Biometric Authentications to Control ATM Theft

Ahmad Tasnim Siddiqui
College of Computers & Information Technology
Taif University
Zip Code: 21974
Kingdom of Saudi Arabia
E-mail: ahmad.tasnim@tu.edu.sa

Abstract - **In the current scenario the way banking and transaction system is changing in the world, the validation, authentication and confirmation of a person is very important and should be of more concern. Authentication and verification has always been the part to worry about the security and confidentiality of the consumers. In the rapid changing environment it's not easy to maintain integrity and authenticity of persons. There is a lot of risk to losing money and identity if we lose our ATM PIN. If it is hacked by someone then we can lose entire money. To prevent all these frauds we need some foolproof security solution which we can use along with the current available technology. Biometric is one of the technologies which we can combine with the current technology. We can use fingerprints, iris scan, palm scanning along with the PIN authentication and verifications. Even we can use voice recognition also. Combination of such technologies may help in reducing the ATM frauds and hence can improve the security level of other financial transactions.**

Keywords: **Biometric security, biometric technology, ATM theft, biometric ATMs, securing user's data and money.**

I. INTRODUCTION

An identity of a person can be referred as personal identification. We can relate it with a person. And we may use it for recognition of a person for verification purpose [1]. Much identification, verification methods are available to recognize the identity of a person. But as many as the methods for verifications and identifications are available almost same thing is with the fraud techniques. There are many techniques available to forge with people. Due to the innovations of ATM machines, consumers were provided an easy and convenient way, 24x7, to make various transactions like check the account balance, withdrawal of money, deposit the money and later features included to allow customers payment of bills, transfer of money etc. With the development of ATM machinery which provides customers and business personnel's to make the transactions by using an ATM card or a debit card or a credit card. There is a magnetic strip in every type of card which has all the data about the customer. An ATM machine reads and authenticates the card and after verifying the magnetic strip, card number, expiration date, and other details customer is able to carry out the transaction. With the progress in technologies there are also the advancement in hackers and criminals in entire world who are responsible for frauds.

Biometric security solution is the way of authenticating physical characteristics of a person e.g. fingerprints eyes and hands to identify and authenticate a person and the products used in this system which includes fingerprint readers and retina scanners [22]. If you are moving towards biometric security solutions, you should have physical characteristics that are stable and unchanged after some time and are also very difficult to fake. Using biometric identity verification and authentication procedure we can get more and more monetary security and protection from all the theft and fraud personnel's. Passwords and PIN numbers are the easy and key targets to be stolen or discovered by any means and after that it can be exploited by people with criminal mindset over the internet and also at other business places. Moving towards biometric security from the traditional PIN code access controlling may reduce the chances of frauds and it may also eliminates the need of multi password authenticity system. We can get entire access control by the finger touch, iris scan or palm touch.

We can divide biometric technology into two broad categories according to what they measure:

Devices based on physiological characteristics of any person (e.g. the hand geometry or fingerprint) and Systems based on behavioral characteristics of any person (e.g. signature dynamics) [18].

Biometrics techniques can be easily adopted along with the traditionally used techniques in financial organizations such as banks, at retail locations to be used with smart cards, ATM machines, credit cards and debit cards, and anywhere you are able to perform a financial transaction. It may work as standalone or in combination with the PIN to securely identify user as the genuine owner of the card and the person who has permission to exchange the money.

II. LITERATURE REVIEW

Due to the outstanding growth in Information and Communication Technology (ICT), security of information is becoming of more challenging in day by day life even as there are many ways and methods available to malfunction of information security. Phishing is one of the great

challenge and threats for website authentication now days. A phishing can be understand as a type of social engineering damage, in this attack hacker designs user's credentials by fraud login page of any trusted well known bank's web site or any other financial organization's website. Spoofing of a bank's website is the biggest issue and it is extremely popular among the hackers.

Net banking or internet banking system needs more consideration for the development and execution of some reliable security system approach [12]. This requisite needs to plan and develop an competent security system that works very efficiently by which consumers can be validated, verified and granted access to the ATM's as well as Internet banking. By using biometric technology we may decrease all types of frauds including phishing etc. Currently when financial system is going through very much in insecurity, many companies are now started realizing the profit of investment to develop and implement biometric security system.

