Volume: 08 Issue: 04 Pages: 3110-3117 (2017) ISSN: 0975-0290

An Enhanced Automated Teller Machine Security Prototype using Fingerprint Biometric Authentication

Paschal A. Ochang
Department of Computer Science, Federal University Lafia, Nasarawa State
Email: pascosoft@gmail.com
Paulinus O. Ofem
Department of Computer Science, Federal University Lafia, Nasarawa State
Email: paulinus.ofem@fulafia.edu.ng

ABSTRACT

The steady growth in electronic transactions has promoted the Automated Teller Machine (ATM) thereby making it the main transaction channel for carrying out financial transactions. However, this has also increased the amount of fraudulent activities carried out on Automated Teller Machines (ATMs) thereby calling for efficient security mechanisms and increasing the demand for fast and accurate user identification and authentication in ATMs. This research analyses, designs and proposes a biometric authentication prototype for integrating fingerprint security with ATMs as an added layer of security. A fingerprint biometric technique was fused with personal identification numbers (PIN's) for authentication to ameliorate the security level. The prototype was simulated using a fingerprint scanner and Java Platform Enterprise Edition was used to develop an ATM application which was used to synchronize with a fingerprint scanner thereby providing a biometric authentication scheme for carrying out transactions on an ATM.

Keywords – ATM, Database Modeling, Fingerprint Authentication, Security Analysis, Software Testing

Date of Submission: Jan 30, 2017 Date of Acceptance: Feb 23, 2017

1. INTRODUCTION

The Automated Teller Machines (ATMs) provide numerous monetary services to the society at large and the number of users has increased tremendously due to the promotion of cashless societies by major financial institutions [1]. Existing ATMs are based on plastic cards with a metallic chip which is combined with a PIN (Personal Identification Number) [2]. Together this serves as a medium for logging into the banking platform of the ATM in use. The current form of authentication has withstood the taste of time but however, it has not been fail proof as previous research has shown [3]. Individuals making use of ATMs have complained of lost funds due to hackers gaining knowledge of their PINs [4] and furthermore, many individuals have also bemoaned the inability to carry out transactions due to lost or damaged debit cards thereby having to pay for a replacement. These factors have been tackled by previous researchers who propose the introduction of a biometric method of authenticating individuals and the banking community especially in developing countries with a high a level of crime and financial fraud rate.

Biometrics can be defined as a measurable physiological and behavioral characteristic that can be captured and subsequently compared with another instance at the time of verification. It is an automated method of recognizing a person based on physiological or behavioral characteristic. It is a measure of an individual's unique physical or behavioral trait which can be used in validating or authenticating an individual. Common physical biometric characteristics include fingerprints, hand or palm geometry, retina, iris and facial scans while common behavioral characteristics are signature, handwriting, keystrokes and voice match. Biometrics technologies are a very secure way of authentication, this is due to the uniqueness of biometric data which cannot be shared, copied or lost. [5] pointed out that biometric based authentication offers several advantages over other authentication mechanisms and research has shown that the fingerprint technology in particular, can give a considerably more precise and reliable client validation.

2. THE AUTOMATED TELLER MACHINE (ATM)

ATMs were introduced to automate the work of a bank cashier. [1] disclosed that ATMs were first initiated in 1960 by City Bank of New York on a trial basis, the purpose of the machine then was for customers to pay utility bills and get receipts without a bank clerk attending to them. ATMs are now not only located at bank sites but also at a number of business areas for the convenience of customers. The global ATM market forecast research conducted by Retail Banking Research Limited showed that 2.5 million ATMs are in use worldwide as of 2013. In Nigeria, the first bank to use ATM was the Societe Generale Bank of Nigeria (SGBN) in 1990. The trademark name for SGBN's ATM was "Cash Point 24". First Bank Plc., one of the first generation banks then, came on stream with their own ATM in December 1991, a year after SGBN. They also gave a trademark name "FIRST CASH" to their ATM. While that of SGBN was the drive-in-system, while that of the First Bank ATM was through-

Volume: 08 Issue: 04 Pages: 3110-3117 (2017) ISSN: 0975-0290

the-wall. Access to ATMs today is through the use of a Personal Identification Number (PIN) and a plastic card that contains magnetic strips with which the customer is identified. The Banks gives the PIN to the customer directly and the customer is instructed not to reveal the number to anybody or a third party.

