International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2018 IJSRCSEIT | Volume 3 | Issue 1 | ISSN : 2456-3307

Fraud Detection and Control System in Bank Using Finger Print Simulation

Dr. Oye N. D., Jemimah Nathaniel
Department of Computer Science MAUTECH, Yola Nigeria

ABSTRACT

The need to control access to certain information and resources has been taken seriously nowadays due to fraud and other threats to current security systems. The role of ATM in promoting, developing and expanding the concept of "Anytime Anywhere Anyplace" banking is undeniable. It offers a real convenience to those who are on the run in their everyday life, but at the same time, it also carries a big element of risk. This paper believes that no single method, algorithm, key or procedure is entirely secure. Hence a combination of multiple security components is mandatory to provide a high level of protection against fraud and other threats. This research is about enhancing the security feature of an ATM by fingerprint verification and the use of confirmation message. It looks into the vulnerabilities of ATM cards, Personal Identification numbers (PIN) or passwords which are widely used in systems today. As a result, the aim of the research is to propose a framework for user identification and authentication in automated teller machines (ATM) as opposed to PIN. This robust method of user identification and authentication would hopefully reduce the vulnerabilities of ATM in the future. The programming language was chosen for its ideal nature for writing windows based application.

Keywords : Fraud, Fingerprint, ATM, Security

Background to the Study

Fraud is increasing rapidly with the advent of modern technology and the global superhighways of banking transaction, resulting in the loss of billions of dollars worldwide each year. Although prevention technologies are the best way to reduce fraud, as banks are trying, fraudsters become so adaptive and find their ways to circumvent such measures that were put in place by the bank. Fraud is increasing dramatically each year resulting in loss of a huge amount of money and data worldwide Devinaga (2010). Banking fraud can be simply described as any activity by which service is obtained without intention of paying. From the definition above, fraud can only be detected once it has occurred. Fraud detection is the identification of fraud as quickly as possible once it occurs. However, fraud techniques are constantly evolving and whenever a detection method becomes known, fraudsters will adapt a new strategy. The banking sector has no doubts has witnessed advancement in technology just like other sector. Usually to perform a transaction a customer has to use an ATM card which is issued by the respective financial institution and a personal identification number (PIN) which is given along with each card for authorization of the customer's account. Nowadays, crimes at ATMs have become an alarming issue. Security for the customer's account is not guaranteed by PIN. Many people, who aren't familiar with the concept of PIN are unlikely to recognize and memorize it. There are many people who mistrust PIN, such as, if they have lost their card, they would feel unsafe that their account could be accessed by others and they would lose all their money. To enhance security and authentication of the customer's account, the concept of using the biometric fingerprint and PIN is proposed in this work, since biometric fingerprint is unique for each and every human being. They are also readily available, fast easy-to-use, accurate, reliable and less expensive Das and Debbarma (2011).

The development of fraud detection methods and the exchange of ideas in it is limited by the fact that it makes no sense to describe the methods in detail, given the difficulty that the banks face in detecting financial statement fraud, coupled with their increasing responsibility to detect it, there is definite need to develop audit procedures or strategies more specifically focused on fraud detection.

Statement of the Problem

The present methods of controlling fraud activities will in no doubt pose tremendous difficulties as earlier discussed due to unreliability of security factors but however, there is need to develop software that will enhance the proper control measures of accurate fraud detection and prevention in banking sector. Due to the problem that led to the low achievement in system, the following questions would be put into consideration. What steps are to be taken to develop the new system? what benefit will the new system be to the management and the reaction of the staff to the new system? How will fraud be detected and in what ways will the menace be controlled? The system design focuses on how to detect fraud and control its menace using an ATM card. In addition to the use of the PIN (personal Identification Number) which provides the authorization to access your account, this work adds the feature of using biometric fingerprint which allows the actual owner of the account to perform transaction by himself and the use of confirmation message in case of a third person performing the transaction.

Aim and Objectives of the Study

This research is aimed at designing a system for fraud detection and control in bank using fingerprint simulation with the following objectives:-

i. To analyze the problem of the existing system.

ii. To design an application software for fraud detection and control within the banking transaction.

iii. To design a system which creates user profiles and compares them with future activities of the user for the identification of latter cases of fraud.

