16 March 2017; Published: 08 October 2017

***Abstract*—**The current use of Personal Identification Number (PIN) for verification of the validity of a customer's identity on Automated Teller Machine (ATM) systems is susceptible to unauthorized access and illegal withdrawal of cash from the ATM, hence, the need for more reliable means of carrying out user authentication. We present a three-tier authentication model with three layers of authentication using password, fingerprint and One-Time-Password (OTP). The identity of an ATM user is validated using password, fingerprint and OTP. Object-Oriented Analysis and Design Methodology (OOADM) was employed in the investigation of the existing system and analysis of the proposed system. Microsoft Visual Basic.NET and Microsoft SQL Server were employed in the implementation of the system. The result is a three-tier authentication model for ATM. Alphabetic keys and some special character keys were introduced to the existing numeric keypad for authentication. The ATM was interfaced with a fingerprint reader for improved security.

***Index Terms*—**Automated Teller Machine, Authentication, Password, Fingerprint, One-Time-Password, Security.

I. Introduction

Automated Teller Machine (ATM) is considered the commonest e-banking technology adopted by banks. This assertion was supported by the report of the Nigeria Interbank Settlement System (NIBSS) in its electronic payment factsheet for 2016, which disclosed that the value of cash withdrawals through ATMs rose sharply to 4.7 trillion, indicating appetite for cash transactions among Nigerians [1]. ATM is a computerized machine that provides customers of banks the facility of accessing their accounts for dispensing cash and to carry out other financial transactions without the need for a human cashier, clerk or bank teller [2]. It combines a computer terminal, recordkeeping system, and cash vault in one unit, permitting customers to enter a financial firm's bookkeeping system either with plastic card containing a personal identification number (PIN) or by punching a special code number into a computer terminal linked to the financial firm's computerized records 24 hours a day [3]. ATMs have been adopted by banks because they offer considerable benefits to both banks and their depositors. The most exciting experience for customers as well as bankers is that the ATM is replacing all the difficulties of bank transactions such as personal attendance of the customer, banking hour restrictions and paper-based verification [4]. It is quite easy to withdraw money from ATM instantaneously at any time. ATMs allow one to perform multiple banking functions such as withdrawal of cash, making balance enquiries, transferring money from one account to another, paying insurance premium, making small loans and payment of bills.

Notwithstanding the numerous benefits of ATM systems, security of customers' information has become a huge challenge and source of worry not only on the part of the banking industry but also to the customers. Criminals tamper with the ATM and steal users' credit card and password by illegal means [5]. ATMs eliminate the need for round-the-clock human involvement and tend to be located in places that make them more vulnerable to attack as they are often attractive targets for perpetrators [6]. Activities of card fraudsters has been on the increase, this is as a result of the growth of the number of ATM card holders, e-payment awareness and deployment of ATM cash points, [7]. The proliferation of identity theft among ATM users calls for a more reliable method of carrying out the validity of customers' identity. In conventional ATM systems, authentication of users' identity is performed using an ATM card and PIN. This method has some shortfalls as stolen cards can be used by unauthorized users to access customers' account details if the PIN is known to them. This is possible because many ATM users resort to the use of PIN that is simple and can

be remembered easily such as birthdays and social security numbers.

However, the introduction of three-tier authentication model to ATM system will in no small measure provide solution to the problem of identity theft which has bedeviled the conventional ATM. The use of password in place of PIN, biometrics identifier (fingerprint) and OTP to verify the validity of customers' identity at three different layers of authentication will provide a robust security. Biometric identifier is a biological authentication based on some physical characteristics of the human body [8]. Authentication with biometric is reliable and always available. This is because it cannot be lost, stolen, forgotten or forged. An OTP is a passcode that is valid for only one login session or one single transaction. It expires once it is used [9]. The most important advantage addressed by OTP is that it is not vulnerable to replay attack in contrast to static password. The use of three-tier authentication model will undoubtedly improve ATM security by eliminating the rate of card fraud, currency fraud and identity theft thereby restoring the confidence of customers on the use of ATM systems.