An ATM combines a computer terminal, recordkeeping system, and cash vault in one unit, permitting customers to enter a financial firm's bookkeeping system with either a plastic card containing a Personal Identification Number (PIN) or by availing a special code number into a computer terminal linked to the financial firm's computerized records 24 hours a day. An ATM can be described as a cash dispenser which is designed to enable customers to enjoy banking services without coming in contact with Bank Tellers or Cashiers [6].

2.1 ATM Fraud Analysis

[7] expressed that the issue of ATM frauds is a worldwide phenomenon and its consequences are on bank patronage and it should be of concern to the stakeholders in the banking industry. In his paper, he identified the dimensions of ATM frauds in Nigeria and proposed possible solutions that will put ATM frauds in the Nigerian banking system under check. His paper employed both primary and secondary data to investigate the ATM frauds in Nigerian banks. The chi-square statistical technique was used to analyze the data gotten and test the hypothesis raised in the course of the analysis. The paper concluded that both bank customers and the bank have a joint role to play in bringing to an end the spread of ATM frauds in the banking industry. Card jamming, shoulder surfing and Stolen ATM cards was found to constitute 65.2% of ATM frauds in Nigeria.

Previous research has shown that there is no statistically significant difference in the perception of the positive impact of ATM in terms of carrying out banking and financial transactions. However, research has also shown that the current security implementations currently in place do not fully prevent the security risks on ATMs and financial transactions [8].

2.2 Types of ATM Fraud

There are several kinds of ATM frauds and researchers have been able to place them into categories. Using a report on global ATM frauds conducted in 2007 ATM attacks and frauds can be categorized into the following:

a) Skimming Attack: This is the most popular ATM fraud in which a skimmer device (card swipe device) is placed at the ATM slot. The skimmer downloads the personal data of everyone who inserts his/her card into the ATM and this allows the fraudster to duplicate the customer's ATM card. A single skimmer device can store information for more than 200 ATM cards before being reused.

b) Card Trapping: in this case, a trapping device is placed inside the ATM by an authorized person to capture or trap a customer's card. Here, when the user leaves the ATM without his/her card, the card is retrieved by the criminal and used to gain access to the customer's account illegally and probably transfer or withdraw fund from the customer's account.

c) Phishing Attack: Phishing scams are designed to lure ATM users into providing card numbers and PINs of their ATM card. In this case, the scammer sends an e-mail to the user claiming that the user account information is incomplete or that the user needs to update his/her account information to prevent the account from being closed. The user is asked to click on a fraudulent link and then follow the directions provided. The site directs the user to input sensitive information such as card number and PIN. The information is collected by the scammer and then used to create the duplicate card.

d) ATM Malware: This is an attack which requires an insider such as an ATM technician who has a key to the machine to place the malware on the ATM. After this act, the attacker inserts a control card into the machine card reader that act as a malware. This gives him/her control of the ATM and the ATM's keypad. Malware captures magnetic stripe data and PIN codes from the private memory space of the transaction processing application installed on an ATM.

e) ATM Hacking: In this case, an attacker uses sophisticated programming techniques to break into a website which resides on a financial institution network. Bank systems are accessed to locate the ATM database and also to collect card information which are later used to make a clone card.

f) Physical Attack: physical attacks are attempts on the safe inside the ATM through mechanical means with the intention of breaking the safe to collect the money.

g) Fraudulent Placement: this is a case where an ATM card production request is made without any indication from the account owner. This is commonly done by the bank employees.

Having analyzed traditional ATMs in terms of flaws and security issues, it is necessary to also analyze previous architectural frameworks that have been proposed by researchers in other to enhance authentication and increase security.

