Three-Factor Authentication for Automated Teller Machine System

Jane Ngozi Oruh
Department of Computer Science,
Michael Okpara University of Agriculture,Umudike,
Umuahia, Nigeria.
ngozibenphilips@gmail.com

Abstract – This paper discusses three-factor authentication for the Automated Teller Machine system; pointing out the security vulnerabilities in the two-factor authentication method of the ATM system where password (PIN) and smartcard (ATM card) are currently used for banking transaction authentication. It was seen from the study presented here, that two-factor authentication has not provided effective security for the ATM system. A proposal was made for a system that will integrate biometric authentication as a third level authentication in the system, creating a three-factor authentication ATM system that includes user smartcard, user PIN and user fingerprint information.

***Keywords:** Three-factor, ATM, Biometric-Authentication*

I. INTRODUCTION

In the current ATM system where what obtains is two-factor authentication, security can be breached when password is divulged to an unauthorized user or card is stolen by an impostor. Reference [4] states that ATMs have been incorporated in our way of life. They offer real convenience to those on the run, but this advantage can be undone if customers do not feel secure when using the facilities. Moreover, they are prone to fraud, and offer some elements of risk.

Furthermore, simple passwords are easy to guess by any impostor while difficult password may be snooped using sophisticated techniques; therefore, this system is not secure. Having the first two security mechanisms (two-factor authentication) in place might not be enough. However, it is based on this argument that adding a third level authentication can provide significant authentication strength by relying on something that the user 'is'. This means something about that person that cannot be changed and easily mimicked, such as fingerprints, facial features or eyes, which can be used as a factor of identity verification, hence three-factor authentication. Three-factor authentication is the use of three independent mechanisms for authentication. To solve this problem, we added fingerprint verification to this method. Fingerprint Verification System is an easy-to-use library that allows programmers to integrate fingerprint technology into their software without specific know-how.

A. PROBLEM STATEMENT

As ATM technology evolves, fraudsters are devising different skills to beat the security of the system. Various forms of frauds are perpetuated, ranging from; ATM card theft, skimming, PIN theft, card reader techniques, PIN pad techniques, force withdrawals and lot more [18]. Also, [18] further posits that managing the risk associated with ATM fraud as well as diminishing its impact is an important issue that faces financial institutions as fraud techniques have become more advanced with increased occurrences. Smartcard-based password authentication provides two-factor authentication, namely; a successful login that requires the client to have a valid smartcard, and a correct password or PIN. While it provides stronger security guarantees than just password authentication, it could also fail if both authentication factors are compromised (e.g., an attacker has successfully obtained the password and the data in the smartcard). In this case, a third authentication factor can alleviate the problem and further improve the system's assurance. This motivates the three-factor authentication, which incorporates the advantages of the authentication based on PIN, smartcard and biometrics [17].

II. ATM FRAUD

Reference [1] identified security as well as power outage as major challenges facing the ATM users in Nigeria. Reference [8] expressed concern about the lack of cooperation among banks in the fight to stem the incidence of ATM frauds now plaguing the industry. He expressed that the silence among banks on ATM frauds makes it difficult for banks to share vital information that will help curb the menace. Reference [12] blamed the menace of ATM frauds on indiscriminate issue of ATM card without regard to the customer's literacy level. According to him one of the frequent causes of fraud is when customers are careless with their cards and PIN as well as their response to unsolicited e-mail messages to provide their card detail. Reference [14] opined that the current upsurge and nefarious activities of Automated Teller Machine (ATM) fraudster is threatening electronic payment system in the nation's banking sector with users threatening massive dumping of the cards if the unwholesome act is not checked.

Reference [13] citing A Report on Global ATM Frauds, 2007 identified the following types of ATM Frauds:

(a) Shoulder Surfing: This is a fraud method in which the ATM fraudster use a giraffe method to monitor the information the customer keys in into the ATM machine unknown to the customers.

(b) Lebanese Loop: This is a device used to commit and identify theft by exploiting Automated Teller Machine (ATM). Its name comes from its regular use among Lebanese financial crime perpetrators, although it has now spread to various other international crime groups.

(c) Using Stolen Cards: This is a situation in which the ATM card of a customer is stolen and presented by a fake presenter.

