International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2015): 78.96 | Impact Factor (2015): 6.391

Biometric Security Transaction in Banking System: The Automated Teller Machine (ATMs) in View

Ogah, U. S.[1], Ahmed A. M[2]., Adamu G. M.[3]

[1, 2, 3]Department of Computer Science, Federal Polytechnic Mubi, Adamawa State, Nigeria

Abstract: ***Automated Teller Machine (ATM) fraud is a growing problem in the banking sector today all around the world, where fraudsters impersonate, uses wrong Personal Identification Number (PIN) to defraud other customers. This has led to the loss of huge amounts of cash by bank customers and even the banks and has created fear in the minds of the bank customers hence loss of confidence on the bank security for their monies. This is as a result of inefficiency in Personal Identification Number (PIN) and password usage in our current ATMs.This paper try to identify the problems associated with the use of convectional ATMs and went further to propose the implementation of Biometric Security in ATMs transaction in the banking industry. This new system will help stop the problems associatedwith the convectional use of ATMs, hence build customers confidence.***

Keywords: Automated teller machine (ATM), bank customers, biometric security, fraud

1. Introduction

Biometric ATMs are self-service automated teller machines (ATMs), or cash machines, that use a biometric measure to identify customers and allow them to withdraw cash [8].

Biometric authentication may be the only customer identifier used, or it may be used in conjunction with another format, such as a payment card, a mobile device or an additional security credential, such as a PIN [3].

The application of information and communication technology concepts, techniques, policies and implementation strategies to banking services has become a subject of fundamental importance and concerns to all Banks and indeed a pre-requisite for local and global competitive banking [14]. The advancement in Technology has played an important role in improving service delivery standards in the Banking industry. In its simplest form, Automated Teller Machines (ATMs) and deposit machines now allow costumers carry out banking transactions beyond banking hours.

A biometric system is a technological system that uses information about a person (or other biological organism) to identify that person. Biometric systems rely on specific data about unique biological traits in order to work effectively. [9] A biometric system will involve running data through algorithms for a particular result, usually related to a positive identification of a user or other individual. Governments, businesses and organizations can use biometric systems to get more information about individuals or about a populace as a whole. Many biometric systems are developed for security applications [10]. An airport scanning device, a "bio-password" system, or an internal data gathering protocol is an example of a biometric system that uses identifying data for a security result.

More traditional means of access control include token-based identification systems, such as a driver's license or passport, and knowledge-based identification systems, such as a password or personal identification number.Since biometric identifiers are unique to individuals, they are more reliable in verifying identity than token and knowledge-based methods [1].

Figure 1: ATM Machine (Field, 2017)

Businesses are growing at a very fast rate, in line with this growth, banking industry are making frantic efforts to satisfy customers [9]. The fact of marketing concept is that an organization attempts to determine the needs and wants of its target markets and adapts itself to delivering the desired satisfaction more efficiently and effectively than their competitors. The same thing is in line with the banking sector [12]. Nowadays, each bank is searching for alternative way to gain competitive advantage over other banks that is why they keep changing from the conventional system to the computerized system mode of operation [10][11].

The delivery channels today around the world electronic Banking is quite numerous as it is mentioned here, Automatic Teller Machine (ATM), Point of Sales (POS), Telephone Banking, Smart Cards, and Internet Banking etc. Technology must provide security to meet the challenges encountered by ATM customers [2]. [4] Opined that virtually all software and hardware vendors claim to build secure products, but what assurance does an ATM user have of the security of his/her money [9]?

1.1 Problem

Customers want a Bank that will offer them services that will meet their particular needs (personalized Banking) and support their Business goals for instance; businessmen want

to travel without carrying cash for security reasons. They want to be able to check their balance online, find out if a cheque(s) are cleared, transfer funds among accounts and even want to download transaction records into their own computer at work or home. Customers want a preferential treatment and full attention by their choice Bank. All these are only achievable through a secured system like the biometric security.