II. Related Works

Patil, Chandrekar, Chavan and Chaudhri [10] proposed an ATM system built on the technology of embedded system. It uses an 8-bit AT Mega 16 microcontroller developed by Microchip technology and the original verifying method (the use of PIN) to authenticate users. Reference [10] aimed at improving ATM security through the use of biometrics technology (fingerprint). This ATM system is related to the model presented (three-tier authentication model) in the use of biometric authentication. However, the system by [10] employed PIN authentication as a second factor authentication. The use of PIN is susceptible to replay attack and illegal access to customers' credentials. If a false acceptance rate error occurs with the fingerprint device, a criminal with the correct PIN of an account holder can easily access the customer's account illegally.

Jaynthi and Sarala [11] developed an ATM system that uses PIN for user authentication. The system sends an approval SMS alert to the corresponding mobile phone number of an account holder upon a successful authentication. An acceptance message received from the account holder grants access to the user else access is denied. Simultaneously, the image of the person who made the transaction is sent to the e-mail account of the bank and that of the account holder. If any misuse of card or ATM hijack occurs, the system automatically alerts both the bank manager and the police by switching on a buzzer. The system achieves this through the use of GSM technology and Internet communication network.

Iwasokun and Akinyokun [12] developed a fingerprint-based authentication framework for ATM. This ATM system is based on fingerprint authentication, eliminating the use of PIN and ATM card for authentication. The Internet serves as the operational environment and platform for the system. The thumbprint database of customers is available on the Internet. User verification involves enrollment, enhancement, feature extraction and matching. This work is related to the current study in the use fingerprint authentication. However, it has some defects such as the use of PIN as a means of authentication. The use of PIN is considered to be unreliable, in that if false acceptance rate occurs, the security of the system will be greatly compromised. Again, hosting sensitive information as customers' fingerprint database on the Internet could be risky as well since cybercrime has been prevalent in recent times.

Shimal and Jhunu [13] presented an enhanced ATM security system using two-level authentication where PIN and OTP were both used for user authentication. This second level authentication (the use of OTP) was employed if a customer wishes to exceed a specified withdrawal limit otherwise the customer is authenticated using only PIN. This ATM system operates in two modes. The first mode operates like the traditional ATM system when a customer-specified withdrawal limit is yet to be attained. The second mode is an enhancement on the traditional ATM system. It is only used when a customer wishes to exceed the withdrawal limit.

Malviya [14] developed an ATM authentication model which uses face recognition technique to authenticate users for improved security. The ATM system consists of embedded camera that recognizes the face standing about 2 feet far in front of the system and performs matches against the facial database. The findings of Mwaikali [15] identified insecurity as one of the major challenges facing ATM users in Tanzania.

III. The Proposed Three-Tier ATM Authentication Model

We developed and implemented a an ATM model using three-tier authentications adopting the Object-Oriented Analysis and Design Method (OOADM). The investigative phase of the OOADM was deployed as the paradigm for systematic study in order to obtain information on the current trends in the research area of ATM. The information obtained necessitated the definition of a high-level model (Fig. 1). Universal model language (UML) diagrams were also used to represent processes within system. The implementation of the three-tier authentication model for ATM was achieved using a combination of windows operating system, Microsoft Visual Basic.NET and Microsoft SQL Server.

The system uses three different layers of authentication to validate ATM users' identity to foster improved security. The three authentication mechanisms used are: password, biometric identifier (fingerprint) and OTP. The system is made up of alphabetic keys, numeric keys and some special character keys for authentication (Fig. 2). The ATM was interfaced with a fingerprint reader for improved security. In addition, the system also has a card reader, cash dispenser, screen, fingerprint scanner, and bank database. When the system is idle, a greeting message is displayed, the keys on the keypad remain

inactive until a bank card has been inserted.

