International Journal of Applied Information Systems (IJAIS) – ISSN : 2249-0868
Foundation of Computer Science FCS, New York, USA
Volume 7– No.7,August 2014 – www.ijais.org

Fingerprint Authentication System: Toward Enhancing ATM Security

Awotunde, Joseph B.
University School,
University of Ilorin,
Ilorin, Kwara State, Nigeria

James, Tolorunloju R.
Department of Computer Science,
College of Education,
Igueben, Edo State, Nigeria

Fatimoh T. Adewunmi-Owolabi.
Department of Computer Science,
University of Ilorin,
Ilorin, Kwara State, Nigeria

Abdulkadir, Suhurat I.
Department of Computer Science,
School of Applied Science,
Federal Polytechnic, Offa, Nigeria

ABSTRACT

One of the major problems people face is the loss of the password and not remembering it again, these have cause a lot of damage to many people and organizations. ATM fraud has been very common in all banks and the problems has created fear in many costumers heart that they prefer going to the bank to collect their money than to use an ATM, also many people are illiterate that they don't know how to use the ATM card. So, the main aim of introducing ATM machine has not been met because you still find long queues in almost all banks in Nigeria. The existing ATM machine uses PIN-Card as a security which is very weak and easy to contravene. This paper tries to find a solution to the above problems by introducing fingerprint authentication into the existing ATM machine. A program prototype was designed to imitate a typical ATM system that uses fingerprint identification to enhance the security of the ATMs. The proposed system demonstrated a three-tier architectural structure. The verification system which centered on the enrolment, enhancement, feature extraction and matching of fingerprints. The backend database system that serves as warehouse of the templates of all ATM account holders' pre-registered fingerprints. The system's platform creates related transactions such as withdrawals, bill payment, buying of credit cards and balance enquiries etc. The results obtained confirm that the current approach could significantly reduce ATM fraud if not totally eradicate it.

Keyword and Phrases:

ATM Machine, Verification, Authentication, Minutiae-Base, Account Holder

1 INTRODUCTION

Nowadays the interest towards different systems of biometric identification among users of computer systems has grown up. Spheres of use of technologies of identification are not bounded. Government and private organizations are interested in technologies of fingerprint as it allows for increase in the level of protection of secret and confidential information. Companies that deal in the sphere of information technologies are interested in technologies of fingerprints, face, voice, iris recognition in order to check penetration of outside people to their net.

Payment processing has long been the weakest link in the transaction processing cycle of a typical online business. Despite the advancement in technologies for E-commence 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 has 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) is to introduce Biometric authentication of Point of Sale (PoS) and Automated Teller Machines (ATMs) by 2015 [2].

The apex bank had taken a giant step to gain the confidence of ATM consumers following the circular enforcing migration from Magstripe 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 e-payment solutions such as Paydirect, Autopay, Direct Debit, Verve Card, Quickteller, Webpay and Smartgov".

``The Biometric authentication for POS and ATMs to address safety of customers' fund and avoid losses through compromise of PIN is being considered by the apex bank and it will be implemented by 2015,'' [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.

2 AIM AND OBJECTIVE OF THE PAPER

In Nigeria, ATM technology is becoming more common than it ever was. ATMs appear to be mainly provided by banks in Nigeria. Yet, there is widespread adoption that peoples' awareness of the technology is diverse, which in turn affects their decision whether to use ATM or not. Hence the objectives of this paper are:

- To study the existence mode of operation of the present ATMs by examining the related literature.
- Modeling and building a prototype of an ATM machine that will copy a typical ATM system that uses fingerprint authentication to enhance the security of the ATMs.

3 RELATED WORK

For customers to really 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 misplaced or lost the card this will prevent any attacker from using the card on any ATM machine. Since security measures at ATM centers play a significant role in preventing attacks on customers money, several researches have proposed the used of fingerprint in a like manner of this paper, to shift from PIN to biometric based security. Fingerprinting has been the most widely used during the 20th century. The maturity of Biometric techniques and generally the dramatic improvement of the captured devices have 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 global distortion as compared to other fingerprint representation [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 fingerprint orientation model based on 2D Fourier expansions (FOMFE) in the phase plane. Though FOMFE does not require prior knowledge of singular points, it is able to describe the overall ridge topology seamlessly. [9] 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. [10] 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. [11] 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. [12] and [13] present ground-breaking 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.

[14] 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. [15] 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.

4 METHODOLOGY

The authors proposed ATM with biometric, a fingerprint security system, in order to meet the customers' needs who many of them have savings account and need to have access to their money during banking and non-banking hours. A descriptive conceptual approach which includes Unified Modelling language (UML) tools such as Use case models, activity diagrams & sequence diagrams is adapted. The work is implemented using Java Programming Language, the programming language was used because of its platform independence, scalability, easy integration, implementation and upgrade, and it was used to design the user interfaces and/or cardholder interaction with the ATM Machine.

