SECURITY VIOLATION MANAGEMENT FOR ATMS TRANSACTIONS IN THE BANKING SECTORS USING BIOMETRIC FINGERPRINTS

Mbachu, C. B. and Ogamba, M. O.

Department of Electrical/Electronic Engineering, Chukwuemeka Odumegwu Ojukwu University, Uli, Anambra State, Nigeria

ABSTRACT

Fingerprints, an impression left by the friction ridges of a human finger are an important part of the studies of forensic science. They are deposited and left everywhere on suitable surfaces (such as: glasses, metals, and/or polished surfaces) by some natural secretions of sweat from the eecrine glands that are present in the epidermal ridges. Involving or adopting the use of fingerprints into the banking sector for the security of ATMs and customers would go a longer way in playing a critical role in preventing attacks on the banks and customers. This can equally lead to check-mating the loop-holes and vulnerabilities that are linked to the bank-ATM frauds. Banks must meet and employ certain standards so as to ensure a safer banking environment. This paper focuses on the flaws and the increasing waves of criminal activities taking hold on ATMs (Automated Teller Machines) where quick cash in transit is the primary target on the customers. A biometric means as the measure of enhancing this security has emerged from the discourse.

Keyword: Security, ATM, Crime, Biometrics

1.0 INTRODUCTION

Automated teller machine is a mechanical device that has its roots embedded in the accounts and records of a banking institution. It is a machine that allows the banks customers carry out banking transactions like, deposits, transfers, balance enquiries, and withdrawal. Notwithstanding, presently people no longer want to encounter long queues for any reason, they appear impatient on queues for so long a time before they could be attended to and this has led to the increasing services being rendered by banks to further improve the convenience of banking through the means of electronic banking. But most of these introductions of new services exist as cryptographic based transaction, although with its own flaws. Crime at ATM's has become a global issue that faces not only customers, but also bank operators. Despite the advancement in technologies for E-commerce applications, payment related activities have been the sources of major breach and security concerns. As fraud continues to increase every year, many financial institutions are looking for possible solutions to this problem. Among those new technologies for dealing with payment processing, biometric payment technology have recently attracted more and more attention as a viable solution to decrease identity theft [1]. In a bid to address issues of safety of customers' funds and avoiding losses through compromise of Personal Identification Numbers (PIN), the apex bank, Central Bank of Nigeria (CBN) introduced Biometric authentication of Point of Sale (PoS) and Automated Teller Machines (ATMs) by 2015 . The apex bank had taken a giant step to gain the confidence of ATM consumers following the circular enforcing migration from Magnetic stripe type of debit card to chip and Pin (EMV compliance) type of debit card. Statistics show that this effort has reduced the fraud incidences by 90 per cent. Many customers are now embracing these electronic (ATM and PoS) channels in their transactions because of near-impossible efforts of would-be fraudsters to clone debit cards to perpetrate fraud as was the case during the pre-migration era". Interswitch also helps customers with the availability of its epayment solutions such as Paydirect, Autopay, Direct Debit, Verve Card, Quick-teller, Webpay and Smartgov". ``The Biometric authentication for POS and ATMs to address safety of

customers' fund and avoid losses through compromise of PIN is a reliable option [2].

Fingerprint based authentication is a prospective contestant to replace password-based authentication. Among all the biometrics, fingerprint based identification is one of the most mature and proven technique. At the time of transaction fingerprint image is acquired at the ATM terminal using high resolution fingerprint scanner. Security measures at banks can play a critical, contributory role in preventing attacks on customers [3]. Because fingerprint-based authentication offers several advantages over other authentication methods, there has been a significant surge in the use of biometrics for user authentication in recent years [4]. In this paper the existing security of the ATM (Automated Teller Machine) system has been improved by integrating the fingerprint of the user into the bank's database as to further authenticate it. This was achieved by modeling and building a prototype of an ATM simulator that will imitate a typical ATM system. The end result is an improved fingerprint authenticated ATM system that ensures greater security and improved customer's confidence in the banking sector. The primary focus of this work is on developing a biometric strategy (Fingerprint) to enhance the security features of the ATM for effective banking transaction.