(d) Card Jamming: Once the ATM card is jammed, fraudster pretending as a genuine sympathizer will suggest that the victim re-enter his or her security code. When the card holder ultimately leaves in despair the fraudster retrieves the card and enters the code that he has doctored clandestinely.

(e) Use of Fake Cards: Fraudsters use data collected from tiny cameras and devices called 'skimmers' that capture and record bank account information.

(f) Duplicate ATMs: The fraudsters use software which records the passwords typed on those machines. Thereafter duplicate cards are manufactured and money is withdrawn with the use of stolen Passwords. Sometimes such frauds are insiders' job with the collusion of the employees of the company issuing the ATM Cards.

(g) Card Swapping: This is a card theft trick whereby a fraudster poses as a "Good Samaritan" after forcing the ATM to malfunction and then uses a sleight of hand to substitute the customer's card with an old bank card. As the customers is endlessly trying to push the card through, the fraudster offer assistance by pretending to help the customer push through the card.

Reference [3] in their study concluded that the location of ATM is a high determinant to fraud or crime carried out at ATM point. From their research over 75% of the respondents affirm that the location of ATM in secluded place contribute to the fraud perpetuated at ATM point. ATM within the banking premises is more secure than ATMs outside the bank premises. Also, it is obvious that the location of ATM in attractive place does not make it prone for fraud. Reference [6] states that the major form of ATM fraud is PIN theft which is carried out by various means; skimming, shoulder surfing, camera, keypad recorder etc. This study elucidates that the common type of fraud perpetuated is PIN theft which is mostly as a result of congestion at ATM points. Other forms of fraud that were enumerated by respondents were; force withdrawal, card theft, and skimming and congestion method fraud at ATM.

Reference [5] states that the 24 hours access to the ATM machine is a double edge sword, it has both advantage and disadvantage. It is easy to deduce that ATM fraud is carried out most in the day time. Also there are occurrences at night but most ATM users prefer to make withdraw during the day thus preventing incidences of robbery at night.

A. AUTHENTICATION

Authentication is the process of determining whether someone or something is, in fact, who or what it is declared to be. In private and public computer networks (including the Internet), authentication is commonly done through the use of logon passwords. Knowledge of the password is assumed to guarantee that the user is authentic [10].

Reference [16] defines authentication as the act of confirming the truth of an attribute of a single piece of data or entity. In summary, user authentication is a means of identifying the user and verifying that the user is allowed to access some restricted service; for example, a user must be identified as a particular student with an assigned property in the form of a registration number in order to have access to their student information.

Two-factor authentication

This is a security process in which the user provides two means of identification, one of which is typically a physical token; such as a card and the other of which is typically something memorized, such as security code [10]. This is also called strong authentication. It may also be any two of the following;

- Something known, like a password,
- Something possessed, like your ATM card, or
- Something unique about your appearance or person, like a fingerprint.

When the confidentiality of information is particularly needful, the use of two-factor authentication may not guarantee enough protection. A stronger means of authentication, something that is more difficult to compromise is necessary. This is what we hope to achieve with the three-factor authentication model.

Three-factor authentication

This includes something you know, something you have and something you are [7]. It involves the use of three independent variables for authentication, which will normally include the following;

- Password (something known only by an individual i.e. password, passphrase or PIN)
- ATM card (token held by an individual)
- Fingerprint (something the individual only, is).

The use of three-factor authentication improves the security of any given system, making it almost impossible for attackers and hackers to break into the system without specialized aid.

Biometric authentication

Biometric authentication is one of the most exciting technical improvements of recent history and looks set to change the way in which the majority of individuals live. According to [2], biometric systems recognize individuals based on their anatomical traits (fingerprint, face, palm-print, iris, voice) or behavioral traits (signature, gait). Before now, [9] had already proposed a two ID-based password authentication scheme where users are authenticated by smartcards, passwords and fingerprints. Biometric authentication is built on the fact that no two individuals can share the same morphological characteristics. Reference [15] presents integration of two technologies, namely biometrics and smartcard to meet some of the technical challenges posed in a network-based authentication system. Biometrics provide the accuracy needed by these systems with smartcards providing security far beyond the magnetic strip cards. By combining the two, the overall system requirements are better met than each of them individually.

In all, biometrics in general – especially fingerprint technology in particular, can provide a much more accurate, secure and reliable user authentication method especially for the proposed three-factor authentication system for ATMs.