Significance of the Study

In the present system of banking transaction, fraud is very common due to lack of security and user authentication system. However, this work significantly studies detecting and controlling of fraud in banking transaction using ATM Machine. This work lays a solid foundation of monitoring operations so as to detect fraud and its prevention. With an effective internal control system, erroneous and fraudulent transactions and irregularities are less likely to happen in banking transaction via ATM. Ozten *et al*; (2012).

The implementation of the new system includes the following:

i. Security of Customers information about Banking transaction is ensured

ii. Error free in banking activities is enhanced

iii. Retrieval of customer's information is simplified

Definition of Terms

i. Microsoft Visual studio 2010: This is object oriented programming software used for windows based application program.

ii. Detection: The act of discovery or the act fact being discovered.

iii. Fraud: An illegal act that involves obtaining something of value through wilful misrepresentation

iv. Database Management System (DBMS): Is a software system that expands and maintains a database. It provides an interface between the user and the data in any existing database in order to use the data appropriately for decision making process.

v. Biometric fingerprint: are patterns formed on the epidermis of the finger, composed of ridges and valleys which makes the important evident characteristics of the finger.

vi. ATM: Automatic Teller Machine (ATM) is a cash dispenser which is designed to enable customers enjoy banking service without coming into contact with Bank Tellers (Cashiers).

vii. Database: Is a collection of logically related and organized data, with the duplicate of data items been minimized.

viii. Data: Is used to describe basic facts about the activities of a business.

ix. PIN: Personal Identification Number

x. Theft: Unlawful taking of the property of another person.

Literature Review

The Computer Crime Research Centre (2009) opined that the traditional and ancient society was devoid of any monetary instruments and that the entire exchange of goods and merchandise was managed by the 'barter system'. The use of monetary instruments as a unit of exchange replaced the barter system and money as the sole purchasing power. The modern contemporary era has replaced these traditional monetary instruments from a paper and metal based currency to 'plastic money' in the form of credit cards, debit cards etc. As further investigated by Chinedu *et al* (2012), the converging forces of technology have tremendously altered manual systems of delivering banking services and have subsequently paved way for electronic delivery platforms in recent time. The ATMs is one of existing replacements of the cascading labour-intensive transaction system affected through what is popularly referred to as paper-based payment instruments. Chris (2006) in his research on Bank ATM Security Advice states that E-Banking in general and ATMs in particular have given the consumers a quality of life allowing them to access cash and other financial information. Chris (2006) also states that ATM offers a real convenience to those who are on the run in their everyday life, but at the same time it causes a big element of risk. The traditional banking risk, in some instances, are magnified when banks offer 24/7 transactional websites. As banks move into this new territory, several challenges arise in the context of banking risks Anita (2001).

Adepoju and Alhassan (2010) while analyzing the cases of ATM usage and fraud occurrences with some banks in Nigeria discussed that consumers have come to depend on and trust the Automatic Teller Machine (ATM) to conveniently meet their banking needs. They also shared their concern on the growing number of ATM frauds and have suggested using the SMS encrypted messages to authenticate the users to improve ATM security against frauds and crimes. Amurthy and Reddy (2012), proposed the use of embedded fingerprint system, which is used for ATM security application. ATM hacking is now on the rise with some organized and highly sophisticated attacks. This has now become a real headache because both banks and customers are prone to heavy losses. Criminals are taking the battle a stage further, by directly manipulating the software inside the ATMs to give them money. An effective remedy for prevention of ATM frauds, however, cannot be provided unless we understand the true nature of the problem.

The Nature of the Problem

The nature of problem can be best understood by having an insight of the modus operandi used for the commission of ATM frauds. A Report on Global ATM Frauds (2007) identified the following types of ATM Frauds: One method of such is placing a device on an ATM that prevents the machine from reading a card. Once an inserted card is struck a fraudster pretending as a genuine cardholder will suggest that the intended victim re-enter his or her security code. When the cardholder ultimately leaves in despair, the fraudster retrieves the card and enters the code that he has watched clandestinely. Another method involves use of fake cards using data collected from tiny cameras and devices called "skimmers" that capture and record bank account information. This is lesser risky as it does not involve any fraudster-victim interaction and the absence of any fraudster makes the cardholder more relaxed and lesser conscious about the safety of the password. Diebold (2012) explored another interesting method of ATM fraud which involves the use of "duplicate ATMs" by the fraudsters that uses 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 an inside job with the collusion of the employees of the company issuing those cards. Obiano (2009) blamed the menace of ATM frauds on indiscriminate issue of ATM card without regard to the customer's literacy level. Whatever the mode of these frauds, it is definitely illegal and punishable as per the law of the concerned country. The punishment may, however, not bring back the money lost in the process. Thus, the punishment of an offender will though prove deterrent to other offenders yet it may not be the best method of restoration of stolen property. Thus, preventive safeguards and insuring the ATM fraud risks seems to be the right approach.

