Jagannath University Journal of Business Studies, Vol. 3, No. 1&2, 157-166, 2013

INTRODUCTION OF THE BIOMETRIC ATM IN THE BANKING SECTOR OF BANGLADESH: A WAY TO REDUCE THE DIGITAL CRIME

Taslima Akther[1] and Arifin Islam[2]

Abstract

In parallel with the global development, the Banking sector of Bangladesh has gained an admirable progress up to date, with the use of advancement in technology. ATM service is the most convenient service of the bank, but it is not beyond criticism. Identity theft or ATM card frauds has become the most talked topic now a days, whereas Biometric ATM has emerged as a solution to this problem. This study deals with the safety issues of Biometric ATM, as the authors are highly interested whether the Biometric process is safer than the existing traditional ATM. We have found that Biometric ATM is safer than the existing traditional ATM and it can lessen the digital crime such as ATM frauds.

Key words: Biometric, ATM card, Identity theft, digital crime.

1. Introduction

Identity theft has become the fastest growing crime in the world. Identity theft is an activity that takes place when an individual's personal details are taken over or stolen by someone else in attempt to impersonate him/her and have access to particular information or service, perform financial transactions, or even commit crimes (Khouri and Bal, 2013). Identity theft leads to digital crimes such as ATM card frauds. In this world of innovation and use of new technology Implementation of biometric system in securing financial transaction has become a vital concern. Biometric means the use of unique physiological characteristics to identify an individual and to authenticate the person's identity. Various types of physiological characteristics are used for biometric authentication such as fingerprint, facial features, hand geometry, voice, iris, retina, vein patterns, palm print, DNA, keystroke and so on. Adding the human element secure and personalize financial transaction with biometrics. Automated teller machines (ATMs) were the first well-known machines to provide electronic access to customers. With advent of Automatic Teller Machines (ATM), banks are able to serve customers outside the banking hall. It is operated by a plastic magnetic-strip card with its special features. The plastic card is replacing check, personal attendance of the customer; banking hour’s restrictions and paper based verification. ATMs have made hard cash just seconds away all throughout the day at every corner of the globe. ATMs allow doing a number of banking functions – such as withdrawing cash from one’s account, making balance inquiries and transferring money from one account to another using a plastic, magnetic-strip card and personal identification number issued by the financial institution. (Singh & Komal, 2009)

[1] Lecturer, Department of Accounting & Information Systems, Jagannath University, Dhaka-1100

[2] Lecturer, Department of Accounting & Information Systems, Jagannath University, Dhaka-1100

With the expansion of world economy Bangladesh is also trying to keep pace with the development in banking sectors. Identity theft is very common nowadays even in Bangladesh. We may hear the stories of ATM crimes from our nearer ones. Rising menace of ATM card forgery, Bangladesh Bank and commercial banks are yet to come up with reassuring preventive measures. Despite reports of growing incidents of card forgery, the central bank and commercial banks are yet to come up with concrete measures that would assure the clients of the safety of their money. Measures taken so far by the banks are scanty and wrapped in confusion, with some banks still in a state of denial about high-tech forgeries taking place in ATM booths. (Hossain and JebunNesa, 2013).

Although Biometric ATM Card is common in outer world but in Bangladesh, there is almost no instance of using Biometrics in the banking sectors. Recently Prime Bank Ltd. and Dipon Consultancy Services jointly brings a banking service, a Biometric Smart Card based alternate banking service in the brand name "Prime Cash" for the un-banked rural and urban people to address banking needs and payment needs of the broader Bangladesh community. Prime Cash is a Biometric Smart Card where thumb impression will work as authentication code. Fingerprint and Prime Cash Card is all you need to authenticate with the system. (Prime cash, 2014)

1.1 Objective of the Study

Use of the biometric system to authenticate and secure the financial transaction in the banking sector of Bangladesh is a new concept compared to other countries. Banking sector is using the latest technologies to provide the services to their clients. However this ATM card services is no longer safe as the pin number and the card can be stolen by any one and money can be withdrawn by anyone.

The objective of this study is to find out whether the introduction of Biometric ATM card in banking sector of Bangladesh will be safer than the existing ATM card and it will be able to reduce the identity theft or digital crime.