III. NEW SYSTEM DESIGN

The proposed new ATM system will comprise three input devices. The input devices include card reader, keypad and fingerprint sensor. They provide interface through which authentication will be done.

Card Reader

The card reader reads data from the smartcard (ATM card) and is part of the identification of a particular account. The ATM card provides the first level authentication for the user. A magnetic strip on the reverse side of the ATM card is used for connection with the card reader. The card is swiped or pressed on the card reader which captures the card information. The captured information from the card is passed on to the ATM processing server. This server uses the captured card information to get the account information of the card holder.

Keypad

The keypad provides an interface for ATM users to key in their PIN into the system. The PIN is the second level authentication coming after the smartcard. The PIN is transmitted in encrypted form to the ATM server which checks the correctness of the PIN. When this check returns positive, the machine prompts the user to complete the third factor authentication which is the fingerprint information.

Fingerprint Sensor

The fingerprint sensor provides the last level of authentication for the user. Users only need to place their finger on the scanner for the fingerprint information to be captured. Once captured, the information is encrypted and transmitted to the ATM server. The ATM server matches the fingerprint information with the one stored on the database (the template). If a match is confirmed, the server establishes a connection with the customers' bank server and subsequently opens transaction interaction with the customer via the ATM display screen. On the ATM display screen, the customer can select and perform any transactions of their choice.

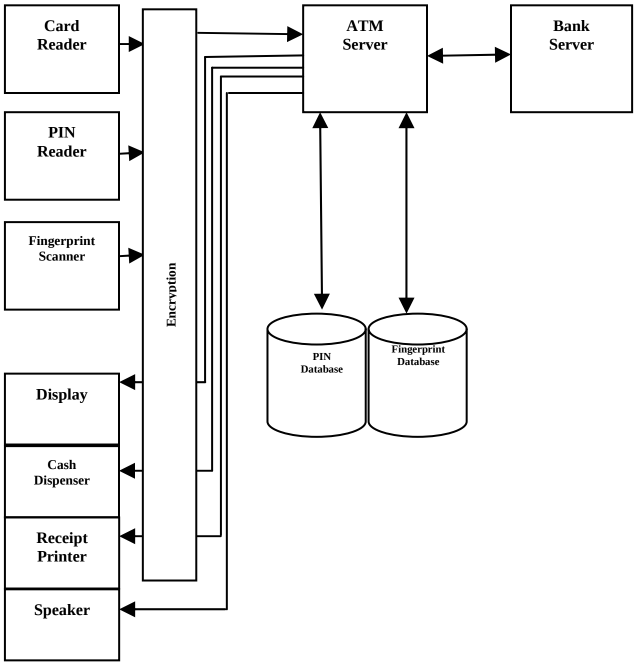

Fig. 1 Architectural diagram of the proposed ATM system

A. AUTHENTICATION ALGORITHM

The authentication algorithm for the proposed system follows a simple process as explained below;

1. User inserts the smartcard (ATM card) on the card slot. The card reader reads the card information and transmits the encrypted card information to the ATM server.

2. The ATM server decrypts the card information to get user's account detail; and subsequently prompts the user through the ATM display screen to supply their PIN.

3. The user keys in their PIN using the keypad, the PIN is encrypted and transmitted to the ATM server.

4. The ATM server decrypts the PIN and checks with the PIN database for the correctness of the PIN; and if correct prompts the user to supply their fingerprint information through the display screen or return "invalid PIN" if not correct and subsequently requests user to retype their PIN.

5. User places their finger on the fingerprint sensor to take a scan. The fingerprint reader processes the fingerprint information, encrypts it and transmits it to the ATM server.

6. The ATM server checks with the fingerprint database for correctness of the information; and if correct establishes a connection with the User's bank for transaction operations or returns "invalid fingerprint" and subsequently takes the user to algorithm number 3.

7. When the first transaction is completed, user only needs to supply their fingerprint information to perform another transaction so long as the card has not been ejected.

8. When user completes their entire transactions, the card is ejected and the operations are terminated.

B. BIOMETRIC SYSTEM OPERATION

The biometric system will normally comprise the biometric sensor (camera or scanner), the biometric processor (device and software algorithm that process the biometric information), the cryptographic module and the biometric information database. The biometric sensor is integrated in the ATM machine while the biometric database is integrated in the ATM server. Also, the biometric processor and the cryptographic module are integrated both in the ATM machine and the ATM server.