The solution to the above problems can be grouped as:

i. Solution for banks

ii. Solution for the customers

Solution to the Banks

The solutions for the banks providing ATM services can further be grouped as:

i. Technological solutions, and

ii. Insurance solutions.

(i) **Technological solutions**: These may include:

(a) *Designated time*: The customers can choose times for using ATMs by phone. The customers can change the chosen time any time and even defer total use of ATMs as per their convenience. This method is not only economical but also effective to tackle forged cash card scams as the fraudster has to match not only the password but equally the "timing" as well.

(b) *Microchip technology*: The banks can also provide cards containing a microchip that can make them harder to forge.

(c) *Biometric tokens*: Biometrics tokens are the safest bet for prevention of ATM frauds. The most widely used biometric tokens include those of fingerprints, irises, faces and palms. The fraudster can match everything but he can never match the biometric peculiarities.

(d) *Enhanced security*: The banks may enhance the security features of the ATM's for providing a better service.

(e) *ATM Monitoring*: The banks can monitor ATMs continuously by installing closed-circuit cameras and other devices.

(f) *Customized software*: The banks must use customized software that records relevant information on ATM cards or credit cards so that banks can establish whether an unauthorized ATM transaction has taken place by using a counterfeit card.

(g) *Customer motivation*: The banks must encourage customers to report any suspicious activity on ATMs by providing the basic infrastructure.

(h) *Alerts:* The bank must alert customers if the customized software notes any unusual transaction patterns.

(ii) **Insurance solutions**: The banks must also secure themselves the protection of insurance cover since they may find themselves liable for the payment of money lost due to these frauds. This is generally happening in foreign countries and very soon the same may be the position in Nigeria. In the world of "Internet Banking" no bank can afford to remain indifferent and aloof to this possibility. Thus, an insurance cover is a must for these banks.

Solutions for customers

The solutions for the customers availing ATM services can be grouped as:

(i) Precautionary solutions, and

(ii) Insurance solutions.

Precautionary solutions: It is very important for cardholders to protect their cards from being misused.

Here are some of the measures a cardholder should adopt, to protects their card from being misused:

i. Never leave your credit card unattended in a vehicle or changing room.
ii. Avoid leaving your card loose in pockets or bags.
iii. Always keep your card secure in your wallet or handbag.
iv. Keep a close watch on your credit card and wallet/bag/briefcase in public places.
v. Never allow anyone else to use your card.
vi. Sign new cards as soon as they arrive and cut up old cards when they expire.
vii. When purchasing goods, please be patient if your card is sent for authorization or verification.
viii. If your card is lost, stolen or not received, please inform the card issuing bank/organization immediately.
ix. Always retain sales/charge slips to compare with the amount specified on the billing statement.
x. When travelling abroad or within the country, ensure that you carry the telephone number of the card issuing bank/organization.
xi. Do not disclose your PIN (Personal Identification Number) to anyone.
xii. Always memorize your PIN.
xiii. If you forget your PIN, please contact card-issuing bank/institution and the bank will then send you a new card with a new PIN, on receipt of which you should immediately cut up your old card.
xiv. If your card ever gets stuck in the ATM, do not reveal your PIN even to the concerned bank official/institution. It would suffice to let him / her know that your card has got stuck in the ATM. With the above measures, one could help protect his credit cards from possible misuse.