A. Customer Registration

To perform a transaction, a customer is expected to undergo a registration process in order to obtain an ATM card. During the registration, the customer's personal detail is taken including the mobile phone number where OTP will be sent to. Fingerprint enrollment of customers is also carried out during registration and stored in the bank database together with other personal details. At the end of the registration process, the customer is issued an ATM card and a passcode which has to be changed to password of choice.

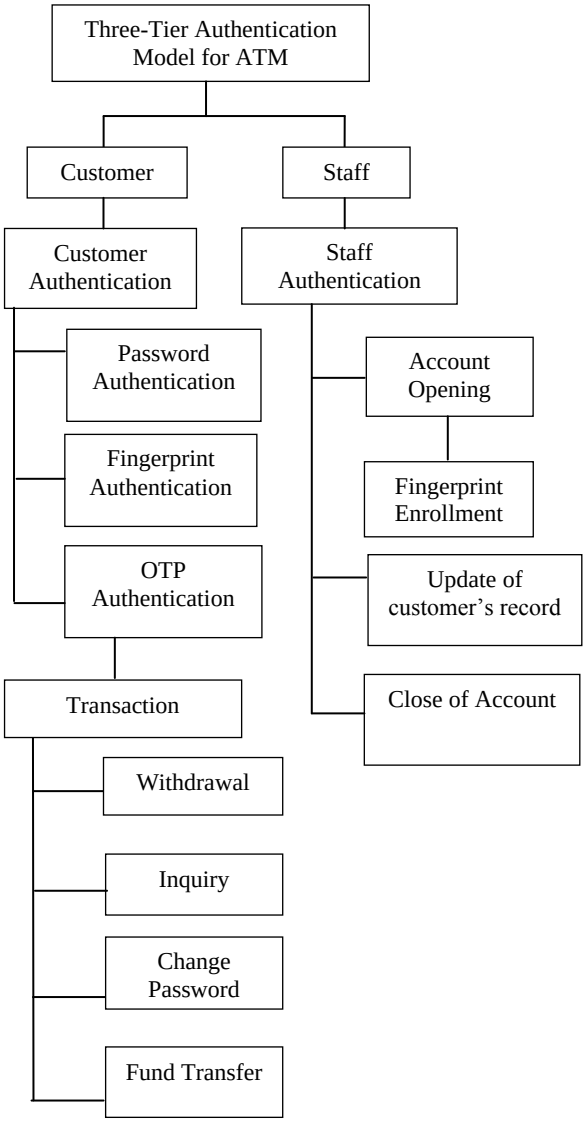

Fig.1. High Level Model of the Proposed System

B. User Authentication

The system proposes character password and OTP of more than four (4) characters. In this system and for the purpose of demonstration, a six-character password and an eight-character OTP were used. At the ATM, the customer inserts an ATM card into the card reader slot, after card validation, the system prompts that password be supplied by the customer which will be displayed on a screen. This is the first level of authentication; the customer uses the keypad to input six (6) alphanumeric characters as password.

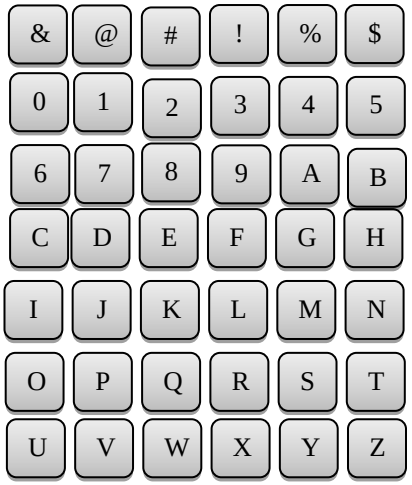

Fig.2. Alphanumeric Keypad

This is one of the distinguishing features of the proposed system. The system validates the password by comparing it with the one encoded on the card, if there is a match, the user proceeds to the second level of authentication which is the use of biometric identifier (fingerprint). A fingerprint is provided by the customer using the fingerprint scanner. The system compares the fingerprint with the one encoded on the card, if there is a match the user is provided with the final stage of authentication, which is the use of OTP. The customer is required to enter eight (8) characters OTP generated by the system and sent to the customer's mobile phone. If the OTP is correct and entered within the specified time limit, the customer is authenticated and granted access to perform the transaction of choice which could be withdrawal, change of password, balance inquiry or transfer of fund. The transaction goes through a network and connects to customer's' account in the bank's database. The cash dispenser provides cash to the customer in the case of withdrawal transaction, if the customer wishes to perform no other transaction, a transaction receipt is printed and card ejected.