Biometric Enrollment

During card registration also called biometric enrolment, a new user supplies their biometric information to the biometric system. The biometric sensor captures and sends the information to the ATM client-side biometric processor. The client-side biometric processor processes the information, and with the help of the cryptographic module, encrypts and transmits the encrypted information over the network to the ATM server-side processor. The server-side processor decrypts and processes the encrypted information and extracts some unique features such as fingerprint minutiae using a software algorithm called feature extractor. Other identifiers (name and identification number) are added and sent to the biometric database for storage as a template. This completes the biometric enrollment.

In this work, we have proposed four-finger enrollment, meaning a new user will have to supply fingerprint information for their two thumbs and two index fingers. This limits the probability of a denial of service due to system errors or mild fingerprint changes.

During authentication, when the system returns a mismatch for the first finger, users can choose to try any of the other three fingers.

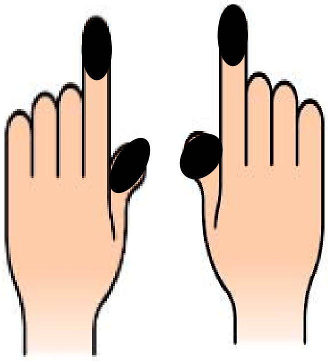

Fig. 2 Thumbs and index fingers for biometric capture

C. USER THIRD-FACTOR AUTHENTICATION

During biometric authentication referred to as user third-factor authentication, a user presents new biometric sample information to the biometric system through the sensor. The client processor processes the biometric information and with the cryptographic module encrypts the information and sends it to the server side processor. At the server side processor, the supplied information is decrypted and processed. The unique features together with the name and identification number are extracted and placed on the sample memory map. The server side processor then queries the biometric database with the sample name and identification number. The requested templates are supplied and placed on the template map. The processor now uses a biometric matcher to compare the sample and all four templates associated with the user for similarities. The matcher returns a match score representing the degree of similarity between the closest template and the sample. The system accepts the identity claim only if the match score is above a predefined threshold.

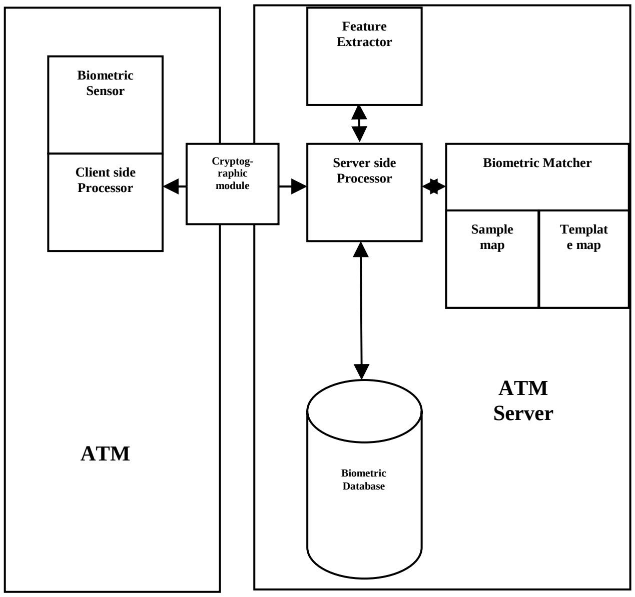

Fig. 3 Macro model of the proposed biometric authentication system

IV. LIMITATIONS OF BIOMETRIC AUTHENTICATION

Though biometrics as a third factor authentication for the ATM system adds improved security to the system, it does have its own problems. Reference [2] named the two authentication errors that are mainly seen in biometric systems to include false nonmatch and false match. They further explained that false match occurs when two samples from the same individual have low similarity that the system cannot correctly match them, while false match occurs when two samples from different individuals have high similarity that the system incorrectly declares them as a match. The former case results in a Denial of Service to a legitimate user while the later results in intrusion into the system by an unauthorized user.The system proposed here adopts four-finger enrollment, making it more difficult for a denial service to occur.

Similarly, the fact that we are adopting a three-factor authentication system in our model means that an impostor will need to have the smartcard, the user PIN and hope that a false match occurs to be able to break into the system. This decreases the chances of an impostor breaking into the system.