As a result of this, the paper identified the following problems that are associated with the use of conventional system mode of ATM operation:
1) Increase in ATM fraud
2) Financial insecurity
3) Loss of customer's confidence.

Therefore, the use of biometric security in the banking setup, will solve the problem of customers' dissatisfaction, increase the efficiency of operations and hence help to curb financial crimes in the banking industry particularly in ATM transaction.

1.2 Purpose of the paper

The purpose of this paper is to present a Biometric Security system in the banking setup and particularly in ATMs transaction which will help solve the problems of fraud associated with the convectional ATMs system.

2. Literature Review

2.1 Biometric Overview

The word biometric can be defined as "life - measure." It is used in security and access control applications to mean measurable physical characteristics of a person that can be checked on an automated basis[17].

Although you may not think about it, your driver's license contains biometric information about you. Your height, weight, hair color and eye color are all physical characteristics that can easily be checked. However, your height changes with age (18 years old drivers get taller, senior citizens get shorter). Your hair color changes naturally (and on purpose). You can wear colored contact lenses that change your eye color; everyone's weight fluctuates over time. Security personnel look for biometric data that does not change over the course of your life; that is, they look for physical characteristics that stay constant and that are difficult to fake or change on purpose. Most of us can remember when biometric security checks were the stuff of science fiction or action movies like James Bond. However, biometric identification is becoming commonplace as hardware and software come down in price [17].

2.2Biometric Authentication

[12][13] Refer to the identification of humans by their characteristics or traits. Biometrics is used in computer science as a form of identification and access control. It is also used to identify individuals in groups that are under surveillance.Biometric identifiers are the distinctive, measurable characteristics used to label and describe individuals [6].

Biometric identifiers are often categorized as physiological versus behavioral characteristics.
a) **Physiological** characteristics are related to the shape of the body. Examples include, but are not limited to fingerprint, face recognition, Palm print, hand geometry, iris recognition, retina and odour/scent [6].
b) **Behavioral** characteristics are related to the pattern of behavior of a person, including but not limited to: typing rhythm, and voice.Some researchers have coined the term behaviometrics to describe the latter class of biometrics [6][7].

Biometrics is used to identify the input sample when compared to template, used in cases to identify specific people by certain characteristics [18],[11]. Possession-based uses one specific "token" such as a security tag or card and knowledge-based with the use of a code or password Standard validation system often uses multiple inputs of samples for sufficient validation, such as particular characteristics of the sample[16].This intends to enhance security as multiple samples are required such as security tags or codes and sample dimensions. Recently, a new trend has been developed that merges human perception to computer database in a brain machine interface. This approach has been referred to as cognitive biometrics [5].

3. Methodology

3.1Method of Data Collection

In this research, oral interview was used in data collection as well as data from related textbooks, journals and seminar papers.

3.2 Input and Output Design

The use of controls such as buttons, menus, drop-down menu, textboxes and other kinds of graphical controls were employed in the design of an appropriate graphical user interface for the system, which facilitated good user-system interaction in the data entry process.

3.2.1 Input Design

The data process takes care of different features such as account details, capturing fingerprint and the Iris.

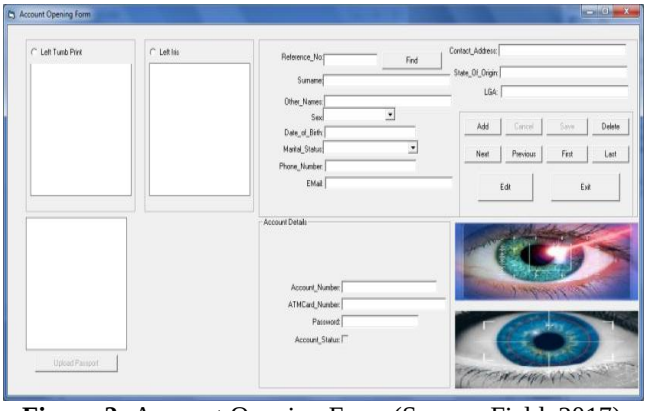

Figure 2: Account Opening Form (Source: Field, 2017)