C. Modeling the Functions of the Proposed System

Use case modeling was used to model the functions of the system in terms of business events, who initiated the events, and how the system responds to the events. The use case models of the proposed system are shown in Fig. 3a. and Fig. 3b.

D. Justifcation of the Proposed Three-Tier Authentication Model

1. The system provides strong security with the use of biometric identifier and alphanumeric characters for password. This password becomes very difficult if not

impossible to be guessed correctly by fraudsters
2. ATM card theft will be reduced since a person's biometric is not transferrable. This is required before a successful authentication process.
3. The level of security provided by the system will make it impossible for would-be perpetrators. This will discourage ATM fraud.
4. The problem of replay attack is completely eliminated with the use of OTP.
5. Customers' confidence will be restored on the use of ATM to meet their banking needs

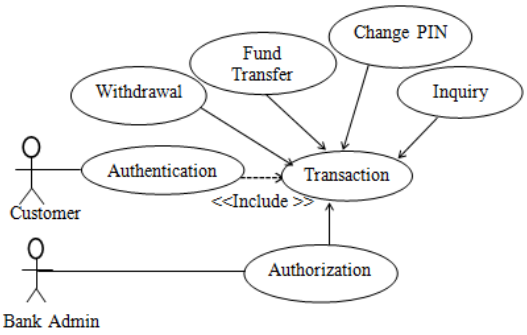

Fig.3a. Use Case Model of Events Initiated by Customers

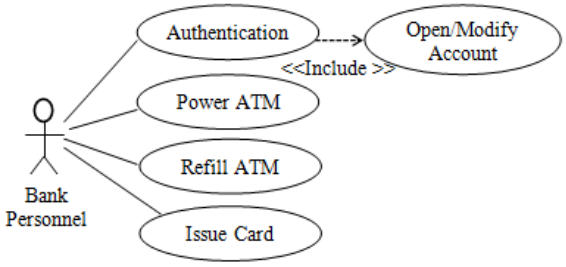

Fig.3b. Use Case Model of Events Initiated by Bank Personnel

IV. Design of the Three-Tier Authentication Model

Three-Tier Authentication Model seeks to design an ATM system with three layers of authentications – the use of password, fingerprint and OTP. Therefore, the system is interfaced with a fingerprint scanner for biometric authentication and it is capable of generating token as OTP. In addition, the system introduced alphabets and special characters to the existing numeric keypad of an ATM system. The design is aimed at providing robust security to the existing card-based ATM system by eliminating the problem of identity theft through the introduction of password as a substitute for PIN, and the use of fingerprint and OTP for second and third tier- authentication respectively.

A. High Level Model (HLM) of the System

The HLM of the system (Fig. 1) presents the primary list of the system components from which the subsystems evolved. The proposed system is a complex one, hence, the need to break the system into subsystem for easy manageability.

B. CusomerSubsystem

The Three-Tier Authentication Model consists of the customer and staff subsystems respectively as depicted in Fig. 1. The customer subsystem enables a customer to perform transactions such as withdrawal, fund transfer, balance inquiry and change password. However, before a customer can perform any transaction, the customer must undergo authentication to avoid unauthorized access to customers' account details. The customer authentication subsystem handles the authentication process. The first level of authentication involves the use of six-character password, which is a combination of numbers, alphabets and special characters. The interface is shown in Fig. 4.