V. CONCLUSION

Biometric-based authentication offers several advantages over other authentication methods such as passwords, passphrase and PINs. This is so because, the fraudster may match everything but may never match the biometric peculiarities. Biometric tokens are the safest means of preventing ATM fraud. By further integrating biometric authentication in the ATM system as a third-factor authentication, we are sure that attackers, impostors and fraudsters as the case may be, would have a difficult time breaking into peoples' accounts.

Though there exists a probability of a possible compromise of the system, the attacker would have to weigh the attack-resources needed to achieve this with the possible gain; and because our proposed system offers extremely high attack-resources to gain ratio, such efforts may well be an exercise in futility.

The massive adoption and implementation of the system proposed here will go a long way in solving our ATM security needs.

REFERENCES

[1] Adeloye, L.A., "E-banking as new frontiers for banks," *Sunday punch* (Nigeria), 14 September, 2008 P.25.

[2] Anil K. Jain and Karthik Nandakumar, "Biometric authentication: system security and user privacy," Published by the IEEE Computer Society, November, 2012.

[3] Brunner, A., Decressin, J. & Kudela, B., "Germany's three-pillar banking system – cross country perspectives in europe," Occasional Paper, International Monetary Fund, Washington DC., 2004.

[4] Chris, E. M., "ATM machine security: bank ATM security advice," retrieved October 15, 2014 from http://www.crimedoctor.com/business.htm

[5] Cynthia, B., "The measurement of white-collar crime using Uniform Crime Reporting (UCR) Data," S department of Justice, Federal Bureau of Investigation, New York, 2000.

[6] Diebold, I., "ATM fraud and security: White Paper," New York. Hsu C.T. and Wu J.L. (1999):Hidden Digital Watermarks in Images *IEEE Transactions on Image Processing* vol.8,No.1, pp 58-68, 2006.

[7] Frogtalk technology news, 3 "Factor authentication: why you need it to protect your business," retrieved

Aug 15, 2014 form http://www.ribbit.net/frogtalk/id/121/3-factor-authentication-why-you-need-it-to-protect-your-business

[8] Ihejiahi, R., "How to fight ATM fraud online," *Nigeria Daily News (*Nigeria), 21 June, 2009 P. 18, June 2009.

[9] Kim, H.S. Lee, J.K. and Yoo, K.Y., "ID-based Password Authentication Scheme Using Smart Cards and Fingerprints," ACM SIGOPS Operating Syst. Rev., vol. 37, no. 4, pp. 32-41,Oct. 2003.

[10] Margaret R., retrieved Oct 10, 2014 from http://www.searchsecurity.techtarget.com/definition/two-factor-authentication

[11] Margaret R., retrieved Oct 12, 2014 from http://www.searchsecurity.techtarget.com

[12] Obiano, W., "How to fight ATM fraud," Online Nigeria *Daily News*, 21 June, 2009 http://www.Krepublishers.com/02-Journals/JSS/JSS-27-000011-Web/JSS-27-1-000-11

[13] Olabode J. A., "Automated teller machine (atm) frauds in nigeria: the way out," 2011.

[14] Omankhanlen O., "ATM fraud rises: Nigerians groan in Nigeria," *Daily News*, Sunday (Nigeria), 21 June, 2009 P. 8-10

[15] Ratha, N.K. and Bolle R.M., "Smart card based Authentication," *IBM Systems Journal*, retrieved August 2014 from http://www.cse.msu.edu/~cse891/Sect601/textbook/18.pdf

[16] Wikipedia, "Authentication," retrieved Oct 12, 2014 from http://en.wikipedia.org/wiki/Authentication

[17] Xinyi Huang, Yang Xiang, Ashley Chonka, Jianying Zhou, and Robert H. Deng, "A Generic framework for three-factor authentication: preserving security and privacy in distributed systems," IEEE Transactions on parallel and distributed systems 2010

[18] (Selina O. et al, 2012)

AUTHORS' PROFILE

Jane Oruh received a bachelor's degree in Computer Science from Michael Okpara University of Agriculture, Umudike (MOUAU), Abia State, Nigeria, in 2005. She received her M.Sc in Computer Science from Ebonyi State University, Abakaliki in 2013. She is currently an Assistant Lecturer with the Computer Science department of Michael Okpara University of Agriculture, Umudike, Nigeria. Her research interests are information Security, biometric authentication systems and context aware systems.

I.