There are many ways for biometric scanning's e.g. retina scan, face recognition, vein geometry, fingerprint identification etc. available and in practice. These can be summarized as:

- **Fingerprint Verification** – The fingerprints of any person remains the same throughout the life and no two fingerprints are ever same. But for this to work accurately it requires clean hands without having any injuries to their prints otherwise it'll prevent proper identification.
- **Face Recognition** – This is one of the most flexible methods as it can be done without the person being aware that they are being scanned.
- **Scanning of Retina** – The pattern of the blood vessel at the back of every eye is absolutely unique and is never changing. The disadvantage of this system is that it takes around 15 seconds of cautious attention to complete a good scan.
- **Scanning of Hand Geometry** – This will work in insensitive working environments. It is not measured as intrusive and often used in industrialized environment.
- **Vein Geometry Recognition** – This is also a very good type of security scan. In vein geometry the geometry of veins in a hand is analyzed and identification and authorization can be done on the basis of result.
- **Iris Scanning** - This is also very difficult to reproduce and stays the same with your entire lifetime. But obviously it is difficult for children and the sick people.
- **Signature Biometrics** – This is easy to gather and is not actually intrusive.
- **Voice Analyzing** - This method of security biometric can be implemented and tested without the person's awareness.

There are still the chances of fingerprint spoofing or creating fake biometrics, but it is absolutely easier to make a replica of a card number.

Many countries are using biometrics technology (fingerprint authentication to be precise) and it has been successful to combat ATM frauds by financial organizations such as the Western Bank in the USA, Barclays Bank in the UAE, Groupo Financiero Banorte in Mexico, Banco Falabella in Chile and many more banks around the world are using biometrics [2].

According to Harris & Spence, financial organizations are increasingly more in danger due to the outsourcing of all secure and important personnel information which can be leaked to their rivals. In addition, Banks and other financial organizations also look for guarantee that information such as the security system, trade secrets, software code, architectures, designs and algorithms are not getting leaked.

According to a report [3], in developing countries, ATM frauds is to committed by in general people who are associated to banks or bank personnel, officers who can very simply provide important information like pin numbers and other significant information to execute such type of crimes. By using biometric security tied up with the current used technologies, such type of incidents can be prohibited and minimized. We can use biometrics as an extra added advantage of verification; authentication and authorization method which make sure that even after the correct pin and having another person's ATM or debit card, a cheater is not able to carry out any type of transaction since the biometric features of all mankind is distinctive and is unable to duplicate.

A survey was done by Biometrics Institute Industry in 2012, which shows the Adoption of Biometrics in our daily life replaced. This was the done in general, in both ANZ and Europe and between both customers and suppliers [7]. The table below shows the adoption of biometric security:

TABLE 1 – ADOPTION OF BIOMETRIC TECHNOLOGY

Most significant development	2011-2012	2010-2011	2009-2010
All respondents (208 in 2012)	Adoption of Biometrics in day by day life	Biometrics at the Border	Increased User Acceptance
ANZ (94 in 2012)	Adoption of Biometrics in day by day life		
Europe incl. UK (61 in 2012)	Adoption of Biometrics in day by day life		
Users (100 in 2012)	Adoption of Biometrics in day by day life		

Suppliers (78 in 2012)	Adoption of Biometrics in day by day life		

III. INVESTING IN BIOMETRIC SECURITY SYSTEM

Now day's biometrics technology is becoming cheaper for both in its application and practice. Financial bodies like banks and other organizations need to think on it and should spend extra effort and money in biometric technology and they should also endorse as a way of securing commercial transactions, across the counter and at the same instance while using the ATM. To provide protection for executing transactions in this manner, financial bodies can also offer more and more extra services at the ATM which can make more profits and slash down on the cost of services [4]. If financial institutions are offering support for different type of services at the ATMs they can decrease the population at the bank counters. This will be a benefit to the organizations because they will absolutely get return in offering the services at the ATM centers.

Biometric technology is being used around the world. For example, In UAE (United Arab Emirates), Barclays Bank has successfully implemented biometric system to secure ATM transactions in the year of 2007 [5]. Barclays enables customers to be authenticated for transactions using fingerprint scanning. Biometrics is very useful to providing confidence and mental peace to bank depositors and consumers successfully.

Fig. 1. Biometric Fingerprint scanner (Image Source: Google.com)

With the advancement of such technologies, we have to further educate customers and clients for the best practice to change their ATM pin numbers. And they should know that not to use common numbers related to that person such as date of birth, car registration number, cell phone digits etc This awareness and education will certainly help everyone to go a long way in reducing the higher level of ATM fraud around the world. Installation of ATMs in a secure, public environment, with CCTV camera may also help out in reducing the ATM frauds [21].