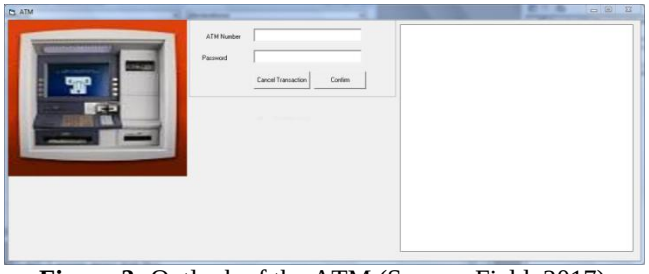

Figure 3: Outlook of the ATM (Source: Field, 2017)

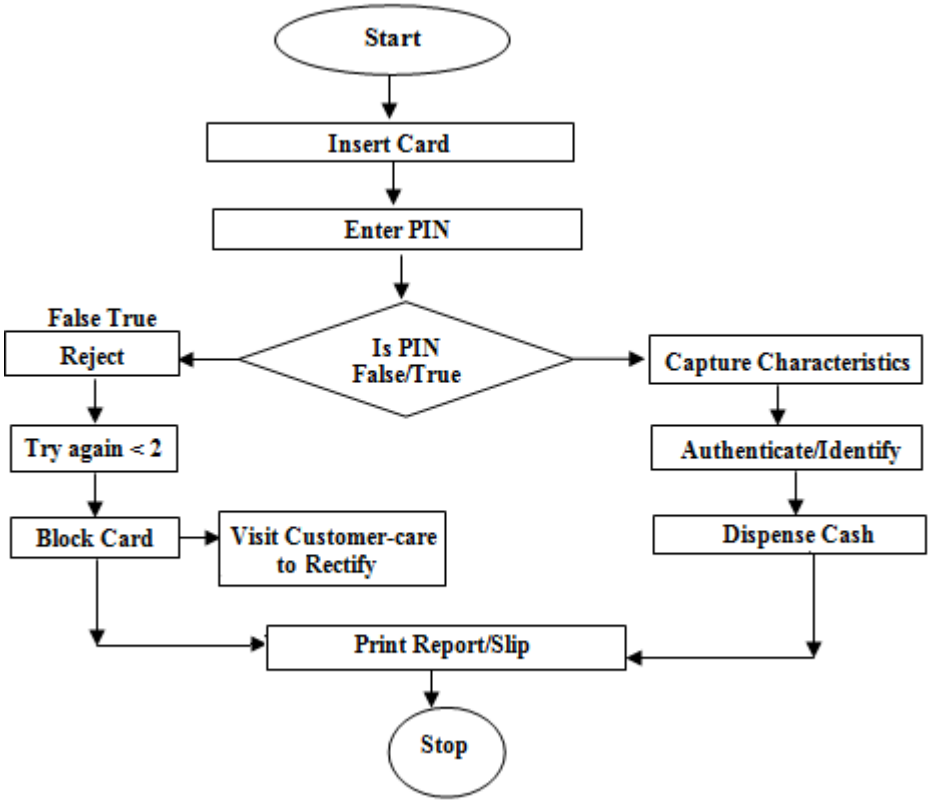

Figure 4: Program Flowchart

4. Results and Discussion

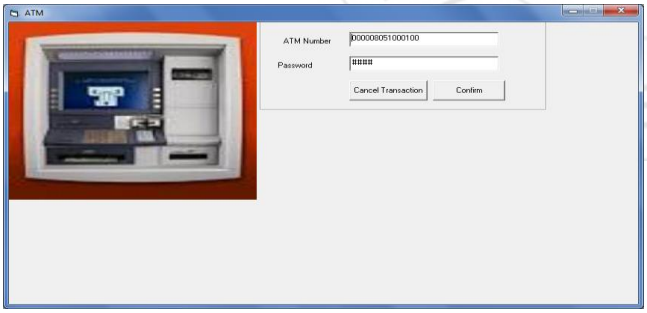

Figure 5: Unsuccessful Transaction due to wrong Pin

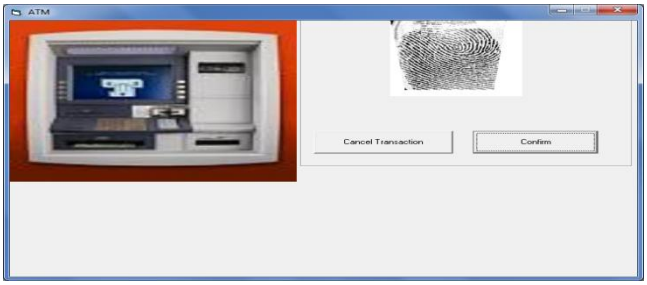

Figure 6: Unsuccessful Transaction due to wrong Fingerprint

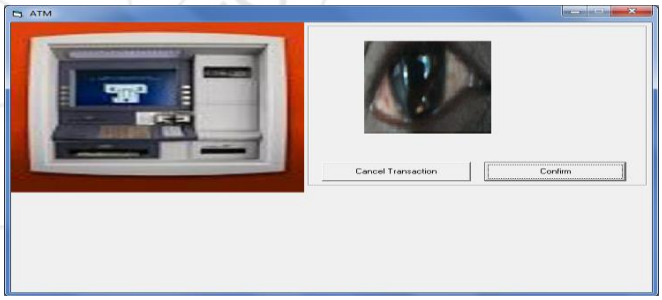

Figure 7: Unsuccessful Transaction due to wrong Iris

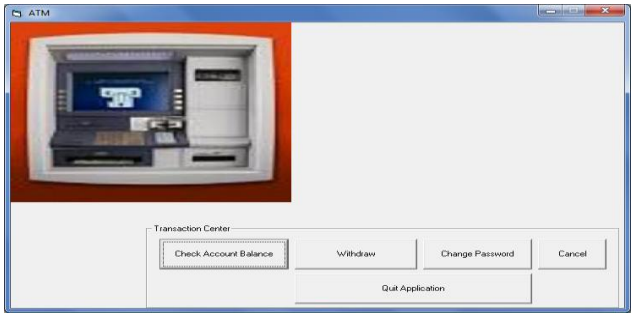

Figure 8: Successful Transaction after all verification confirmed

Table 1: Summary Report of Customers ATM Transaction

transaction_table									
SN	Transact_ Date	Account_ Number	ATMCard_ Number	Pin_ status	Finger_print_ status	Iris_ status	Bal_ Before	Bal Affter	Remark
6	3/2/2013	10020017	2.34E+15	Valid	Valid	Valid	400	400	Insufficient Funds
7	12/2/2013	10020017	2.34E+15	Valid	Valid	Valid	10000	9500	Successful
8	3/3/2013	10020017	2.34E+15	Valid	Valid	Valid	9500	9000	Successful
9	21/3/2013	10020017	2.34E+15	invalid	Valid	Valid	9000	9000	Unsuccessful