2.3 Previously Proposed ATM Authentication Frameworks

[9] proposed An ATM framework called Dyna-Pass. In this framework the client accesses his or her account using a debit card through the ATM with the use of a PIN. The ATM reads this card and checks the PIN with the bank server through a dedicated network. The server now connects to an SMS (short messaging system) center in other to send a password called the Dynamic Password to the user which is a randomly generated password. Finally, the client gets this dynamic password and enters this password into the ATM. The ATM again affirms this

Volume: 08 Issue: 04 Pages: 3110-3117 (2017) ISSN: 0975-0290

dynamic password with bank server and afterwards responds to the client.

An ATM framework was proposed by [10] in which an embedded fingerprint system was utilized for ATM security applications. In their system, bankers collect customers' fingerprints and cell phone numbers while opening accounts. The mode of operation was such that when a customer places a finger on the fingerprint module it automatically generates a different 4-digit code as a message to the mobile phone of the authorized user. The code received by the customer is entered into the ATM by pressing the keys on the touch screen. After entering it checks whether it is a legitimate one or not and permits the customer further access if confirmed legit. The system proposed by [10] had a drawback in the sense that they might be a network delay which can trigger late arrival of messages on the users mobile phone thereby prompting the user to initiate the process all over again therefore it will be a good approach if the customer uses a fix password that the customer has set by himself/herself and not a dynamically generated one each time he or she wants to make a transaction.

[11] talked about biometric verification in relation to payment systems and ATMs and proposed a verification framework which will replace the combination ATM cards and PINs with only biometrics for more convenience. He proposed an idea in which an infrared machine scans through a fingerprint pool for approval and validation. It compares the fingerprint layout with the ones stored in the database and if there is a match, it allows access for transaction else it denies access. The disadvantage of this framework is the one factor authentication it provides for security purposes because it is not safe using Biometrics only as your measure of verification, therefore PINs were eliminated.

[12] proposed a system in an article titled "Enhanced ATM Security System Using Biometrics" they presented the importance of Biometric methodology. They proposed that biometrics is the only viable approach for ATM security and that the level of security must be understood by decision makers before using the biometric systems and they must also be well aware of that differentiability between the user perception of security and reality of sense of security. The biometric system is the only process that will assume a vital part in verification as well as authentication process, and other part of the entire process will also play a comparable part in determination of its adequacy.

[13] "A Review on Secured Money Transaction with Fingerprint Technique in ATM System" wrote that a Biometric ATM system is very secure in the light of the fact that it meets the expectations of data contained within body parts. Biometrics is uniquely bound to individuals and may offer organizations a stronger method of authentication and verification. However, the research pointed out that biometric ATMs were very useful but also very difficult to implement.

2.4 Summary of Review

After a careful analysis and review of related literature it is noted that multiple frameworks have been proposed due to the importance of this research area. However, we intend to differ in our approach in which we intend to design and experiment a simplified framework which harmonizes the previous work in this field in terms of using fingerprint technology in congruence with PINs thereby eliminating the need for plastic cards or debit cards and thus differing from previous research.

3. METHODOLOGY

In other to design and test the proposed prototype an evaluation of the overall architectural design and workflow of a traditional ATM was analyzed while the bank enrolment process for a customer opening or updating an account with his or her financial institution was also evaluated. This will enable the fusion of our intended design using case diagrams and activity diagrams to design a model integrating a fingerprint module as part of the authentication flow and also to identify all the elements and parties involved. A flow chart will also be used to handle transfer of processes and authentication and transaction flow. This approach will enable the development of an ATM application software prototype which will be interfaced with a fingerprint scanner in other to test the authentication process.

