ATM Security Using Fingerprint Biometric Identifer: An Investigative Study

Moses Okechukwu Onyesolu
Department of Computer Science
Nnamdi Azikiwe University, Awka
Anambra State, Nigeria.

Ignatius Majesty Ezeani
Department of Computer Science
Nnamdi Azikiwe University, Awka
Anambra State, Nigeria.

***Abstract*—The growth in electronic transactions has resulted in a greater demand for fast and accurate user identification and authentication. Access codes for buildings, banks accounts and computer systems often use personal identification numbers (PIN's) for identification and security clearances. Conventional method of identification based on possession of ID cards or exclusive knowledge like a social security number or a password are not all together reliable. An embedded fingerprint biometric authentication scheme for automated teller machine (ATM) banking systems is proposed in this paper. In this scheme, a fingerprint biometric technique is fused with the ATM for person authentication to ameliorate the security level.**

Keywords- ATM; PIN; Fingerprint; security; biometric.

I. INTRODUCTION

Rapid development of banking technology has changed the way banking activities are dealt with. One banking technology that has impacted positively and negatively to banking activities and transactions is the advent of automated teller machine (ATM). With an ATM, a customer is able to conduct several banking activities such as cash withdrawal, money transfer, paying phone and electricity bills beyond official hours and physical interaction with bank staff. In a nutshell, ATM provides customers a quick and convenient way to access their bank accounts and to conduct financial transactions. Personal identification number (PIN) or password is one important aspect in ATM security system. PIN or password is commonly used to secure and protect financial information of customers from unauthorized access [1]. An ATM (known by other names such as automated banking machine, cashpoint, cash machine or a hole in the wall) is a mechanical system that has its roots embedded in the accounts and records of a banking institution [1]-[2]. It is a computerized machine designed to dispense cash to bank customers without need of human interaction; it can transfer money between bank accounts and provide other basic financial services such as balance enquiries, mini statement, withdrawal and fast cash among others [3].

The paper is arranged as follows. Section II provided the background of ATM security and the need for biometrics. Section III introduced the related works on biometric identifiers. Section IV described the materials and methods employed to conduct the survey. Section V presented the results obtained and the discussions on the results. Section VI concluded the paper.

II. RESEARCH BACKGROUND

Crime at ATMs has become a nationwide issue that faces not only customers, but also bank operators and this financial crime case rises repeatedly in recent years [4]. A lot of criminals tamper with the ATM terminal and steal customers' card details by illegal means. Once users' bank card is lost and the password is stolen, the users' account is vulnerable to attack. Traditional ATM systems authenticate generally by using a card (credit, debit, or smart) and a password or PIN which no doubt has some defects [5]. The prevailing techniques of user authentication, which involves the use of either passwords and user IDs (identifiers), or identification cards and PINs (personal identification numbers), suffer from several limitations [6]. Passwords and PINs can be illicitly acquired by direct covert observation. When credit and ATM cards are lost or stolen, an unauthorized user can often come up with the correct personal codes. 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. Biometric authentication technology may solve this problem since a person's biometric data is undeniably connected to its owner, is nontransferable and unique for every individual. The system can compare scans to records stored in a central or local database or even on a smart card.

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 automated methods of recognizing a person based on a physiological or behavioral characteristic [7]. It is a measure of an individual's unique physical or behavioral characteristics to recognize or authenticate its identity [8]. Common physical biometrics characteristics include fingerprint, hand or palm geometry, retina, iris and face while popular behavioral characteristics are signature and voice. Biometrics technologies are a secure means of authentication because biometrics data are unique, cannot be shared, cannot be copied and cannot be lost.

III. Related Works

Shaikh and Rabaiotti [9] analyzed the United Kingdom identity card scheme. Their analysis approached the scheme from the perspective of high volume public deployment and described a trade-off triangle model. They found that there is a trade-off between several characteristics, i.e., accuracy, privacy and scalability in biometric based identity management system, where emphasis on one undermines the other.