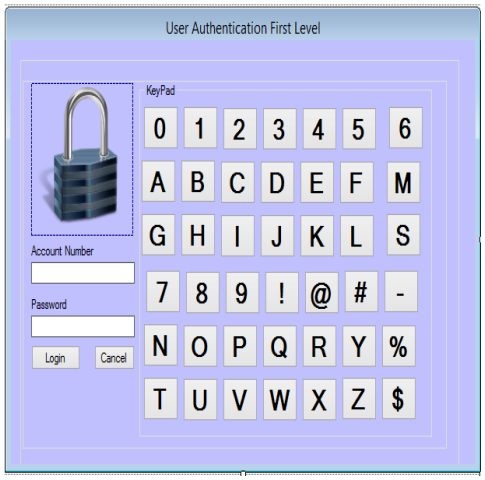

Fig.4. First-Tier of User Authentication

If there is a match with the password encoded on the customer's card, the customer is prompted with the second level of authentication which is the use of fingerprint.

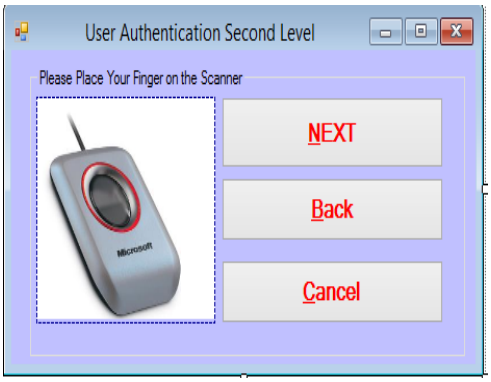

Fig.5. Second-Tier of User Authentication

The customer at this level provides a live fingerprint template using the fingerprint scanner attached to the ATM system. The fingerprint interface is depicted in Fig. 5. If there is a match with the one encoded on the card an OTP will be generated automatically and sent to the customer's mobile phone. The customer will be prompted with the last level of authentication to supply the eight-character OTP received using the interface as shown in Fig. 6.

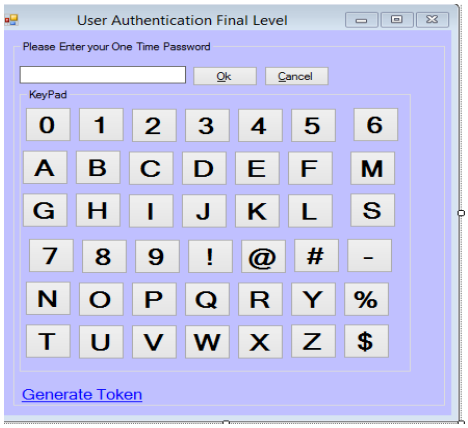

Fig.6. Third-Tier of User Authentication

If the OTP entered is correct the customer will be granted access to perform transaction of choice. However, at every level of authentication, if a customer supplies a wrong parameter (password, fingerprint template or OTP), two more attempts will be granted to the customer to provide the correct parameter else the session will be terminated and card ejected.

C. Staff Subsystem

The staff subsystem enables the bank personnel to perform ATM related tasks. Bank personnel must be authenticated before having access to the system. The bank personnel authentication interface is shown in Fig. 7.

Fig.7. Bank Personnel Authentication

The bank personnel are saddled with the responsibility of opening a new account for customers, registering customers for ATM usage and issuance of ATM cards. Customers' details collated by the bank personnel are stored in the bank's database. Account opening interface is shown in Fig. 8.

D. Transaction Subsystem

The transaction subsystem handles different transactions that can be performed by a customer. The interface is shown in Fig. 9. If a withdrawal transaction is selected, the user will be asked to specify the amount to be withdrawn. If the account contains sufficient fund, the fund will be dispensed to the user through the cash dispenser.