2.0 LITERATURE REVIEW

If actually customers must embrace the use of ATM for their major transactions, the issue of ATM security must be taken with all seriousness. ATM cards must be very secure even when the owner misplaces or lose the card this security will prevent any attacker from using the card on any ATM machine. Since security measures at ATM centre's play a significant role in preventing attacks on customers money, several researches have proposed the used of fingerprint, to shift from PIN to biometric based security. Fingerprinting has been the most widely used during the 18th century. The maturity of Biometric techniques has led to the proposal of fingerprinting in multiple applications but in the last years, minutiae have been the main type of algorithm used. The minutiae are relatively stable and robust to contrast, image resolution and distortion as compared to other fingerprint images [5]. [6] provided a better understanding of the benefits and limitation of integration of biometrics in a PIN-base payment authentication system. Based on their review they proposed a biometric that can be integrated in a PIN-based authentication infrastructure by binding a fixed binary, renewable string to a noisy biometric sample. The South African Social Security Agency (SASSA) has introduced a new SASSA Payment Card that has a fingerprint authenticated features. The card is a SASSA branded smart payment MasterCard, which has an embedded chip containing personal details, fingerprint and secret PIN. With the card the customers can easily withdraw and make payment at point-of-sale (POS) center, purchase airtime, pay water and electricity bill from the accounts, or open accounts [7]. [8] proposed a smartcard based encryption/authentication scheme for ATM banking system. The first layer of the scheme is used to perform authentication based on available information on the smartcard. Fingerprint based authentication via feature and minutiae matching then followed on the second layer. [9] focused on vulnerabilities and the increasing wave of criminal activities occurring at ATMs and presented a prototype fingerprint authentication for enhancing security. The systems adopt the same measure as the current work by formulating modules for fingerprint enrolment, enhancement, feature extraction and database and matching. [10] proposed an ATM security enhancing method with secured Personal Identification Image (PII) process. A detailed study on various existing biometric systems is also presented stating the strengths and limitations. [11] and [12] present

groundbreaking models for biometric ATMs which replaces card system with biometric technology. The proposed systems hybridize feature-based fingerprint, iris and PIN to provide reliable and fool-proof ATM authentication. [13] Provided a network security framework for real time ATM application using a combination of PIN, thumb scanning and face recognition to foster security. The proposed framework is expected to register thumb and face features to be stored at a server side in encrypted format. Authentication is done by decrypting patterns from database, and matching with input pattern before access is granted for ATM operations. The integrated system uses Principal Component Analysis (PCA) and Eigen algorithm for face recognition, LSB algorithm for stegnogaphy and AES algorithm for cryptography. Though the framework looks promising, its practicality is not supported by detailed implementation and evaluation. [14] proposed an enhanced e-banking system where customer can access multiple accounts over different banks institutions with a single ATM card with fingerprint authentication. A match-on-card technique was used that relies on a one-to-one matching where the data from the ATM fingerprint sensor is compared only to the template stored on the user's ATM card. This will help in privacy concern of users; the system will also help the users to have access to multiple accounts with a single ATM card. It is secured and help in reducing ATM fraud. The paper used the characteristic features of fingerprint to overcome the limitations of the PIN based ATM authentication. However, the proposed method presented adequate implementation and evaluation to back-up the performance claim. The proposed system is different from others approaches because it makes use of the UML modeling in designing the system, used a three-tier architectural structure and minutiae for the extraction of the fingerprint.

3.0 METHODOLOGY

A growing security issue in ATM machine especially the use of card-PIN method has been of great concern to many researchers because the attacker can easily compromise the machine by using different methods of approach. In view of this, this paper try to see how these problems of Card-PIN can be reduced if not totally eradicated; this paper comprises the following implementation process: The process of enrolment involve the account holder opening an account and register with the bank of their choice. This will enable the bank to have all the enrollee's information and all necessary details that concern the enrollee and take the biometric data captured of the person that owns the account and store in the database, which will be used later for the process of verification and further update of information. The process of extraction and verification make used of minutiae-based techniques [5]. This is to obtain an efficient and thoughtful result in order to reduce or eradicate the problems which is associated with the use of card-PIN and high rate insecurity people faced in using ATM machine.