1.2 Overview of the Biometric System

The meaning of the word "Biometrics" is "life measurement". However the term is usually associated with the use of unique physiological characteristics to identify an individual and to authenticate the person's identity. Various types of physiological characteristics are used for biometric authentication such as fingerprint, facial features, hand geometry, voice, iris, retina, vein patterns, palm print, DNA, keystroke dynamics, ear shape, odor, signature and so on. The application which most people associate with biometrics is security.

Biometric identification systems may be broadly classified into physiological and behavioral systems.

Table-1: Classification of Physiological and Behavioral System

Biometrics	
Physiological	**Behavioral**
Face	Keystroke
Fingerprint	Signature
Hand	Voice
Iris	
DNA	

Source: Authors compilation, 2014

1.2.1 Physiological:

This form of biometrics consist of the following forms of recognition

Facial recognition

Face recognition uses the spatial geometry of distinguishing features of the face. It is a form of computer vision that uses the face to identify or to authenticate a person. An important difference with other biometric solutions is that faces can be captured from some distance away, with for example surveillance cameras.

Fingerprint verification based recognition

Fingerprint authentication describes the process of obtaining a digital representation of a fingerprint and comparing it to a stored digital version of a fingerprint. Electronic fingerprint scanners capture digital "pictures" of fingerprints, either based on light reflections of the finger's ridges and valleys, ultrasonic, or the electrical properties of the finger's ridges and valleys. These pictures are then processed into digital templates that contain the unique extracted features of a finger.

These digital fingerprint templates can be stored in databases and used in place of traditional passwords for secure access. Instead of typing a password, users place a finger on an electronic scanner. The scanner, or reader, compares the live fingerprint to the fingerprint template stored in a database to determine the identity and validity of the person requesting access**.**

Hand Geometry based recognition

The enroller places his or her hand on a plate and three sequential images of the hand are taken during the enrollment process. The images are then analyzed based on thickness, length, width and surface area to create a template. When the claimant put his /her hand on the plate for the verification process, a verification template of the hand is created , which is then matched to the enrolment template.

Irish and retinal scanning based recognition

This approach is based on iris and retina of the eyes. The iris and retinal patterns are captured via a video based - image acquisition system. The types of light used is near- infrared light and generated through an LED. The uniqueness of an individual’s iris and retinal patterns helps in identifying and verifying user.

1.2.2 Behavioral

Key stroke

Over a sustained period of computer usage, users develop a distinct way of typing, particularly in the case of frequently typed word such as user name and password. The idea here is to identify the parameters such as the length of time the key remains pressed and the time taken between keystrokes.

Signature verification

This technique involves the dynamic analysis of signature in order to authenticate a person .It is based on the measurement of certain parameters such as speed, pressure, and angle used by the person while he/she is signing.

Speech recognition

This method leverages an acoustic feature of speech which is distinct over individuals. The acoustic patterns such as mouth size and learned behavioral patterns such as voice pitch and speaking style.

1.3 The following table shows the advantages and drawbacks of different Biometric System.

Table-2: Advantage and Drawbacks of Biometric System

Biometric System	Advantage	Drawbacks
Fingerprint verification based recognition	This approach is a proven and highly accurate one. Hence it is used widely and has the ability to enroll multiple fingers.	Impaired or damaged fingerprints can be difficult to verify.
Irish and retinal scanning based recognition	Operations are highly reliable and hand free and characteristics remain stable over a life time.	This is highly sophisticated technology that needs proper training. Sometimes glasses with strong lenses can impact the performance of the system.
Hand Geometry based recognition	This can operate in challenging environments. It is perceived as a non-intrusive and highly perceived technology.	There can be a perception of bio hazards due to potential spread of germs. Possible changes to the shape of hand can lead to failed authentication.
Facial recognition	This can operate without user compliance , work from a distance and leverage existing image database to establish identity	The system is susceptible to error. Non matching depends on item such as camera angle, lighting and facial alterations caused by surgery, accidents and the like.