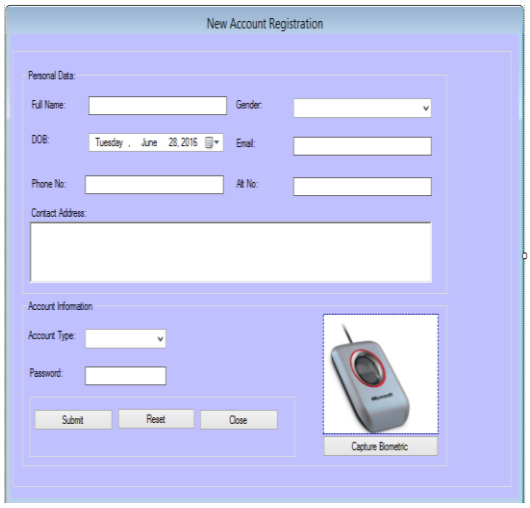

Fig.8. Account Opening Interface

In the case of balance inquiry, the user will be asked to specify the account whose balance is requested, the balance will be displayed on the screen. In fund transfer transaction, the user will be asked to specify the account and bank in which the fund is to be transferred to and the amount to transfer. For change of password transaction, the user specifies the old password, the new password and confirms the new one for change to be effected.

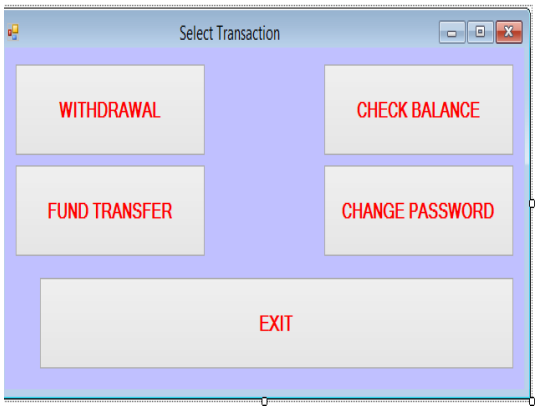

Fig.9. Transaction Module

E. Database

The database development tool used in the study is Microsoft SQL Server. It is a software product with the primary function of storing and retrieving data. The system proposed contains tables in the database, relationship among tables were created because a database consisting of independent and unrelated tables serves little purpose, this can lead to data redundancy and update inconsistency. The database used by the proposed ATM system stores customers account details.

F. Algorithm

Insert ATM card
DO WHILE count <= 3
PRINT 'Enter Account number'
PRINT 'Enter Password'
IF Password = 'Password' And Account number =

```
        'Account number' THEN
        PRINT 'Capture fingerprint'
  IF fingerprint ='fingerprinttemplate' THEN
        PRINT 'Enter OTP'
  IF OTP = 'OTP passcode' THEN GOTO 50
50      PRINT 'Select Option'
REPEAT PRINT '1. Make withdrawal'
        PRINT '2. Make inquiry'
        PRINT '3. Change password'
        PRINT '4. Transfer fund'
        PRINT '5. Quit'
   IF Option = 1 THEN
        PRINT 'Enter amount to withdraw'
        Balance = Balance – amount
    ELSEIF Option = 2 THEN
        PRINT 'Your Balance' = Balance
    ELSEIF Option = 3 THEN
        PRINT 'Enter new Password'
        PRINT 'Confirm Password'
   IF Newpassword = Confirmpassword THEN
        PRINT 'Password change successful'
   ELSEIF Option = 4 THEN
        PRINT 'Enter receiver's account number'
        PRINT 'Enter Amount'
UNTIL Option = 5
STOP
```

V. Results

The result of the proposed Three-Tier Authentication Model for ATM a system with improved security, interfaced with a fingerprint scanner for biometric authentication and an ATM keypad with a modified form factor. The incorporation of alphabets and special character keys to the existing numeric keys changed the form factor of the keypad. The system is also capable of generating OTP for third-tier authentication to eliminate any possibility of replay attack. The system was evaluated alongside the existing system in terms of speed and the level of security each provides.

A. Security

The existing systems employ only one means of verifying customers' identity. In the case of identity theft, where a successful guess is made on a customer's PIN by fraudsters or where customers' debit cards and PINs are stolen or forcefully taken from them, cash are withdrawn from the ATM through illegal means. This undoubtedly leads to huge financial loss to both the customer and the bank.

However, the new system provides improved security on ATM system by employing the use of three different authentication mechanisms. The essence is to cover up every loophole which could lead to identity theft. It is obvious that the three security protocols can never fail at the same time, hence, eliminating the problem of identity theft completely.