Insurance solutions: The customers, like banks, can also secure themselves the protection of insurance cover for the money lost due to these frauds. This trend is very popular in foreign countries and very soon the same may find a place in Nigeria as well. As the Internet is becoming popular, many sectors such as banking and other financial institutions are adopting e-services and improving their Internet services. However, the e-service requirements are also opening up new opportunity to commit financial fraud. Internet banking fraud is one of the most serious electronic crimes (e-crimes) and mostly committed by unauthorized users. This research presents a new dynamic key generation scheme that facilitates a fraud prevention mechanism. In the system, a combination of a biometric feature such as a fingerprint and smart card is used to effectively confirm the users' identity and prevents illegal attempts. It also eliminates the need for storing a long-term shared key which makes the system insecure during transactions. We show that the new scheme is secure against various kinds of attacks.

Fraud Detection Methods

Adeloye (2008) identified security as well as power outage as major challenges facing the ATM users in Nigeria. 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.

Fraud Detection Tools

Fraud detection tools should have the sub components to identify fraudulent activities. First of all, suspected transaction detail records have to be collected before the start of detection activity. These activities are as follows;

(i) The ATM cards should be provided with microchip technology that will make it difficult to forge.

(ii) Banks should monitor the ATMs continuously by installing closed-circuit cameras and other devices.

(iii) The banks should install customized software that records relevant information on ATM cards so that banks can establish whether unauthorized transaction has taken place or not.

(iv) Banks must alert customers on any suspicious and unusual transaction on their accounts.

(v) There must be adequate security around the ATM.

(vi) Biometrics tokens are the safest means of preventing ATM frauds. The most widely used biometric tokens today include finger prints, irises, faces and palms. The fraudster may match everything but they can never match the biometric peculiarities. From the list above, biometrics fingerprint is the one that is used in the course of this work.

ATM Fraud Prevention

The below list should be adhered to by all the stakeholders and customers in banking transactions to minimize the ATM frauds in Nigeria.

(i) Customers must ensure that they are not careless about their Personal Identification Number and must not release their cards or delegate anyone to ATM machine.

(ii) To protect themselves from shoulder surfing, customers must ensure that those who are on the queue for similar transaction are far away from where they are doing transaction with ATM machine and cover the panel when typing their PIN

(iii) Illiterate customers should not be issued ATM cards.

(iv) If the ATM of a customer is stolen or lost, the customer should alert the bank immediately.

(v) Sign new cards as soon as they arrive and cut up the old ones when they expire.

(vi) If your card got stuck in the ATM, do not reveal your PIN even to concerned bank officials. It suffices for the official to know that your card got stuck in the ATM.

Analysis of the Proposed System

The main purpose of analyzing the proposed system is to create a system that is capable of meeting the Biometric Security requirements of the user, that is, the system has the capability of improving the method of using only PIN number to secure bank transactions using ATM, and this is done through the incorporation of fingerprint biometrics and confirmation SMS, and it follows the under listed sequences;

i. Customer/User provides his/her PIN number.

ii. Customer/User is verified and authenticated using Fingerprint reader

iii. Customer/User receives confirmation Text Messages alerts for any transaction by third person

iv. Bank staff login to enrolled a new user

Input Analysis:

The input to the system is the Customer/ User information form. This form is used to receive and validate the inputs to the system. The customer fingerprint is collected at the point of opening the account.

Process Analysis:

The information collected from the input system will be queried in the database and if the information matched the one in the database, it is then processed and allows transactions by the customer/user.

Output Analysis

The system provides an interactive user interface through which the customer uses his thumb finger to the hardware biometric fingerprint scanner system. If it is then matched with the one stored in the database, it then allowed transactions. The system prompts "unauthorized usage" of once account and alerts to bank administrators a particular username has been illegally tampered. Login records of the existing system is also being taken care of for further referencing by the administrators for fraud cases.

More of the output generated is on Customers PINs, Withdrawal reports, Deposit reports and other transactions reports.

Problems of the Existing System

The traditional method of using Personal Identification Number (PIN) in fraud detection and control in ATM centres in Banks has shortfalls which includes but not limited to:

i. Using ATM Card and PIN as a password cannot verify the customer/user identity exactly.

ii. The use of PIN number in ATM Banking is a single authentication method and can easily be forged by fraudsters.

iii. Higher privacy concern is required by the customers/users when using PIN password on ATMs.