3.1 Enrollment Process: Before an Account holder being identified or verified by a biometric device, the enrollment process must be completed. The aim of this enrollment process is to create a summary profile of the user (Card Holders').

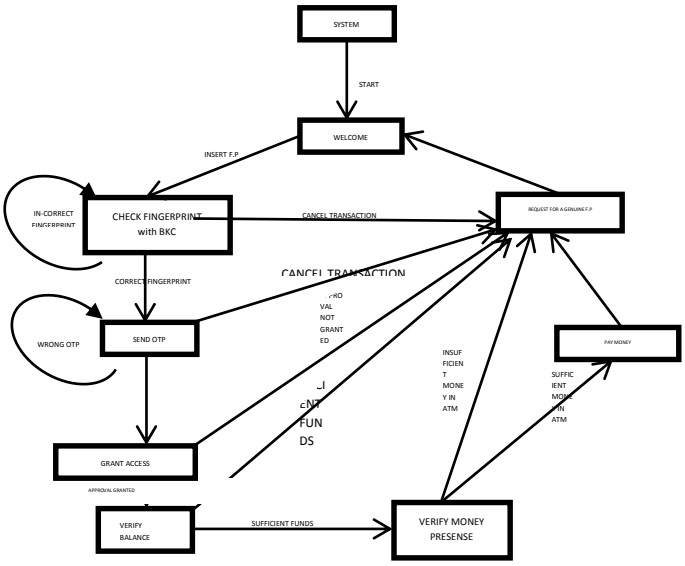

Figure 1: System Enrollment Flow Model

3.1.1 Biodata: This comprises the Following: Surname, First Name and Last Name which takes alphabetic characters, Account Type: Current, or Saving, this also takes alphabetic characters, picture of the enrollee which can take binary characters, Nationality of the enrollee takes alphabetic and string characters, date of birth takes string characters and the date account was issued takes string characters too. Fingerprint Image Capture: The Account Owner fingerprint will be captured with fingerprint scanner for a minimum of two or three biometric readings, by placing a finger in a fingerprint reader. Not all the samples will be stored; the technology analyzes and measures various data points unique to each individual. The number of measured data points varies in accordance to the type of device. Minutiae Feature Extraction from Image: This is where the minutiae extraction is done and of course processes like binarization, thinning and bifurcation provide a perfect minutiae feature extraction from the image.

3.1.1.2 Rotation and Displacement of Image: This is where the image is normalized to get an authentic and effective image to be stored in the database, which aids the process of matching.

3.1.1.3 Template Database Storage: This part stores all the templates and information that are been generated from the process of minutiae extraction and rotation and displacement of image.

3.1.1.4 Conversion and Encryption: The Account Owner measurements and data points are converted to a mathematical algorithm and encrypted. These algorithms cannot be reversed to obtain the original image. The algorithm may then be stored as a user's template in the database servers and on the ATM card

3.1.1.5 The Enrollee Storage: This has all the details of all the people that have been enrolled and its stores them with the account number. when there is need to view enrollee's details or make amends this can easily be done with the use of account number to trace individual's details and it makes the process of verification easier and faster as it saves time.

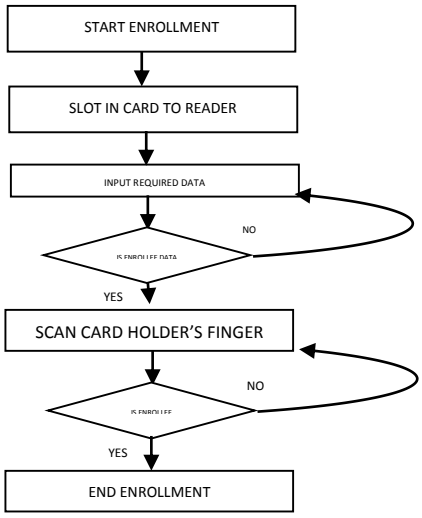

Figure 2: Flowchart for Enrollment process

Once the account holder has been enrolled in a system; such holder can start to use biometric technology to have access to his/her account via the ATM machine or related system to authorize transactions.