3.1 The Proposed System

Based on the study of current ATMs, The first interface the bank customer interacts with on the ATM machine prompts the customer to enter his/her debit card after this the PIN number is requested. If the user enters an invalid PIN number, a message box appears prompting an invalid PIN and the system returns enter a valid PIN number. After validating the customer's PIN number, the customer is taken directly to the transaction menu where he or she can select the desired operation. However, in our research and proposed prototype, the customer is directed to the next phase of the authentication process which is inputting the valid fingerprint. This is the final interface the customer interacts with in the authentication process. It requests from the customer the enrolment of his/her fingerprint to be placed on a Fingerprint reader. The fingerprint reader accepts the fingerprint and seeks to match the live sample with the already enrolled templates in the banks database. When the fingerprint is found correct, the customer is taken to the transaction phase where he/she will choose among the transaction operations, otherwise the customer is denied access.

3.2 The Proposed System Modeling and Design

3.2.1 Use Case Diagram

Based Use case diagrams are used to model the interaction between a system and the intended user. Use case diagram aids system designers in fully understanding system requirements and it is important in project development, planning, and documentation of system requirements. It shows the activity of the users and the responsibility of the system to its users. It describes the uses of the system and

Volume: 08 Issue: 04 Pages: 3110-3117 (2017) ISSN: 0975-0290

shows the sequence of actions that can be performed as well as defining what happens in a system. In essence, the use case model tries to systematically identify uses of the system and provides an external view of a system or application. It is directed towards the users or the "actors" of the systems, not its implementers.

The Fig 1 below shows the use case diagram for the system design of the proposed prototype, where customers can perform transactions by inputting their fingerprints and PIN. It shows another important actor which is the bank administrator which is an entity responsible for enrolling a new customer and capturing necessary details during an account opening or update process

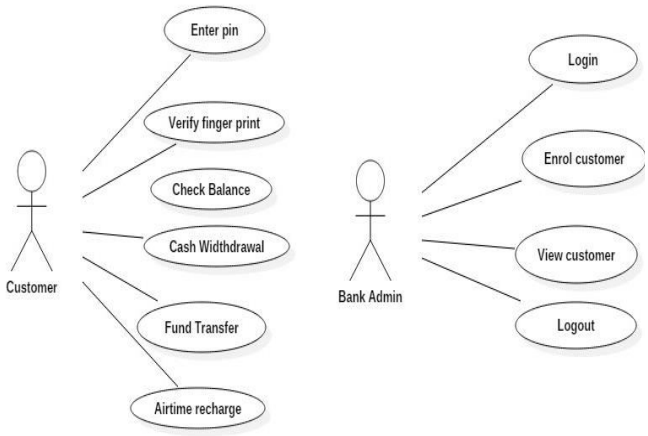

Fig. 1. Use Case diagram of the actors and their processes in the proposed prototype

3.2.2 Activity Diagram

Having modeled the actors in the authentication process an activity model was used in other to highlight PIN validation, Fingerprint validation, transaction, withdrawal, deposit, fund transfer and successful completion of other transactions. An activity diagram is a Unified Modeling Language that represents the graphical workflow of stepwise activities and actions with support for iteration, choice and concurrency. It thus shows the overall flow of control.

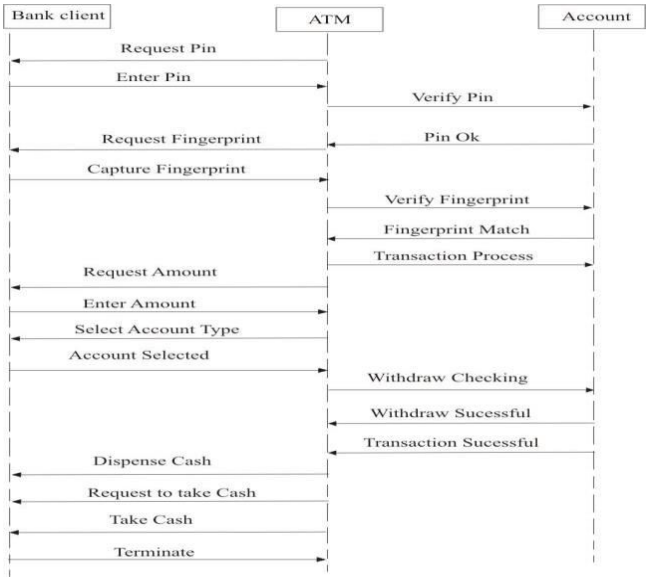

Fig. 2. Activity diagram of the proposed prototype

The activity diagram and use case diagram models shows that the customer and the bank administrator who registers the customer can be separated into different modules, furthermore the data collected from the customer has to be stored in a database which will serve as the backend of the proposed model, this was done by the design of an entity diagram showed in Fig. 3 below which enabled the use of MySQL in designing a dynamic database to store information from both modules.