Justification for the New System

The new system will help to solve all the problems inherent in the existing system. The justification for the new system includes:

i. It's a multiple authentication and verification method that uses fingerprint unique recognition features and this will make the system so secure.

ii. The confirmation SMS added to the system will be useful to the customer/user in case of unforeseen emergency, a nominee user can be sent to perform transaction on his behalf.

iii. Low Privacy concern is required by the customer when performing his transaction on Banks ATMs.

iv. The embedded GSM technique that sends confirmation alerts goes a long way in securing the customer's Account from unauthorized access or fraudulent transactions.

Requirement Analysis for the System Design

Hardware requirement for the system design

i. Biometric finger print scanners

ii. Personal computer with 512 RAM and above,

iii. Hard drive of 100Gigabyte and above

iv. Keyboard

v. mouse

Software Requirement for the System Design

PC with windows such as XP, Vista, Windows 7, 8 and 10 respectively.

ii. Visual studio 2010 (vb.net)

iii. Microsoft access 2010 database.

Advantages of the proposed system over the existing System

The best reason why fingerprint is getting more popular and widely implemented is a convenience of having authenticating mechanisms with a user. It does not need to be memorized and need not to be changed periodically as with passwords. Fingerprint can last virtually forever.

(i) **Uniqueness**: As noted previously, fingerprints are a unique identifier specific to the individual.

(ii) **Security**: Fingerprints cannot be lost or stolen, and are difficult to reproduce. Furthermore, storing fingerprint templates as statistical algorithms rather than complete copies ensures that the ability to reproduce these unique identifiers is significantly reduced.

(iii) **Acceptance**: As most people are familiar with the use of fingerprinting for identification purposes, it is generally accepted as a technology. Most people understand its applicability to access control.

(iv) **Accuracy**: By and large, fingerprint technology is accurate. There is a small chance of rejection of a legitimate print, i.e., there is a chance of accepting a false print or a chance of rejecting a legitimate print. The chances of accepting a false print are very low.

(v) **Ease of use**: Very little time is required for enrolment with a fingerprint scanning system. Unlike other biometric devices, such as retina scanners, fingerprint scanners do not require concentrated effort on the part of the user. Accordingly, one could consider fingerprint scanning to be relatively non-intrusive.

Installation: Changes in technology have made fingerprint scanners relatively easy to install and inexpensive. Most fingerprint scanners are now very small and portable. Plug-and-play technologies have made installation very easy. In many cases, the scanning device has been incorporated into keyboards, mouse buttons and even notebook computers.