Again, to prove the level of security the new system provides, different wrong passwords, OTPs and fingerprint templates were tried on the system but access was denied in all cases. This is an indication that the new system provided robust security and cannot be hacked by criminals whose aim is to withdraw customers' cash illegally in a short time.

B. Speed

Time taken to complete user authentication was collated for two categories of users who underwent authentication three times both in the existing system and the proposed system. The result was tabulated as shown in Table 1 and represented using a line chart in Fig. 10.

Table 1. Time Taken to Complete Authentication in both the Existing System and the Proposed System

	User 1	**User 2**	**User 3**
Group A	15 Secs	20 Secs	30 Secs
Group B	40 Secs	53 Secs	87 Secs

Group A in Table 1 represents the existing system while Group B represents the proposed system. Three categories of users performed experiment with both systems to determine the total time it takes each user to complete authentication process in both systems. The result is presented (Fig. 10).

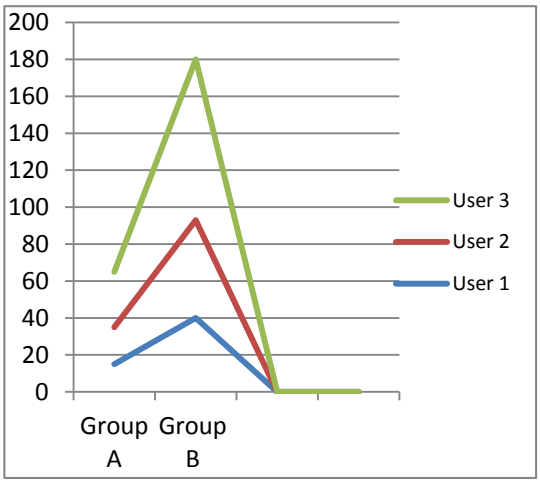

Fig.10. Line Chart of the Time Taken to Complete Authentication Process in both the Existing System and the Proposed System.

Comparing the results from Table 1 and Fig. 10, it is evident that authentication process is faster with the existing system than the proposed system. It takes more time to be authenticated in the proposed system. This is as a result of three levels of authentication compared to one level of authentication in the existing system. It is important to note that security cannot be traded for speed.

VI. Conclusion

The problem of identity theft, unauthorized access to customers' account details and illegal withdrawal of cash from the ATM will be completely eliminated with the adoption of the proposed Three-Tier Authentication Model as the current use of PIN for ATM user's

verification and identification is marred with some level of insecurity. This Three-Tier Authentication Model uses password, biometric identifier and OTP to verify the validity of user's identity at three different layers of authentication. These three authentication mechanisms must be in the affirmative before access is granted to the user. The adoption of the new system by financial institutions will strengthen the security of ATM systems and restore the confidence of customers. The study will no doubt foist a sense of futility on would-be perpetrators. This will discourage ATM fraud. Bank customers are reassured that their account details and cash cannot be tampered with, hence, better service delivery which will attract many customers to use ATM.

REFERENCES

[1] B. Komolafe (2017, Jan.). Nigerians withdraw N4.7 trillion through ATM in 2016 [Online]. Available: Http://www. vanguardngr.com/2017/01/nigerians-withdraw-n4-7-trillion-atms-2016.

[2] N.Y. Asabere, R.O. Baah and A.A. Odefiya, "Measuring standards and service quality of Automated Teller Machines (ATMs) in the banking industry of Ghana," *International Journal of Information and Communication Technology Research*, vol 2, issue 3, pp 216– 226, 2012.

[3] P.S. Rose and S.C. Hudgins, Management and Financial Services, 9th ed. New York: McGraw-Hill, 2013.