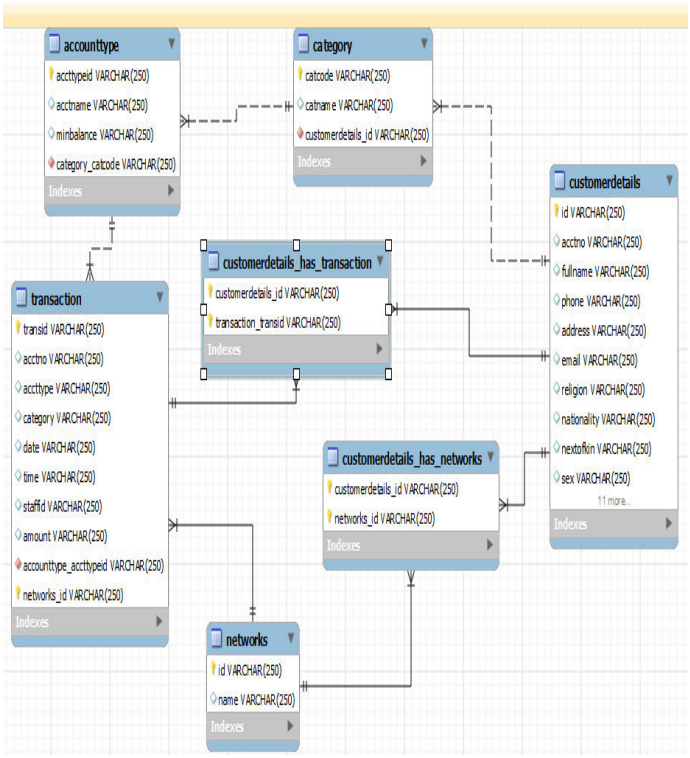

Fig. 3. Entity relationship diagram of the database design

In other to build the frontend of the proposed application prototype Java Platform Enterprise Edition was used to categorize the customer and the bank admin into modules

Volume: 08 Issue: 04 Pages: 3110-3117 (2017) ISSN: 0975-0290

which were harnessed to the MySQL database thereby providing an interface driven application scenario similar to a traditional ATM. The application was built with the drivers of a fingerprint scanner which was also interfaced with the database in other to capture and authenticate fingerprints. The modules depicted each actor as an object, and the activities that can be carried out by each actor were modeled as the methods for the object.

4. IMPLEMENTATION AND DISCUSSION OF RESULTS

The prototype was tested under the activities that can be carried out by the two actors in the use case design which is in relation to the two modules designed in the application frontend. The admin module was tested in terms of registering and enrolling a new customer and the customer module was tested in terms of authentication.

Fig. 4 below shows the administrator module for enrolling new customers and updating existing customers. A user name and password is required to login as an administrator in other to enhance security and access is denied if the user name and password is incorrect.

Fig. 4. Administrator Login

On logging into the admin module the bank administrator can enroll customers in a customer registration form as shown in Fig. 5 below. On submitting the form the prototype prompts for the enrolment of the customers fingerprint and after the fingerprint is captured a customer bio data receipt which can be printed and given to the customer is generated as shown in Fig. 6 below which also generates the users PIN and this information is stored in the database respectively.