Amurthy and Redddy [6] developed an embedded fingerprint system, which is used for ATM security applications. In their system, bankers collect customers' finger prints and mobile numbers while opening accounts, then customer only access ATM machine. The working of the ATM machine is such that when a customer place a finger on the finger print module it automatically generates every time different 4-digit code as a message to the mobile of the authorized customer through GSM modem connected to the microcontroller. The code received by the customer is entered into the ATM machine by pressing the keys on the touch screen. After entering it checks whether it is a valid one or not and allows the customer further access. Das and

Schouten and Jacobs [8] presented an evaluation of the Netherlands' proposed implementation of a biometric passport, largely focusing on technical aspects of specific biometric technologies (such as face and fingerprint recognition) but also making reference to international agreements and standards (such as ICAO and the EU's ''Extended Access Control'') and discussed the privacy issue in terms of traditional security concepts such as confidentiality. Debbarma [1] proposed an embedded Crypto-Biometric authentication scheme for ATM banking system.

IV. Materials and Methods

The target population of this study was customers and staff of some commercial banks in Awka, Anambra State, South-Eastern Nigeria. The customers and students were randomly selected. The instrument used for this study was a 16-item questionnaire developed by the researchers. The items in the questionnaire were derived from extensive survey of relevant literature and oral interview. The instrument has three sections. The first section deals with participants' profile. The second section deals with participants' use and reliability of ATM. The third section deals with the reliability of fingerprint biometric characteristic. Of the 200 copies of the questionnaire administered, 163 usable copies were returned. This represented 82 percent return rate. This study was carried out over a period of four months. The items in the instrument were analyzed using descriptive statistical methods [10]-[13]. The secondary sources of data were obtained from journals, the Internet and textbooks. Expert judgments were used to ascertain the validity of the items in the questionnaire. Two experts face-validated all the items in the questionnaire. The wordings of items were also checked for clarity. Two items in the questionnaire were deleted for irrelevance while three ambiguously worded items were restructured to reflect clarity. After the corrections, the two experts found the items to be suitable for administration on the subjects. The reliability co-efficient of the instrument was tested by using the Cronbach alpha which is adequate for reliability measure. The instrument yielded a reliability coefficient of 0.81.

V. Results and Discussion

The summary of the results obtained is presented (Tables I – III). Table I shows the profile of participants. The range of age of participants was 20-53 years. 85 males and 78 females took part in the study.

TABLE I. Profile of Participants

No	Profile	Description
1.	Age	20-53 years old
2.	Sex (male: female)	85:78
3.	Bank account and ATM card	Respondents own different types of account depending on the bank, bank products and types of services rendered.

Each of the participants own at least one type of bank account. This depended on the bank, the products offered and services provided by the bank. Banks in Nigeria continually churn out new products and services to have competitive advantage. This resulted to the introduction of ATM and the services it provides.

Table II shows the use and reliability of ATM. 139 respondents representing some customers and staff of some banks, representing 85 percent of the population use the ATM while 15 percent of the population is yet to use the machine. This 15 percent of the population is still skeptical about using ATM because of the issues associated with it. Such issues as inability of the machine to return a customer's card after transaction which may take days to rectify, debiting a customer's account in a transaction even when the customer is not paid and cash not dispensed, and "out of service" usually displayed by the machine which most of the time is disappointing and frustrating among others. 100 percent of the population is aware of one form of ATM fraud or another. Most banks in Nigeria constantly update their customers on ATM frauds and measures to be taken to avert them. 89 percent of the population thinks that ATM transactions are becoming too risky this necessitated 93 percent of the population affirming that they will continue the use of ATM because of security issues associated with the machine. Hence, 100 percent of the population preferred a third authentication aside the use of ATM card and PIN and this population believed that with the infusion of biometrics characteristics to the existing ATM card and PIN, ATM security will be improved drastically.

Table III shows the reliability and popularity of fingerprint biometric character. 74 percent of the population is familiar with fingerprint biometric. 63 percent of the population strongly believed that with the incorporation of fingerprint to the existing ATM card and PIN, will provide a better security to the ATM.