The Minutiae-based was adopted due to its popularity and it is a well-known method for fingerprint verification. It is the most popular ones being included in almost all existing fingerprint identification and verification systems. Minutiae-base represents the fingerprint by its local characteristics like, terminations and bifurcations called minutia. Minutiae are small points of interest in the fingerprint image. The minutiae-based method recognition in two stages (i.e. minutiae extraction and minutiae matching) [5].

5 IMPLEMENTATION PROCESS

A growing security issue in ATM machine especially the use of card-PIN method has been of great concern to my researchers because the attacker can easily compromise the machine by using different methods. 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 of 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 own 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-base techniques. 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.

5.1 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'). The process consists of the following:

5.1.1 Biodata:

This comprises the Following: Surname, First Name and Last Name which take alphabetic characters, Account Type: Current, or Saving this also take alphabetic characters, picture of the enrollee which can take binary characters, Nationality of the enrollee take alphabetic and string characters, date of birth take string characters and the date account was issue take 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 would be done have a perfect minutiae feature extraction from the image.

5.1.1.2 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.

5.1.1.3 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.

5.1.1.4 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

5.1.1.5 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:1.

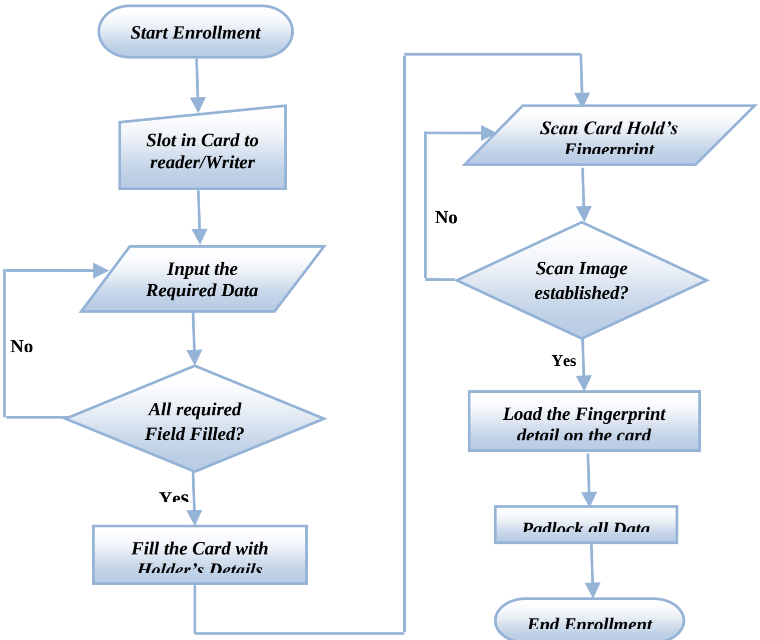
Start Enrollment
Slot in Card to reader/Writer
Input the Required Data
No
All required Field Filled?
Yes
Fill the Card with Holder's Details
Scan Card Hold's Fingerprint
No
Scan Image established?
Yes
Load the Fingerprint detail on the card
Padlock all Data
End Enrollment

Figure 1: Flowchart for Enrollment process

5.2 Identification and Verification process

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

5.2.1 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.

5.2.2 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 figure: 2.

5.2.3 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.