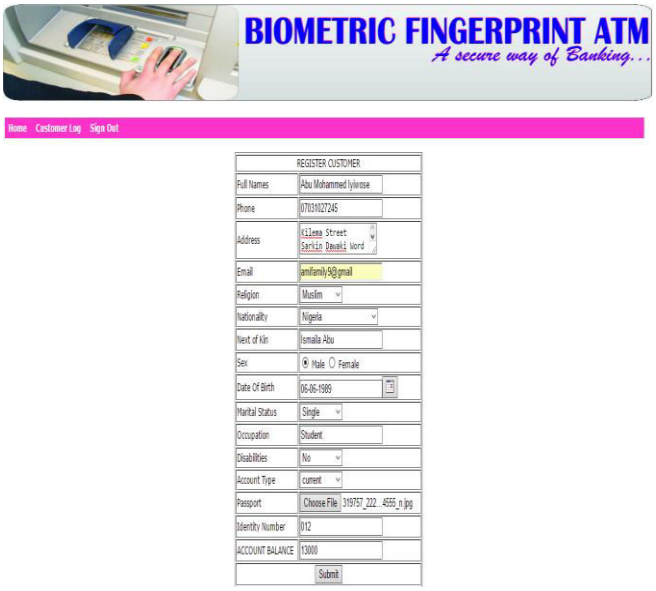

Fig. 5. Customer Registration Form

Fig. 6. Customer Bio data Receipt

On completed the customer's registration a bank account number is automatically generated for the customer which is unique to the customer. This can be shown in Fig. 7 below in the account number field. Furthermore, the Fig. below shows the results of enrolled customers if the database is queried in other to view customer's information on the system.

Volume: 08 Issue: 04 Pages: 3110-3117 (2017) ISSN: 0975-0290

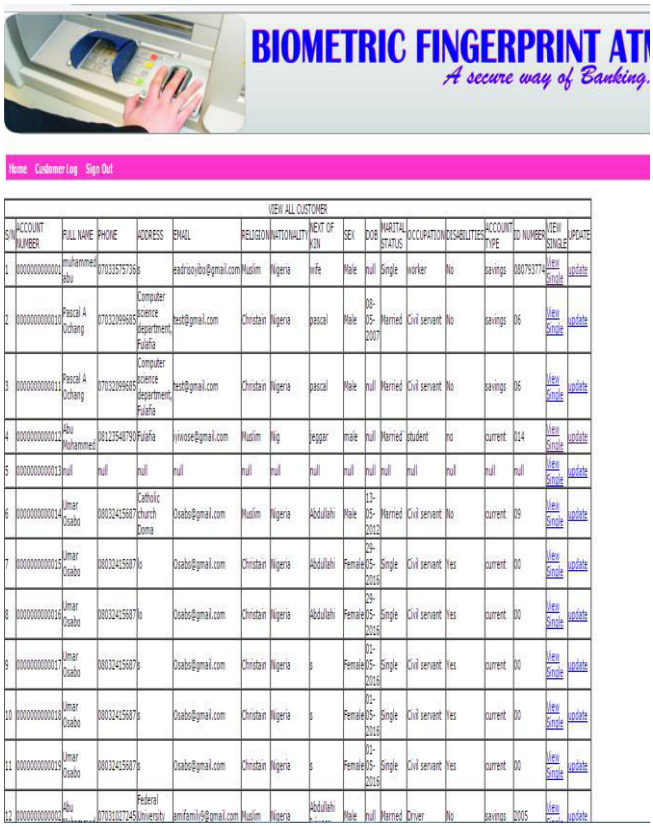

Fig. 7. Query results showing Enrolled customers

In other to test the customer module the PIN generated for one of the test customers was used. The process of inserting a debit card was bypassed in the test due to the inability to get a debit card reader for integration with the prototype. Fig. 8 below shows the customer login interface asking the customer to insert his or her PIN.