10	3/2/2013	10020017	2.34E+15	Valid	invalid	Valid	2000	2000	Unsuccessful
11	3/2/2013	10020017	2.34E+15	Valid	Valid	invalid	6000	6000	Unsuccessful
17	3/2/2013	10020017	2.34E+15	Valid	Valid	Valid	9000	5000	Successful
18	5/2/2013	10020034	2.34E+15	Valid	Valid	Valid	0	0	Insufficient Funds
19	3/2/2013	10020018	2.34E+15	Valid	Valid	Valid	0	0	Insufficient Funds
21	3/2/2013	10020017	2.34E+15	Valid	Valid	Valid	8400	7600	Successful
22	13/4/2013	10020017	2.34E+15	Valid	Valid	Valid	8400	7600	Successful
26	3/7/2013	10020017	2.34E+15	Valid	Valid	Valid	7600	2600	Successful

4.1 Discussion of Results

1) Fig. 5 above shows unsuccessful transaction due to wrong use of Personal Identification Number (PIN).
2) From Fig. 6, there is an indication of failed transaction due to wrong Fingerprint as also appearing in Table 1 above.
3) Fig. 7 shows unsuccessful transaction as a result of wrong Iris
4) While Fig. 8 showcases a successful transaction after all the three features of PIN, Fingerprint and Irish are confirmed right. (See Table 1).