TABLE II. USE AND RELIABILTY OF ATM

No	Question	Responses		Total	Percentage (%)	
		Yes	No		Yes	No
1.	Do you use ATM?	1 39	2 4	163	85	15
2.	Is password (PIN) secured in using ATM?	60	103	163	37	63
3.	How Long have you been using ATM?			163		
	a. Less than a year	23			14	
	b. Greater than one year but less than 3 years	37			23	
	c. More than 3 years	103			63	
4.	Have you ever heard of any ATM fraud?	163	0	163	100	00
5.	Is anything being done about ATM fraud?	150	13	163	92	08
6.	Are ATM transactions becoming especially risky?	145	18	163	89	11
7.	Will you discontinue the use of ATM because of the security issues associated with it?	152	11	163	93	07
8.	Would you prefer a third level security aside card and PIN?	163	0	163	100	00
9.	Have you heard of biometrics as a means of authentication?	143	20	163	88	12
10.	Do you think the use of biometrics can improve ATM security?	163	0	163	100	00

TABLE III. RELIABILTY OF BIOMETRICS CHARACTERISTICS

S/N	Question	Biometric Characteristic	Responses	Percentage (%)
1.	Which of these biometric characteristics have you heard of?	a. Fingerprint	120	74
		b. Iris	9	06
		c. Face Recognition	7	04
		d. Signature	12	07
		e. DNA	2	01
		f. Retina	8	05
		g. voice	5	03
		Total	163	100
2.	Which of the biometrics characteristic will provide better security when fused with the ATM?	a. Fingerprint	101	62
		b. Iris	13	08
		c. Face Recognition	9	06
		d. Signature	12	07
		e. DNA	12	07
		f. Retina	9	06
		g. voice	7	04
		Total	163	100

A. Fingerprint Biometrics

The use of fingerprints as a biometric is both the oldest mode of computer-aided, personal identification and the most prevalent in use today [14].

In the world today, fingerprint is one of the essential variables used for enforcing security and maintaining a reliable identification of any individual. Fingerprints are used as variables of security during voting, examination, operation of bank accounts among others. They are also used for controlling access to highly secured places like offices, equipment rooms, control centers and so on [15]. The result of the survey conducted by the International Biometric Group (IBG) in 2004 on comparative analysis of fingerprint with other biometrics is presented in Fig. 1.

The result shows that a substantial margin exists between the uses of fingerprint for identification over other biometrics such as face, hand, iris, voice, signature and middleware [16].

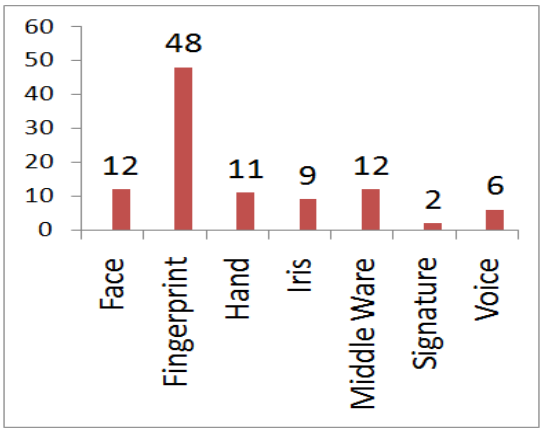

Figure 1. Comparative survey of fingerprint with other biometrics

References [16]-[19] adduced the following reasons to the wide use and acceptability of fingerprints for enforcing or controlling security:

a. Fingerprints have a wide variation since no two people have identical prints.
b. There is high degree of consistency in fingerprints. A person's fingerprints may change in scale but not in relative appearance, which is not the case in other biometrics.
c. Fingerprints are left each time the finger contacts a surface.
d. Availability of small and inexpensive fingerprint capture devices.
e. Availability of fast computing hardware.
f. Availability of high recognition rate and speed devices that meet the needs of many applications
g. The explosive growth of network and Internet transactions
h. The heightened awareness of the need for ease-of-use as an essential component of reliable security.

VI. Conclusion

The growth in electronic transactions has resulted in a greater demand for fast and accurate user identification and authentication. Access codes for buildings, banks accounts and computer systems often use PIN's for identification and security clearances. Conventional method of identification based on possession of ID cards or exclusive knowledge like a social security number or a password are not all together reliable. ID cards can be lost, forged or misplaced; passwords can be forgotten or compromised, but ones' biometric is undeniably connected to its owner. It cannot be borrowed, stolen or easily forged. Using the proper PIN gains access, but the user of the PIN is not verified. When credit and ATM cards are lost or stolen, an unauthorized user can often come up with the correct personal codes. 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. Biometric authentication technology using fingerprint identifier may solve this problem since a person's biometric data is undeniably connected to its owner, is nontransferable and unique for every individual. 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 three functionalities (a) positive identification (b) large scale identification and (c) screening.