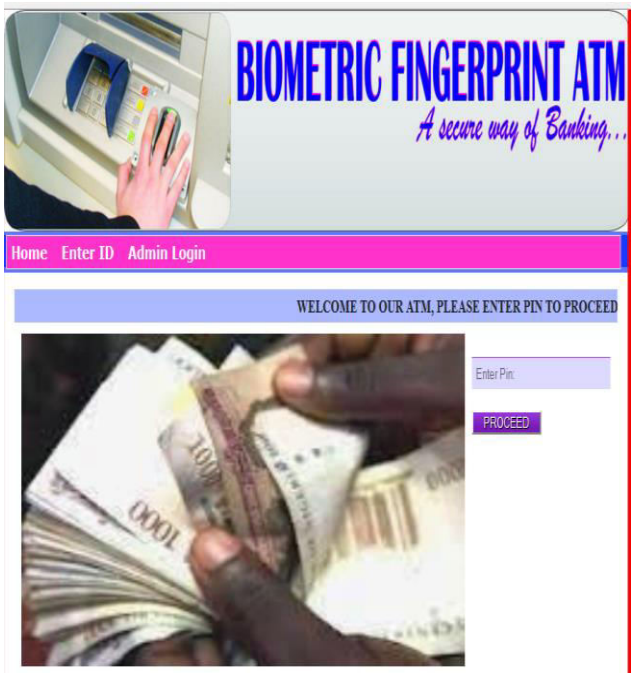

Fig.8. Customer Login interface

The proposed method unifies the PIN and the fingerprint authentication process whereby the users PIN is captured then the fingerprint is also requested and captured as shown in Fig. 9 below. Together this serves as a unified authentication process whereby the PIN and fingerprint are embedded together whereby the PIN is verified together with the fingerprint which matches that of the customer in the database.

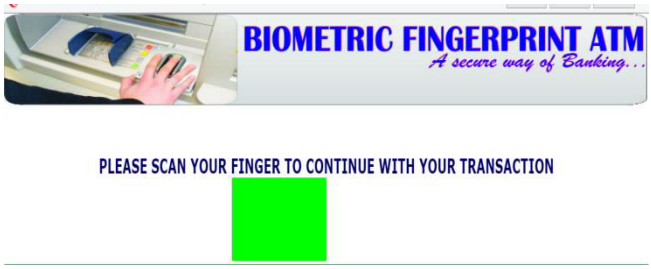

Fig. 9. Fingerprint Authentication request

This method can therefore be used to eliminate the need for a debit card because the fingerprint can be used to match that of an enrolled customer and thereby fetching the customer information and verifying it against the registered PIN. If the user is successful through the authentication process then the user will be able to access transaction services.

4.1 Software Testing

The system was tested with samples from 7 different individuals and was found to be successful. Testing of the prototype was done under each module designed in the application and Table 1 below shows the test case and the outcome.

Volume: 08 Issue: 04 Pages: 3110-3117 (2017) ISSN: 0975-0290

Table 1: Prototype Test results

S/N	Test Case	Discussion	Outcome
1	Testing the pin validity of the Admin	Two tests were carried out. Test 1: we tested a valid Admin pin and it was successful. Test 2: we tested an invalid pin and an "invalid pin" message was displayed.	Test 1: successful Test 2: invalid pin message displayed
2	Registering the customer	We performed an enrollment on 7 test subjects by collecting their details and fingerprint and their pin was generated successfully.	successful
3	Verifying the pin and finger print of an enrolled customer	Test 1: we entered the correct pin and the finger print. Test 2: we entered the incorrect pin and correct fingerprint. Test 3: we entered the correct pin and the incorrect fingerprint. Test 4: we entered the incorrect pin and the incorrect finger print.	Test 1: successful Test 2: invalid pin message displayed Test 3: invalid enrollment fingerprint Test 4: invalid pin and finger print
4	Withdrawa l	Test 1: request available funds Test 2: request more than available funds Test 3: request all the funds	Test 1: withdrawal successful Test 2: no cash to dispense Test 3: minimum balance is #500

5. SUMMARY AND CONCLUSION

Financial transactions on ATMs have seen an exponential growth with a major focus on developing countries where other sources of carrying out financial transactions such as mobile banking and internet banking are gradually being adopted by customers. Research has shown that the ATM witnesses the highest amount of transaction traffic compared to other transaction channels therefore this makes it a prime target for security vulnerabilities in developing regions. Therefore, this calls for advanced security architectures in other to enhance the overall security of ATMs. The use of biometric authentication as shown in this research and methodology shows proof of concept that integrating biometric authentication with ATMs is not only feasible but also enhances security thereby reducing security hazards.