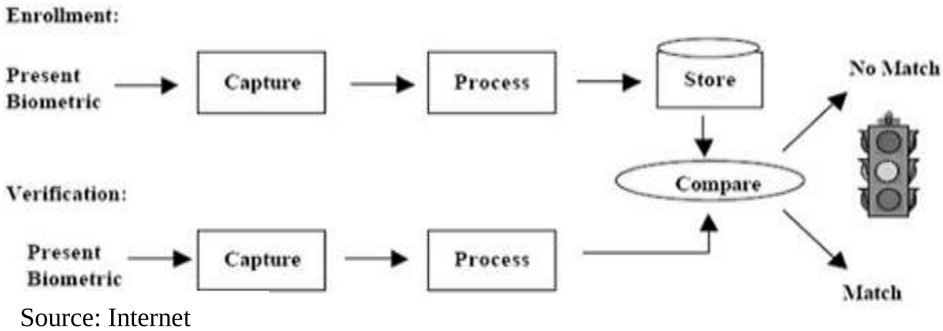
Source: Compiled from the internet, 2014

2. Biometric Authentication Process

Biometric authentication requires to compare a registered or enrolled biometric sample (biometric template or identifier) against a newly captured biometric sample (for example, the one captured during a login). This is a three-step process (Capture, Process, Enroll) followed by a Verification or Identification process.

During Capture process, raw biometric is captured by a sensing device such as a fingerprint scanner or video camera. The second phase of processing is to extract the distinguishing characteristics from the raw biometric sample and convert into a processed biometric identifier record (sometimes called biometric sample or biometric template).

Next phase does the process of enrollment. Here the processed sample (a mathematical representation of the biometric - not the original biometric sample) is stored or registered in a storage medium for future comparison during an authentication. In many commercial applications, there is a need to store the processed biometric sample only. The original biometric sample cannot be reconstructed from this identifier.



Source: Internet

Figure-1: Biometric Authentication Process

Source: Compiled from the internet

Most of the ATM in the past has been using ID cards to identify users but with the wide acceptance of Biometrics, new generations Biometric is being deployed for the wide ranges of Application worldwide.

The method of identification based on biometric characteristics is preferred over traditional passwords and PIN based methods because the person to be identified is required to be physically present at the time-of-identification. Identification based on biometric techniques obviates the need to remember a password or carry a token but a biometric system is essentially a pattern recognition system which makes a personal identification by determining the authenticity of a specific physiological or behavioral characteristic possessed by the user. A biometric system can be either an 'identification' system or a 'verification' (authentication) system, which are defined below.

Identification - One to Many: Biometrics can be used to determine a person's identity even without his knowledge or consent. For example, scanning a crowd with a camera and using face recognition technology, one can determine matches against a known database.

Verification - One to One: Biometrics can also be used to verify a person's identity. For example, one can grant physical access to a secure area in a building by using finger scans or can grant access to a bank account at an ATM by using retinal scan.

2.1Concept of the Biometric ATM

At present our banks are using two factor identification methods. In case of bank check, a piece of paper which is called bank check and a signature is needed over that check to identify and verify the customers or users. In case of On-line authentication a username and password is necessary. ATM is a token based identification system, where a token or a smart card and a pin number of that smartcard provided by the bank is required to identify and authenticate the users. Biometric is a three factor identification/verification method where in addition to the traditional ATM card and PIN, a biometric characteristic such as fingerprint is needed to identify and verify the users of card. The following is the figure of the concept of biometric process:

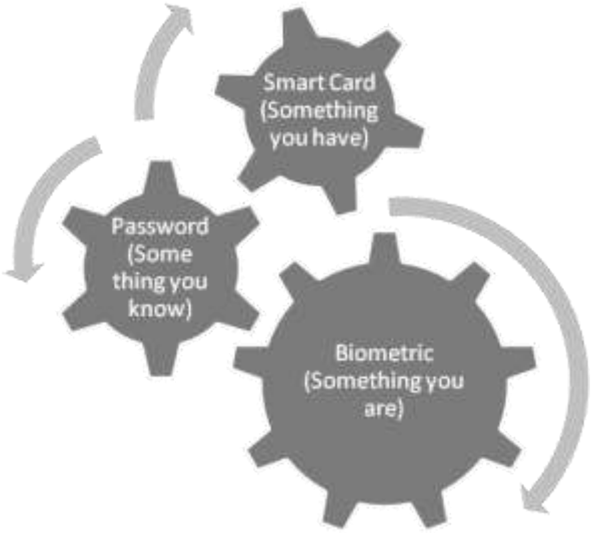

Smart Card (Something you have)
Password (Some thing you know)
Biometric (Something you are)

Figure2: Three factor Identification through the Biometric Process

Source: Authors compilation, 2014

With the present pin based ATM, an ATM fraud has been increased dramatically. The pin number can be shared with others. Criminals can steal or take away the card and pin forcefully and can withdraw money from the ATM booths. It is not possible for the bank to trace the wrong users as the pin number of the users matched with the banks. In addition to frauds and crimes as the pin number can be shared, it can be used by anyone except the true owner. Family members can share the card, then privacy is hampered. Even nowadays banks employees are doing frauds with the clients as ATM Pin can be recorded on booths while customer using their cards, by installing secret camera at the ATM booths.