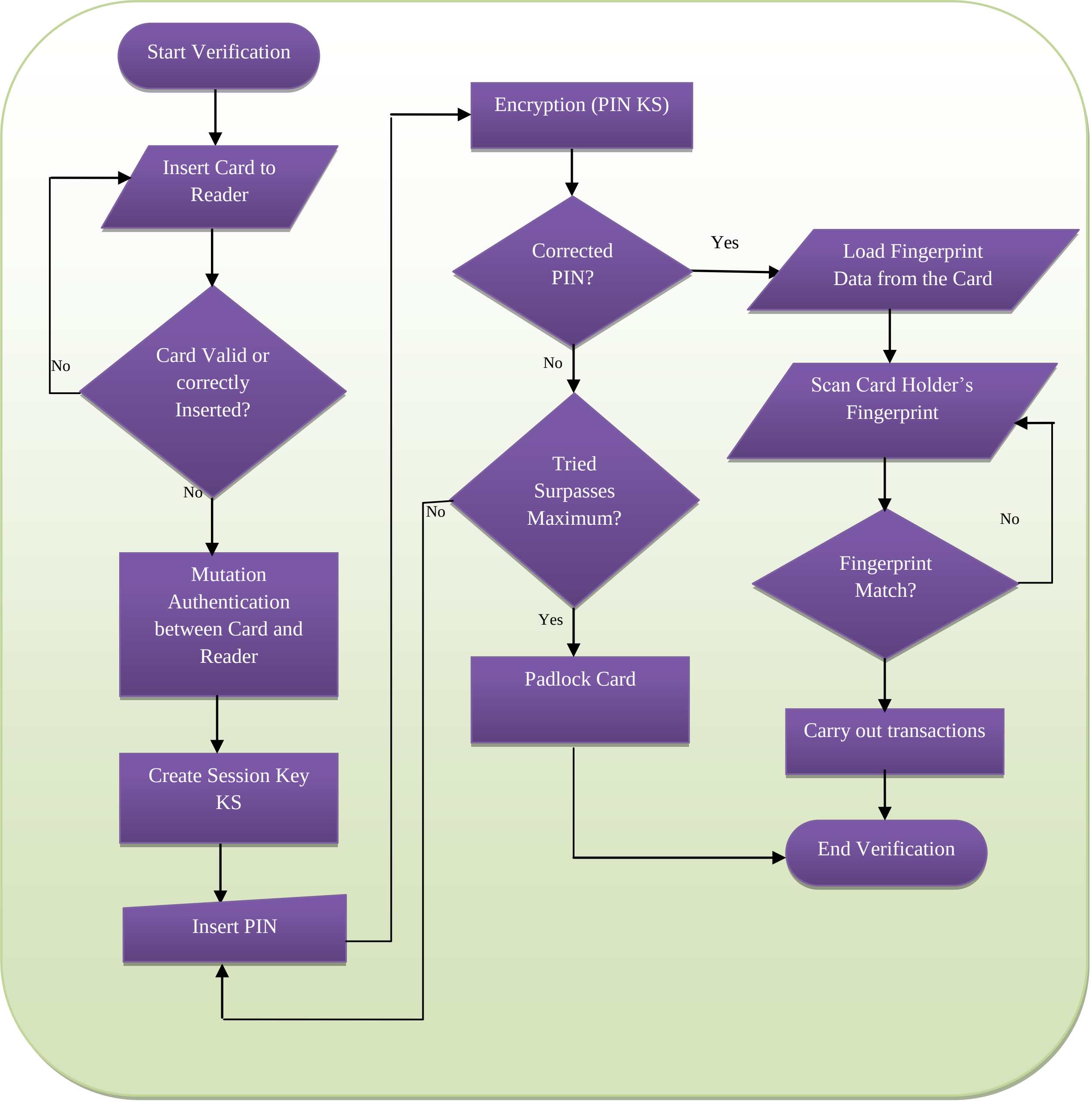

Figure 2: Flowchart for Identification & Verification Process

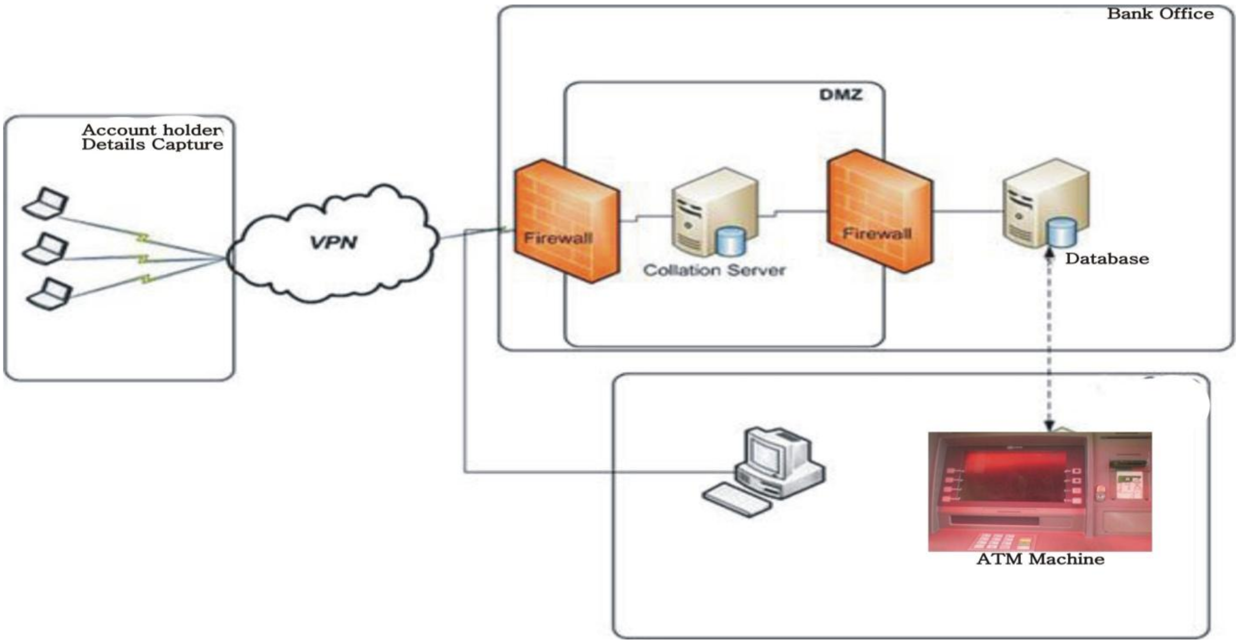

Figure 3: Architectural design of the system

Key

DMZ-Demilitarized zone

Z9PE-D8- This is used for more reliable network

VPN- Virtual Private Network

The above diagram shows the architectural design of the system

5.3.0 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.