[4] J. Hota. (2012) "Window-based and web-enabled ATM: issues and scopes," The IUP Journal of Information Technology, vol. 3, issue 4, pp 52-59. Available: http://www.academia.edu/5043734 /windows-based-and-web-enabled-ATMs-issues-and-scopes

[5] H.A. Hayder (2011) "Implementing additional security measure on ATM through biometric [Online]. Available: http://www.etd.uum.edu.my/2576

[6] Diebold Incorporated (2012). ATM fraud and security. [Online]. Available: http:// securens.in/pdfs/KnowledgeCenter /5_ATM %20Fraud% 20and%20Security.pdf

[7] S.A. Adelewo. (2010, August). "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. 5, issue 2, pp 10-20. Available: http://www.arraydev.com/ commerce /jibc

[8] S.T. Bhosale and B.S. Sawant, "Security in e-banking via cardless biometric ATMs," International Journal of Advanced Technology and Engineering Research *(ITATER)*, vol. *2* issue 4, pp 9-12, July 2012.

[9] Gemalto (2011, Feb). One-Time-Password Solution for Secure Network Access. [Online]. Available: http://www.gemalto.com/brochures-site/download-site/Documents/ent_otp_secure _access.pdf

[10] B. Patil, B.S. Chandrekar, M.P. Chavan and B.S. Chaudhri, "RBI 3X – fingerprint based ATM," *International Journal of Advanced Research in Computer and Communication Engineering*, vol. 5, issue 3, pp 577 – 581, March 2016.

[11] P. Jaynthi and S. Sarala, "Enhanced ATM security using differentiated passwords with GSM technology," *International Journal of Innovative Research in Engineering & Science*, vol. 5, issue 4, pp 28 – 35, May 2015.

[12] G.B. Iwasokun and O.C. Akinyokun. (2013) "A fingerprint-based authentication framework for ATM," *Journal of Computer Engineering and Information Technology*, vol. 2, issue 3. Available: http/dx.doi.org/ 10.4172/2324-9307.1000112.

[13] D. Shimal and D. Jhunu. (2011). "Designing a biometric strategy (fingerprint) measure for enhancing ATM security in Indian e-banking system," *International Journal of Information and Communication Technology Research*, vol. 1, issue 5. Available: http://www.esjournals.org

[14] D. Malviya. (2014, Dec.). "Face recognition technique: Enhanced safety approach for ATM," *International Journal of Scientific and Research Publications*, vol 4, issue 12. Available: http://www.ijsrp.org

[15] E.J. Mwaikali, "Assessment of challenges facing customers in Automated Teller Machine in the banking industry in Tanzania: A case of some selected banks in Tanzania," *International Journal of Research in Business and Technology*, vol. 4, issue 3, pp 480-488, 2014.

Authors' Profiles

Moses O. Onyesolu: Has Ph.D. (Virtual Reality), M.Sc. B.Sc. (Computer Science) from Nnamdi Azikiwe University, Nigeria where he works as a lecturer and researcher. He was the Head, Department of Computer Science, Nnamdi Azikiwe University (October, 2014 to January, 2017).

His research interests are mainly in computer modeling and simulation, e-learning/virtual reality technologies, software engineering and queueing system/ theory and its applications. He has published widely in those areas. He is a member of the following learned societies: Nigerian Computer Society (NCS), Computer Professionals (Registration Council of Nigeria)(CPN), and International Association of Engineers (IAENG), International Association of Computer Science and Information Technology (IACSIT) and European Association for Programming Languages and Systems (EAPLS).

Amara C. Okpala: Has M.Sc. PGD. (Computer Science) and B.Sc.(Ed) (Computer Education) from Nnamdi Azikiwe University, Nigeria. She is a staff of Independent National Electoral Commission (INEC), Nigeria, where she works as a System Analyst in the Department of Information Communication Technology (ICT).

Her research interests are mainly in Software Engineering, Database Administration and Information Security.

How to cite this paper: Moses O. Onyesolu, Amara C. Okpala,"Improving Security Using a Three-Tier Authentication for Automated Teller Machine (ATM)", International Journal of Computer Network and Information Security(IJCNIS), Vol.9, No.10, pp.50-56, 2017.DOI: 10.5815/ijcnis.2017.10.06