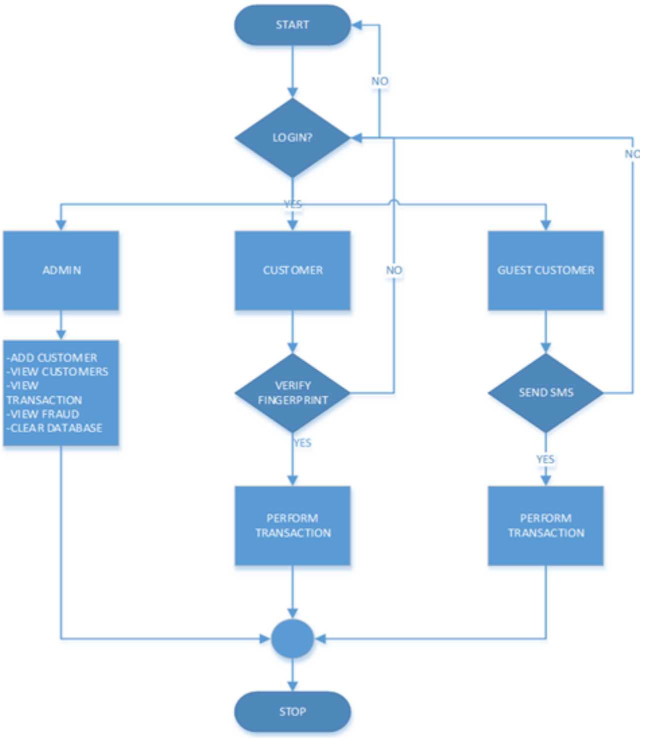


Figure 1 : Flow Chart of the proposed system

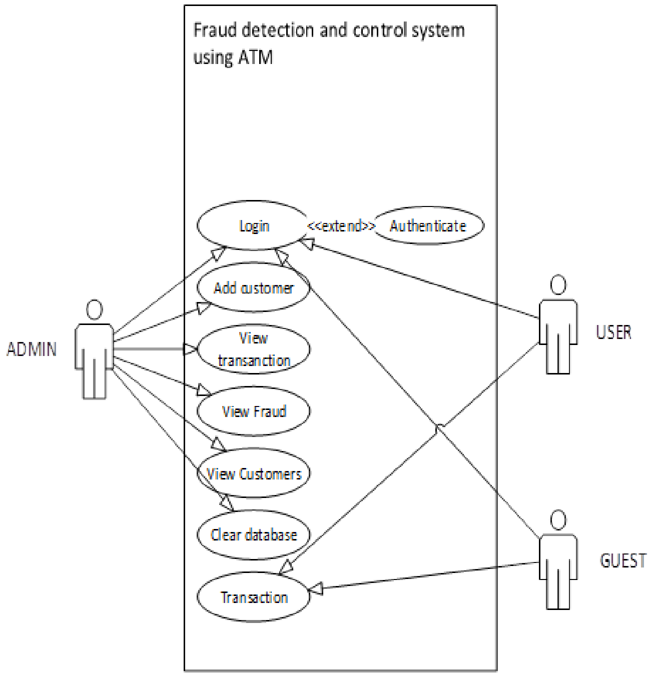
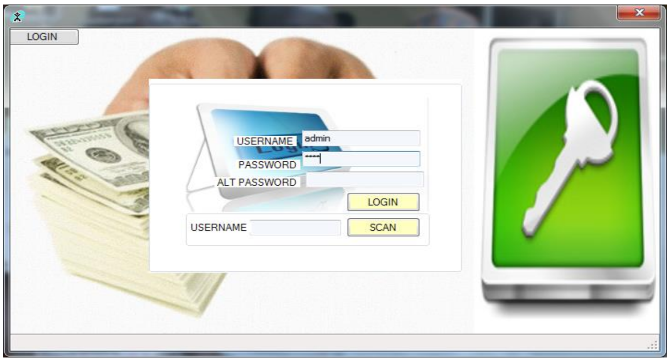


Figure 2 : Use case diagram of the system design

Implementation of the New System

Input Design

The input forms are designs generally based on the necessary data that needs to be entered into the system. In this system, the data are captured through the ATM keyboard and the Fingerprint Sensor on it; the Yes or No confirmation alert message is confirmed through a text from the customer cell phone and stored on a magnetic disk in the database for subsequent query and validation. The new system is composed mainly of one input form i.e. ATM machine form where you enter your 4 digits PIN and the Fingerprint enrolment. This is the login form where the user/admin can login to the system.

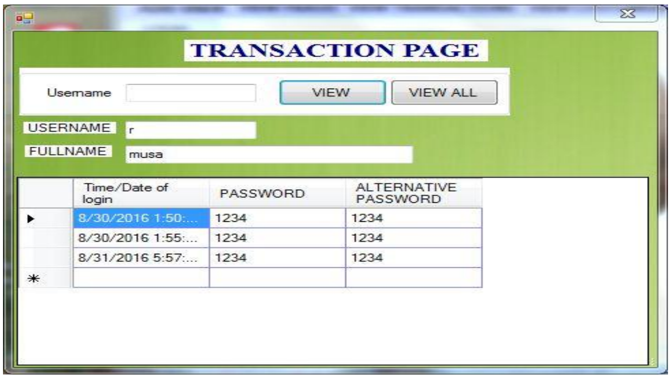


USERNAME admin
PASSWORD ••••
ALT PASSWORD
USERNAME

Figure 4 login form

Output Design

The output design was based on the inputs. The cash collected from the ATM Dispenser, the Transaction confirmation and the various reports generated gives a meaningful report to the Banks management. When the user provides all the required input, the system will process and output the requested result.