4.2 Summary of Findings

From the results above, it is seen that the biometric features of fingerprint and iris are features for identification in a good security work and hence enhances security. This stands stronger and firm than the convectional system of ATM operations. Hence increase in customer's confidence. This is not limited to banking sector but can be applicable at any point of data security.

5. Limitations

Physiological characteristics pose a little challenge to the system since they are notconstant but can change overtime, however this change takes a long time. The system is cost effective but it implementation will solve the pending problems.

6. Conclusion

This paper presents a biometric security system in the banking sector with emphasis on the automated teller machine (ATMs) transactions which will help put an end to the problems associated with the convectional use of ATMs. This system is to use either physiological characteristics of fingerprint, face recognition, Palm print, hand geometry, iris recognition, retina and odour/scent, etc. or behavioral characteristics of typing rhythm, and voice, etc. or both.

7. Recommendation

As banks focuses more on meeting customers' needs, it is quite important to stress here that for the fight against ATMs frauds to be successful the banks equally need to explore the innovations in today's technological advancements, hence a need to implement biometric security in ATM transaction to help curb frauds in the industry and particularly in the ATMs and give customers confidence in dealing with their banks. The banks should train their staff to enable them acquire the necessary skills needed to manage this innovation.

References

[1] Amedu, K. (2005): Computer and Security, UCLA Computer Science Department, Los Angeles, CA 90024, U.S.A 124-218.
[2] Aran J. G. (1987): Introduction to Computer Intelligence, HarvardComputerTechnology Faculty.
[3] Brisbin, L. L. & Austad S. N. (1993): Animal Behaviour, 13th ICPR, Vienna, 69-78.
[4] Dabbah, M. A. (2007): *Secure Authentication for Face Recognition* Presented at Computational Intelligence in Image and Signal Processing, CIISP 2007 IEEE Symposium.
[5] Dade, L. A. (1998): Human Brain Function and Recognition. A PET study on Annals of the New York Academy of Science, 572-574, 858.
[6] Duncan, J. (1994): A Neural basis for general Intelligence Science, Hasting Law Journal, vol. 70(1), 15 & 42.
[7] Esposito, M. (1999): Context Dependent overall Systematic Specific Neuron-physiological Concomitants of Ageing, Paper Presented at the International Conference on Neurons and Ageing, New York.
[8] http:www.cliab.upf.edu,2011
[9] Leonard G. (1987): Computing Concepts: Technology Education. McGraw-Hill/Iwirn Inc. 100-180, New York, 10020, 2nd edition.
[10] John G. (2003): Biometric Verification: It Implications. Retrieved 23rd September, 2012 from www.cbsr.ia.ac.cn/english/iris.asp
[11] Journal of International Affairs (2000), Vol. 51, 289-301
[12] Kong A, Cheung K, and Zhang D (2006): Impacts of Services equality on customer satisfaction, study online banking and ATM services in Malaysia, an Asia bank report retrieved August 23, 2012 from bank report/conference/banks/IAR-0013673/report.htm.

[13] Kesseunpach, et al (2007): Analyzing the factors that influence the adoption of internet banking in Mauritius. International Banking Journal Vol. 1(2) 44-49.
[14] National Institute of Statistics and Technology (NIST), *Report on Cyber-Crimes* 2002, 23-24.
[15] Oxford Advanced Learners Dictionary, 6th edition, 634 .
[16] Pharnila, H. (2004): Internet banking in Malaysia and customers reactions. International Banking Journal Vol. 1(2) 58-62.
[17] Taizo U. (2001): Security and online Transaction: The Way Forward, retrieved September 14, 2012 from www.cbsr.ia.ac.cn/english/iris.asp
[18] (www.cbsr.ia.ac.cn/english/iris.asp)