3.2.1 Identification: This is a one-to-many match. The user provides a biometric sample and the system looks

at all user templates in the database. If there is a match, the user is granted access, otherwise, it is declined.

3.2.2 Verification: This is a one-to-one match it requires the user to provide his/her identification such as a PIN and valid ATM card in addition to fingerprint. The account holder is to establish who he/she is and the system simply authenticates if this is correct. The biometric sample with the provided identification is compared to the previously stored information in the database. If there is a match, access is provided, otherwise, it is declined.

3.2.3 Authentication: This is the part of the database that allows access into and out of the database, this part monitors the kind of people that uses the database and controls unwanted users and unnecessary logins and access into the database for more secured and protected database environment. For security purposes servers must also address the problem of authentication. In a networked environment, an unauthorized client may attempt to access sensitive data stored on a server. Authentication of clients is handled by using cryptographic techniques such as public key encryption or special authentication servers such as in the OSF DCE system.

EXPERIMENTAL RESULT OF NEW SYSTEM

The experiments reported in this work have been conducted on the fingerprint images DB1_B in Secugen Hamster containing fingerprint images of size (128 *128) pixels. The database consists of 4 persons and each person has 10 images for fingerprint capture. For each person 6 images have been used in the training phase and 4 images for test phase. For $\alpha = 0$, the system would be very sensitive to distortions presented in non-training images, i.e. the filter is very discriminating, but distortion intolerant. Conversely, for $\alpha = 1$, the system will be extremely tolerant to distortions in the input, but may struggle to discriminate between different users of the system. α can therefore be used to produce a tighter or more forgiving system, depending on the system requirements. Three performance criteria have been computed: discrimination, distortion and accuracy. Discrimination accounts for invalid inputs which are incorrectly accepted while Distortion accounts for valid inputs which are incorrectly rejected. Accuracy is the proportion of true results. Where true positive is correctly identified, false positive is incorrectly identified, true negative is correctly rejected and false negative is incorrectly rejected. After a set of experiments have been conducted we found these results as shown in Figure 3.

It was observed that the maximum accuracy occurred using threshold (α) of 0.6, when experimented on windows 7, processor core i3 and RAM 6 GB to obtain accuracy and run time.

They gave distortion of 0, discrimination of 0.05, and accuracy of 97.67%.

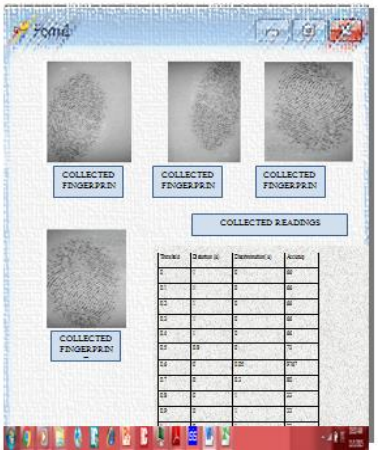

Figure 3: Simulation result

CONCLUSION

ATM has provided evidence that it is useful in reducing queue in banks, since one doesn't have to presently be in bank before withdrawing money. It can also be used to make others transactions like Point-of-Sale (POS), on-line transaction and a lot of other benefits. It is the 24/7 hours operations which permits account holder to withdraw at anytime and anywhere. But notwithstanding the above advantages the account holders have not embraced the use of ATM due to it

security challenges. This paper tried to find a way to eradicate or reduce the insecurity associated with the use of ATM machine by introducing a Smart card-based ATM with biometric authentication to withstand these challenges. The proposed system is cost-effective and much secured compared with the PIN-based ATM card. The proposed system was developed using java programming language, the programming language was used because of its platform independence, scalability, easy integration, implementation and upgrade. The system can run on any operating systems e.g. Windows, Linux etc. with .NET framework and MySQL. These tools were chosen due to their coding versatility, friendliness and compatibility. The proposed system is much secured and will reduce the ATM machine theft if not totally eradicate theft associated with the use of ATM machine.