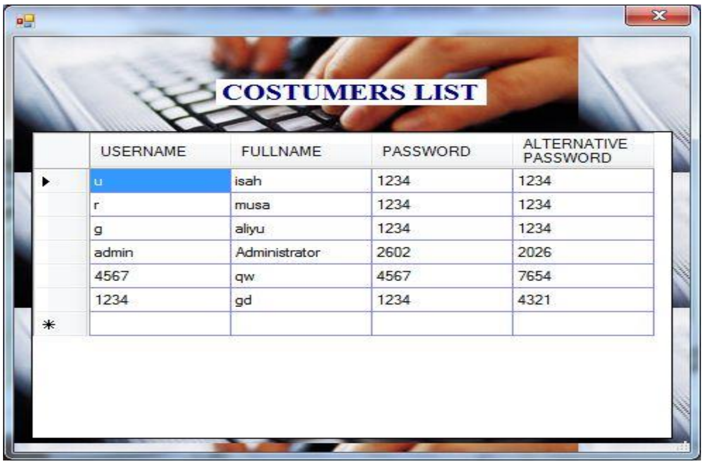
Username
USERNAME r
FULLNAME musa

	Time/Date of login	PASSWORD	ALTERNATIVE PASSWORD
▶	8/30/2016 1:50:...	1234	1234
	8/30/2016 1:55:...	1234	1234
	8/31/2016 5:57:...	1234	1234
*			

Figure 5 Transaction Page

Customers List:

This form keeps records of all customers that have been enrolled. When admin queried for the customer's details, the below form is then display.



	USERNAME	FULLNAME	PASSWORD	ALTERNATIVE PASSWORD
▶	u	isah	1234	1234
	r	musa	1234	1234
	g	aliyu	1234	1234
	admin	Administrator	2602	2026
	4567	qw	4567	7654
	1234	gd	1234	4321
*				

Figure 6. Customers List

Admin Panel

This form contains all the activities that can be perform by the admin. He can view attempts and successful logins, enrolled new user, view transactions, delete customers from the database and view customers list.

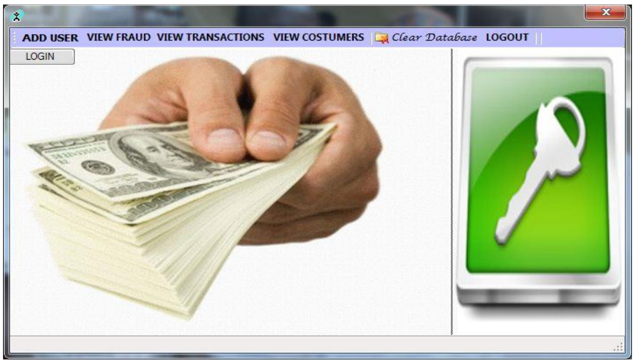
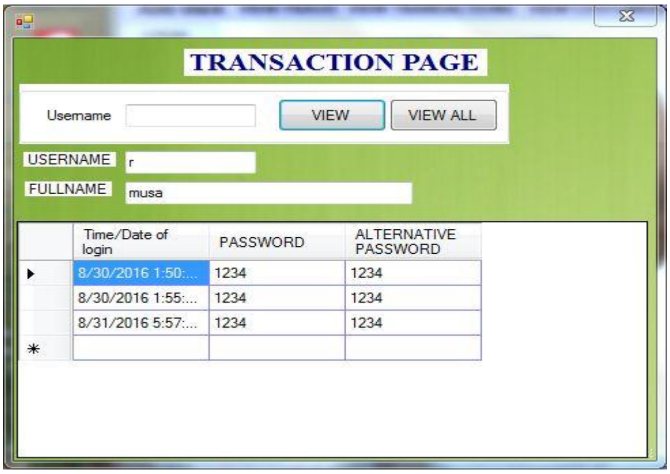


Figure 7. Admin panel

Transaction Page:

This contains all transactions details. It keeps track of the biometrics and the password used to login, the time, date and the alternative password that is used.



Username
USERNAME r
FULLNAME musa

	Time/Date of login	PASSWORD	ALTERNATIVE PASSWORD
▶	8/30/2016 1:50:...	1234	1234
	8/30/2016 1:55:...	1234	1234
	8/31/2016 5:57:...	1234	1234
*			