Biometric process can solves these problems, as it provides strong authentication through the use of biometric characteristics in the authentication process. It is accurate and ensures both security and privacy.

3. Methodology

To accomplish the purpose of the study we have collected primary data by using a questionnaire. Questionnaire included question about the ATM card safety, frauds, crime, etc., and about biometric system. Convenience sampling procedure has been used because of low cost and time and researcher and field worker has the freedom to choose whomever they find. This method is quite frequently used, especially in market research and public opinion survey (M.N.Islam, 2011). The questionnaire was given to different profession people, like banker, researcher, doctor, student, teacher etc. Total 180 respondents were found who has filled up the questionnaire successfully. One of the main purpose of this study was to introduce biometric process for authentication and to see whether people think that biometric process reduces identity theft or is it safer than the traditional ATM? Paired sample t- test has been used to test the hypothesis

H_0: The Biometric ATM and traditional ATM is same regarding the safety issue

$H_{1:}$ The Biometric ATM is safer than the traditional ATM

In our questionnaire we asked respondent to give score on a scale of 10 considering the safety issues of biometric process compared to traditional ATM. These scores were used to test the above hypothesises and paired sample t-test has been used since these two score has come from the same respondent by introducing our respondent to the biometric process of authentication. The test statistics for the paired sample t- test (M.N Islam, 2011) is

$$t = \frac{d}{\frac{s}{\sqrt{n}}}$$

Where,

d = Mean of the difference between the two scores

s = S. D. of the difference between the two scores

$\frac{s}{\sqrt{n}}$ = S. D. of d

4. Analysis and Results

We have already said that main purpose of this study is to introduce biometric to the authentication process and is to see whether it will reduces crime related to traditional ATM. So first we have to see how frequently people using traditional ATM. The following table-2 shows how frequently people uses ATM card.

From the table 1.1 we have seen that most of the people uses ATM 4-6 times in a month that is about 36.1 % , and total percentage of ATM card user is 91.1% while a very few percentage of the people do not uses ATM card or they don't have any bank account. This gives us an idea about how the use of ATM card is increasing day by day.

Table-2: Frequency of using ATM card

No of time use ATM card in a month	Frequency	Percentage
0-3	56	31.1
4-6	65	36.1
7-10	22	12.2
More than 10	21	11.7
Do not uses ATM card	16	8.9

Source: Authors calculation,2014

Since table 2 gives us idea about frequency of using ATM card, table 3 gives us idea about ATM cards crime. To find that we have asked our respondents whether they have fallen in front of criminals or heard from other people or news paper about the ATM card crime.

Table-3: Hearing about ATM crime

Hearing about ATM card crime	Frequency	Percentage
Yes	43	23.9
No	101	56.1
Heard from Other people or Newspaper	28	15.6
No comment	8	4.4

Source: Authors calculation, 2014

From the table 3 we have seen that about 56.1% of people haven't fallen in front of criminals or have no experience about ATM crimes while total 23.9% of the respondent have said that somehow they have fallen directly in front of criminals or couldn't share a experience and 15.6% heard from other people or from newspaper. So total 38.9% of the people somehow know about ATM crimes which is quite a big percentage.

Since one of our objective is to introduce biometric ATM that we have first asked our respondents whether they heard about biometric ATM or not. Table 4 gives us an idea about the what percentage of people know about biometric process

Table-4: Hearing about Biometric ATM

Knows about Biometric ATM	Frequency	Percentage
Yes	103	57.5
No	77	42.5

Source: Authors calculation, 2014

From the table 4 we have seen that 57.5% of the people know about Biometric ATM. 42.5% of the people do not know about biometric which is quite a big percentage. People who don't know about biometric ATM we have given those people idea about biometric process of authentication. After that we have asked the respondents that whether it will be safer than the traditional ATM. The following table display the results of hearing about biometric ATM and is it safer than the traditional ATM.