- Account Details Capture: This is where data collected from account holder are been collected and stored in the database i.e. extraction and matching process.

- VPN: This is known as virtual private network, it is a dedicated network for the system that protects the data been captured and stored in the database for present and future purposes.

- Fire Walls: This is a kind of security that helps protect the network from spam ware and other attacks like hacking, virus attacks etc. of the proposed system. A firewall protects networked computers from intentional hostile intrusion that could compromise confidentiality or result in data corruption or denial of service. It may be a hardware device or a software program running on a secure host computer. In either case, it must have at least two network interfaces, one for the network it is intended to protect, and one for the network it is exposed to. A firewall examines all traffic routed between the two networks to see if it meets certain criteria. If it does, it is routed between the networks, otherwise it is stopped. A firewall filters both inbound and outbound traffic. It can also manage public access to private networked resources such as host applications. It can be used to log all attempts to enter the private network and trigger alarms when hostile or unauthorized entry is attempted. Firewalls can filter packets based on their source and destination addresses and port numbers.

- Collation Server: This is responsible for distribution of information to all clients on the network and even share of resources and other necessary things that are needed on the network.

- Z9PE-D8: This provides additional layer of security to the proposed system's local area network, it provides a good and secured motherboard for more reliable networking environment as it has in built dual Intel, Ethernet that leads to lower CPU utilization and yet it is very affordable

- Minutiae Matching: Once the minutia feature extraction is done the next phase is to compare the live template with the stored template, the system fetches the template from the template database storage and compare it with the live template. Once the matching is done, the matching score from the two templates is computed

REFERENCES

1. Allen, J. (2006), Biometric ID from Fulcrum Biometrics.
2. Auerbach, W. (1998), Handbook on Local Area Network.
3. Barkam, E. B. (1997), Instant Cipher Text-Only Crptanalysis of GSM Encrypted Communication.
4. Benhammadi, F., et al (2012), Biometrics. International Journal of Theoretical and Applied Information Technology , Vol. 37, pp. 17 - 23.
5. Christian, K. (2004), Biometrics: An Indepth Examination, SANS institute.
6. Das, S. S. and Debbarma, S.J. (2011), Designing a Biometric Strategy (fingerprint) Measure for

Enhancing ATM Security in Indian e-banking System, International Journal of Information and Communication Technology Research , Vol. 1, pp. 197-203.

7. Divya Singh, et al (1992), ATM Bankig Behaviour in Kuwait: A Consumer Survey, International Journal of Bank Marketing, Vol. 10, pp. 25-32.
8. Ihejiahi, R. (2009), How to Fight ATM Fraud Online Nigeria: Nigeria Daily Trust.
9. Juels, A. and Wattenberg, L. (2001), Fundamentals of Biometrics Authentication Technologies, International Journal For Image Graphics, Vol.1, No.1, pp. 93-113.
10. Jain A. K., Prabhakar, S. and Pankanti, S. (2002), Similarity of Identical Twin Fingerprints.
11. Wayman, J. A. (2009), An Introduction to Biometric Authentication System.
12. Jiang, X. Y. (2000), Fingerprint Minutiae Matching Based on the Local and Global Structures, International Conference on Pattern.
13. Johnson, A. (2011), Automated Teller Machine (ATM) Frauds in Nigeria: The Way Out, International Journal of Social Science, Vol. 27, pp. 53-58.
14. Juels, A. (1999), A Fuzzy Commitment Scheme, Proceedings of the 6th Conference on Computer and Communicatiobns Security, pp. 28-36.