Figure 8. Transaction Page

Conclusion

The growth in electronic transactions has resulted in a greater demand for fast and accurate user identification and authentication. Access codes for banks accounts and computer systems often use PIN's for identification and security clearances. Conventional method of identification based on exclusive knowledge like a social security number or a password are not all together reliable. Passwords can be forgotten or compromised, but ones' biometric is undeniably connected to its owner. It cannot be borrowed, stolen or easily forged. The incorporation of biometrics, Pin and text message in this work has improved the efficiency and quick service that can be derived from this system and has over weighted the traditional method used in Fraud Detection and Prevention Systems. Despite warning, many people continue to choose easily guessed PIN's and passwords - birthdays, phone numbers and social security numbers. Recent cases of identity theft have heightened the need for methods to prove that someone is truly who he/she claims to be. Biometrics is not only a fascinating pattern recognition research problem but, if carefully used, could also be an enabling technology with the potential to make our society safer, reduce fraud and lead to user convenience by broadly providing the following functionalities which is positive identification, large scale identification and screening. The main purpose of this work is to increase and enhances security on money transactions and has also made ATMs an easier access for the less educated. This method when fully deployed will not only increase the authentication, but will also help in the implementation of complex ATMs. It should be noted that the customers' perception cannot be generalized as it was highly affected by the tradition/culture of the users involves.

Recommendation

To maintain the standard of fraud detection and control in banks using fingerprint Simulation, the following recommendations are made:

i. Awareness should be created on the benefits that can be derived from the use of this software.
ii. There should be time – to – time orientation on the use of computer and this software to facilitate its operation.
iii. Staff should have full orientation on how to use the software to avoid failure.
iv. There will be constant enrolment and reenrolment, of multiple fingers from time to time in order to solve problems of damaged or eliminated fingerprints.
v. The imperfection of this software design should be dully observed and considered by future research.

If a user changes phone number, he/she should report to the bank so that the new number will be linked with their account.

REFERENCES

[1]. Adeloye, L.A. (2008). E-Banking as new frontiers for banks. Sunday Punch, September 14, P. 25

[2]. Adepoju A. & Alhassan, G. (2010). Challenges of Automated Teller Machine (ATM) in Nigeria. Journal of Internet Banking and commerce (JIBC), 15(2), 2-10

[3]. Amurthy P.k. & Reddy M.S. (2012); Implementation of ATM security by using fingerprint recognition and GSM (global system for mobile communication). International journal of electronics communication and computer engineering vol. 3 no1, Pp:83-86. Retrieved from: http://buy.cuna.org/download/diebold_fingerprint paper.pdf

[4]. Anita K. Pennathur. (2001). Clicks and Bricks: E-Risk Management for Banks in the age of the Internet. Journal of Banking and Finance, 2103-2123 http://dx.doi.org/10.1016/S0378-4266(01)00197-2

[5]. Chinedu N. O., Chima B. O., & Emeka E. I. (2012). Analysis of the Negative Effects of the Automated Teller Machine (ATM) as a Channel for Delivering Banking Services in Nigeria.

International Journal of Business and Management,7(7),180-190. Retrieved from http://ccsenet.org/journal/index.php/ijbm/article/view/16034

[6]. Chris E. M. (2006). Bank ATM Security Advice: Effective Method of Security Measures. Virtual Banking. Journal of Internet Banking and Commerce, 11(1) (http://www.arraydev.com/commerce/jibc/)

[7]. Computer Crime Research Center. (2009). Preventive Measures for ATM frauds. http://www.crimeresearch.org/articles/preventive measures-ATM Fraud, (Retrieved 29th March, 2015).

[8]. Das, S. & Debbarma, J. (2011). Designing a biometric strategy (fingerprint measure for enhancing ATM security in India e-Banking system. International Journal of Information and Communication Technology Research Vol. 1 No 5 p 197-203.

[9]. Devinaga R. (2010). ATM Risk Management and Controls. European Journal of Economics, Finance and Administrative Sciences, 21, 161-171. Retrieved from www.eurojournals.com/ejefas_21_13.pdf

[10]. Diebold Corporation, (2012). ATM Fraud and Security (2012).:White Paper, New York Retrieved from www.diebold.com: Accessed September, 12, 2015.

[11]. ICMR. (2007). Report on Global ATM Fraud-2007. Retrieved from www.icmrindia.org/casestudies/catalogue/Business%20Reports/BREP041.htm, accessed July 2015.

[12]. Obiano W. (2009). How to fight ATM Fraud. online Nigeria Daily News, June 21, P. 18 accessed 2015

[13]. Ozten, S. & Kargin, S. (2012) Importance of internal control system in banking sector. p. 133, www.Icbr-archives.com/..../13fec27.pdf