5.3.1 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.

5.3.2 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.

5.3.3 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.

5.3.4 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

5.4.0 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 Fatai, Awotunde & Matiluko (2014).

6 CONCLUSION

ATM has provided evidence that it is useful in reducing queue in our banks, since you don't have to presently be in bank before you can withdraw your 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 24/7 hours operations which enable the account holder to withdraw at anytime and anywhere. But notwithstanding the above advantages the account holders has not embraced the use of ATM due to it security challenge. 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 ameliorate these challenges. The proposed system is cost-effective and much secured compared with the PIN-base 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 for 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.

7 FUTURE WORK

Future researchers can work on how to do away completely with PIN-Card authorization by the introduction of Bimodal biometrics like Palm and Finger vein, fingerprint and face recognition authentication which is very fast, accurate and difficult to contravened. Furthermore, mobile phones can be found in almost every part of the world in both urban and rural areas, therefore a better authentication with biometric can be developed using smart-phones.

REFERENCE

[1] Swann, J. (2004). “Teaching Ethics: It's the Right Thing to Do.” OR/MS Today. 31:10.

[2] http://leadership.ng/news/100713/cashless-policy-cbn-introduce-biometrics-atms-pos-2015#sthash .I0I5wd2G.dpuf Leadership New paper, 10-07-2013.

[3] Kuykendall, Lavonne and W. A. Lee. 2003. “Intermediary Risk? Card Hack Puts OSOs in the Hot Seat,” American Banker, February 21.

[4] Akwaja Chima (2010). “Nigeria Connects 99 million Subscribers”, Fin. Standard., 10: 15-512.

[5] Fatai, O.W., Awotunde, J.B. and Matluko, O.E (2014) A Novel System of Fingerprint Recognition Approach for Immigration Control, IOSR Journal of Computer Engineering (IOSR-JCE) 2278-8727Volume 16, Issue 3, Ver. III (May-Jun. 2014), PP 39-42.

[6] Jeroen B., Ileana B., Koen G., and Emile K. (2011) Evaluation of a template protection approach to integrate fingerprint biometrics in a PIN-based payment infrastructure

[7] The South African Social Security Agency (SASSA) (2013) A leader in the delivery of social security services. Re-register to get yours: SASSA HOUSE 501 Prodinsa Building Cnr Steve Biko and Pretorius Street Pretoria.

[8] Wang Y, Hu J, and Phillips D (2007) A fingerprint orientation model based on 2D Fourier expansion (FOMFE) and its application to singular-point detection and fingerprint indexing. IEEE Trans Pattern Anal Mach Intell 29: 573-585.

[9] Fengling H, Jiankun H, Xinhuo Y, Yong F, and Jie Z (2005) A novel Hybrid Crypto- Biometric Authentication Scheme for ATM Based Banking Applications. Lect Notes Comput Sci 3832: 675-681.

[10] Das SS, and Jhunu D (2011) Designing a Biometric Strategy (Fingerprint) Measure for Enhancing ATM Security in Indian E-Banking System. International Journal of Information and Communication Technology Research 197-203.

[11] Santhi B, and Kumar RK (2012) Novel Hybrid Technology in ATM Security Using Biometrics. Journal of Theoretical and Applied Information Technology 37: 217-223.

[12] Bhosale ST, and Sawant BS (2012) Security in e-Banking via Card-less Biometric ATMS. International Journal of Advanced Technology & Engineering Research 2: 9-12.

[13] Ibiyemi T. S, Obaje S. E, and Badejo J (2012) Development of Iris and Fingerprint Biometric Authenticated Smart ATM Device & Card. 24th National Conference of the Nigeria Computer Society (NCS).

[14] Mali P, Salunke S, Mane R, and Khatavkar P (2012) Multilevel ATM Security Based On Two Factor Biometrics. IJERT 1: 8.

[15] Abayomi-Alli A., Omidiora E.O., Olabiyisi E.O., and Ojo J.A. (2012) Enhanced E-Banking System with Match-On-Card Fingerprint Authentication and Multi-Account ATM Card. The Journal of Computer Science and Its Aplication, An International Journal of the Computer Society of Nigeria (NCS), V0l. 19, No.2 December, 2012