REFERENCES

[1] Adeoti, J.O., 2011. Automated Teller Machine (ATM) Frauds in Nigeria: The Way Out. *Journal of Social Sciences*, 27(1), pp.53–58.

[2] Khatmode Ranjit, P. et al., 2014. ARM7 Based Smart ATM Access & Security System Using Fingerprint Recognition & GSM Technology. *International Journal of Emerging Technology and Advanced Engineering*, 4(2), pp.856–860

[3] Padmapriya, V. & Prakasam, S., 2013. Enhancing ATM Security using Fingerprint and GSM Technology. *International Journal of Computer Applications*, 80(16), pp.43–46.

[4] Onyesolu, M.O. & Ezeani, I.M., 2012. ATM Security Using Fingerprint Biometric Identifer : An Investigative Study. *International Journal of Advanced Computer Science and Applications (IJACSA)*, 3(4), pp.68–72.

[5] Kolhe, H. et al., 2014. ATM Transaction Security System Using Biometric Palm Print Recognition and Transaction Confirmation. *International Journal Of Engineering And Computer Science*, 3(4), pp.5332–5335.

[6] Ogunsemore, 1992. Banking services: *The emergence and impact of electronic banking*

[7] Adewumi, S., 2010. An Ideal ATM Implementation in an Unsecured Environment. In *Proceedings of the International Conference on Software Engineering and Intelligent Systems*. pp. 1–8.

[8] Adesuyi, F.A. et al., 2013. A survey of ATM security implementation within the Nigerian banking environment. *Journal of Internet Banking and Commerce*, 18(1).

[9] Duvey, A.A., Goyal, D. & Hemrajani, D.N., 2013. A Reliable ATM Protocol and Comparative Analysis on Various Parameters with Other ATM Protocols. *International Journal of Communication and Computer Technologies*, 1(56), pp.192–197.

[10] Amurthy, P.K. & Redddy M, 2012. Implementation of ATM Security by Using Fingerprint recognition and GSM. *International Journal of Electronics Communication and Computer Engineering*, 3(1), pp.83–86.

[11] Von Graevenitz, A., 2007. Biometric authetication in relation to payment systems and ATMs. *DuD - Datenschutz und Datensicherheit*, 31(9), pp.681–683.

[12] Oko, S. & Oruh, J., 2012. Enhanced atm security system using biometrics. *IJCSI International Journal of Computer Science*, 9(5), pp.352–357.

[13] Mandal, S., 2013. A Review on Secured Money Transaction with Fingerprint Technique in ATM System. *IJCSN - International Journal of Computer Science and Network*, 02(04), pp.08–11.

Biographies and Photographs

Paschal A. Ochang: Paschal A. Ochang is an Assistant Lecturer in the Department of Computer Science, Federal University Lafia, Nasarawa State, Nigeria. He has worked in the network engineering field for over 9 years. He holds a B.Eng. in Computer Engineering and a M.Sc. in Telecommunications Engineering which was gotten from the University of Sunderland, Sunderland, United Kingdom. He is a Microsoft Certified Professional (MCP) and has worked with the largest CDMA network in Africa called Visafone Communications LTD as a Data Service Consultant. His research interests cover the areas of Voice over Internet Protocol (VoIP) networks, intelligent networks, network architecture, multicast networks and network security.

Paulinus O. Ofem: Paulinus is also an Assistant Lecturer in the Department of Computer Science, Federal University Lafia, Nasarawa State, Nigeria. He obtained his MSc in Advanced Computer Systems Development from the University of the West Scotland, in the United Kingdom and BSc in Computer Science from the University of Calabar, Calabar, Nigeria. He began his academic and research career as a research assistant at Laurea University of Applied Sciences, Finland and the University of the West of Scotland. His research interest include empirical software engineering and software security, service oriented architecture, databases and human computer interaction.