Table-5: Cross tabulation of Hearing about Biometric ATM and whether it is safer than the traditional ATM

Hearing about Biometric ATM	Safer than the existing ATM			Total
	Yes	No	No comments	
Yes	97	5	0	102
No	58	7	9	74
Total	155	12	9	176

Source: Authors calculation, 2014

From the above table 5 we have seen that total 176 respondents has given the answer to this question. From the table we can see that most of the people who don't know about biometric process of authentication, after knowing about the biometric ATM they have said that it would be safer than the traditional ATM card while only 7 and 9 of the respondent have said that it would not be safer than the traditional ATM and they don't want to comment about this matter respectively. On the other hand respondent who know about the Biometric ATM , most of them (97) have said it would be safer than the traditional ATM while only 5 of them said that it wouldn't be. To know in what respect it is safer than the ATM, we asked our respondent "In what respect they think it is safer than the ATM ". For this question out of 180 respondents 175 has given the answer. The following bivariate table shows the result.

Table-6: Cross tabulation of in what respect Biometric safer than the existing ATM

Safer than the existing ATM	In what respect				Total
	Authentic Verification	Use of physiological characteristic	Every aspects	No comments	
Yes	77	52	19	7	155
No	6	0	0	5	11
No comments	0	0	0	9	9
Total	83	52	19	21	175

Source : Authors calculation,2014

From the above table 6 we have seen that total 77 respondents think that biometric ATM are safer than the ATM because of its authentic verification, while 52 and 19 respondent thinks that it is safer because of the use of use of biological characteristics and in every respect respectively. Thus it can be said that the use of biometric ATM would reduce the identity theft which was one of the main problem of ATM card.

To know further about the safety issues of biometric ATM we have asked our respondents to give score on a scale of 10 regarding the safety issues of biometric

ATM compared to existing ATM. After getting the scores we have used paired sample t-test to test the hypothesis which we have discussed in methodology section. The following table 7 shows the results of paired sample t-test.

Table7: Paired Sample t-test of the Score of Biometric ATM & existing ATM

Mean of the Difference	Std. deviation	Std. error of the mean differences	t	DF	P-value
2.1568	1.89940	0.14611	14.762	168	.000

Source : Authors calculation,2014

From the above table 7 we have seen that p value (.000) of the test statistic is significant at 5% level of significant. So we can say that the null hypothesis that is “biometric ATM and traditional ATM is same regarding the safety issue" may be rejected at 5% level of significant. From this result we can say that introduction of biometric ATM would reduce identity theft and it would be safer than the ATM.

5. Conclusion

Banking sector is the most prominent contributing sector towards the economic development of the country. During the last decade there has been a tremendous change in the banking system. Banks are moving towards the paperless banking rather than traditional banking systems with the use of latest technologies. Now it is possible to get the banking service without going to the bank premises through the use of ATM card. Use of ATM card has made the banking services easier and available to the customers. However ATM card users are facing some problem regarding the authentication and verification as because authentication is based on a secret pin. Anyone can use this ATM card by knowing or stealing secret pin. To overcome the security problem of existing ATM card the concept of Biometric ATM has been introduced. Rather than only secret pin, physiological characteristics are being used to authenticate the true owner. It is general view that biometric ATM is safer than the existing traditional ATM. Our research supports that biometric ATM is safer than existing ATM in many respects and it can reduce to the identity theft or digital crime.

References

1. A.M. Al-Khouri and J. Bal, 2007.Digital Identities and the Promise of the Technology Trio: PKI, Smart Cards, and Biometrics, Journal of Computer Science-Vol.3No .5 (361-367)
2. Biometrics, 2010, Wikipedia, the free encyclopedia, [online] available at: http://en.wikipedia.org/wiki/Biometrics
3. Islam,M.N, 2011. Introduction to Research Methods; A Handbook for Business & Health Research. 2nd ed. Dhaka: Mullick & Brothers.
4 . H.I. Ovi, J.N., Alo, 2013. Rising menace of ATM card forgery, Dhaka Tribune, August 7.p.1b
5. Prime Cash 2014, [online], available at : www.primecash.bd
6. S.Singh, Komal, 2009. Impact of ATM on Customer Satisfaction (A Comparative Study of SBI, ICICI & HDFC bank), Business Intelligence Journal -Vol. 2 No. 2 August (276-287)