References

[1] S.S, Das and J. Debbarma, "Designing a Biometric Strategy (Fingerprint) Measure for Enhancing ATM Security in Indian e-banking System", International Journal of Information and Communication Technology Research, vol.1, no. 5, pp.197-203, 2011.

[2] W.W.N. Wan, C.L. Luk, and C.W.C. Chow, "Customers Adoption of Banking Channels in Hong Kong", International Journal of Bank Marketing, vol. 23, no. 3, pp. 255-272, 2005.

[3] Wikipedia the free encyclopedia, "Biometrics", Downloaded March 20, 2012 from http://en.wikipedia.org/wiki/Biometrics.

[4] B. Richard and M. Alemayehu, "Developing E-banking Capabilities in a Ghanaian Bank: Preliminary Lessons. Journal of Internet Banking and Commerce, vol. 11, no. 2, 2006. Downloaded March 15, 2012 from http://www.arraydev.com/commerce/jibc/

[5] P.K. Amurthy and M.S. Redddy, "Implementation of ATM Security by Using Fingerprint recognition and GSM", International Journal of Electronics Communication and Computer Engineering vol.3, no. 1, pp. 83-86, 2012.

[6] N.K. Ratha, J.H. Connell, and R.M. Bolle, "Enhancing Security and Privacy in Biometrics-based Authentication Systems, IBM Systems Journal, vol. 40, no. 3, pp. 614-634, 2001.

[7] N.K. Ratha, S. Chikkerur, J.H. Connell and R.M. Bolle. "Generating Cancelable Fingerprint Templates", IEEE Transaction on Pattern Analysis and Machine Intelligence, vol. 29, no. 4, 2007.

[8] B, Schouten and B. Jacobs, "Biometrics and their use in e-passport", Image and Vision Computing vol. 27, pp. 305–312. 2009,

[9] S.A. Shaikh and J.R. Rabaiotti,. "Characteristic trade-offs in designing large-scale biometric-based identity management systems". Journal of Network and Computer Applications vol. 33, pp. 342–351, 2010.

[10] C.A. Oyeka, An Introduction to Applied Statistical methods. Enugu, Nigeria: Modern Avocation Publishing Company. Pp. 4, 36, 56. 1990.

[11] E.O. Akuezilo, and N. Agu, Research and Statistics in Education and Social Sciences: Methods and Applications. Awka, Nigeria: Nuel Centi Publishers and Academic Press Ltd, 1993.

[12] J.I. Eze, M.E. Obiegbu, and E.N. Jude-Eze, Statistics and Qualitative Methods for Construction and Business Managers. Lagos, Nigeria: The Nigerian Institute of Building, 2005.

[13] F.H. Zuwaylif, General Applied Statistics. 3rd. Ed., California: Addison Wesley Publishing Company, 1999.

[14] L. O'Gorman, "Overview of fingerprint verification technologies", Elsevier Information Security Technical Report, vol. 3, no. 1, 1998.

[15] G.B. Iwasokun, O.C. Akinyokun, B.K. Alese, and O. Olabode. "Fingerprint Image enhancement: Segmentation to thinning", International Journal of Advanced Computer Science and Applications, vol. 3, no. 1, pp. 15-24, 2012.

[16] C. Roberts, "Biometrics". Downloaded February 13, 2012 from http://www.ccip.govt.nz/newsroom/informoationnotes/2005/biometrics .pdf,

[17] C. Michael and E. Imwinkelried, "Defence practice tips, a cautionary note about fingerprint analysis and reliance on digital technology", Public Defense Backup Centre Report, 2006

[18] M. J. Palmiotto, Criminal Investigation, Chicago: Nelson Hall, 1994

[19] D. Salter, "Fingerprint: An Emerging Technology", Engineering Technology, New Mexico State University, 2006

AUTHORS PROFILE

Moses Okechukwu Onyesolu. Ph.D. in Modeling and Simulation (Nnamdi Azikiwe University, Awka, Nigeria, 2011). Researcher/Lecturer, Nnamdi Azikiwe University, awka, Nigeria.

Ignatius Majesty Ezeani. B.Sc. in Computer Science (Nnamdi Azikiwe University, Awka, Nigeria), M.Sc. Software Engineering (University of Bournemouth, Bournemouth, UK, 2006). Researcher/Lecturer, Nnamdi Azikiwe University, Awka, Nigeria.