After combining advanced technology with the observations and effective procedures we can get remarkable success but this should be installed at every ATMs.

It's not easy to say that such and such method and technology is the guarantee to prevent ATM frauds. But with the emergence of new technologies like biometrics we can combine with our traditional technologies and get maximum protection from the frauds. According to Hitachi, there's only a 0.0001% chance of somebody having almost same vein patterns as yours [8].

Using biometric technology means after entering your card into any ATM machine you have to put your finger at finger scanner device attached to the ATM adjacent to the keypad. This scanner will identify your genuineness and after that you are able to perform any transaction [22].

When our ATM card and PIN is connected with biometrics then our data is safe and less at risk. From the security point we can say that if we lost our card then there is negligible or no chance to get cash withdrawal done from ATM. Even if the magnetic strip which contains all the information is skimmed then also we are not in worrying condition about the withdrawal of money from ATM.

Fujitsu one of the biometric solution provider, which provides vein pattern recognition (VPR) to ATMs, it facilitates consumers to keep their palms over the scanner on the ATM. The palm scanner emits infrared lights to read the vein patterns. After reading the pattern, it is recognized with the pattern saved in database and finally after verification process the transaction is carried out [9].

IV. WORKING OF BIOMETRIC PROCESS

The detail of the human being which differs from one person to other is used as unique biometric data to provide as that person's unique identification (ID) or recognition. The body parts such as retinal, fingerprint, iris, palm print and DNA. Biometric system collects and stores this data in order to verify any person's identity. The combination of biometric data and biometric identification/recognition technologies creates the biometric security systems. Biometric system is more and more personnel than anyone's passport [6].

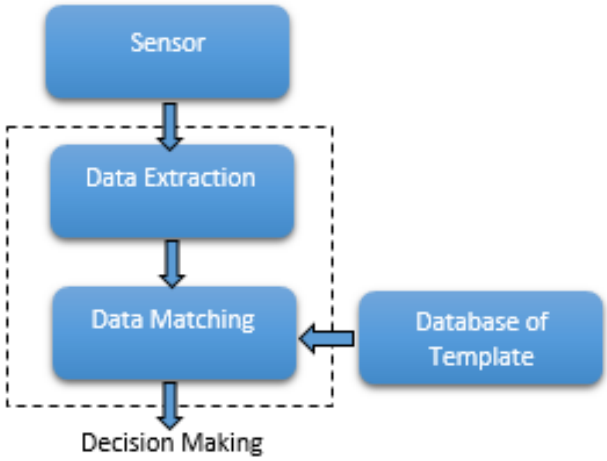

Fig. 2. Block diagram of Biometric Process (Image Source: http://www.fidis.net/resources/deliverables/hightechid/int-d32000/doc/23/)

The functionality of block diagram of biometric system can be explained in below steps [16]:

1. Capturing biometric data: When user places the finger or palm at the sensor, the biometric data is presented to the capturing device.

2. Pre-processing stage: This is the stage before the feature extraction. Here biometric data is recorded and pre-processed by improved input from the sensor. It removes extra noises and distortions. The input is maintained to get the required format for maximum extraction.

3. Feature extraction: In this stage, the pre-processed data is extra processed and features are extracted in a best possible way. Because not all the data captured is required for biometric assessment.

4. Template creation: After feature extraction process is complete, a template is created from entire significant characteristics taken out from the users. The unnecessary data which is not required for the comparison algorithm is washout to reduce the file size and protect the privacy and security of user identity.

5. Storage of the template: Here template is get stored in reusable database, which can is needed at the time of execution of the matching process.

6. Matching phase: This is the last step that involves an algorithm to perform a comparison between the template already stored in the database and the template obtained for decision making. After the decision making the result is then passed on to some application device for further actions.

V. BENEFITS OF A BIOMETRICS SECURITY SYSTEM

Using biometric devices over the traditional security devices has greater advantages. As everything is going global and more and more transactions are taking place through online, banks and other financial organizations people are implementing biometrics to secure the identity and money. Benefits of biometric security can be given as:

- There are possibilities of hacking keys or duplicated; signatures could be forged, passwords could be easily stolen or hacked by a specialist people. To avoid all these accidental losses; we should enter biometric security and all our fears could be laid to rest. Biometrics security system simply allows identifying yourself by your inherent biological features like eye, finger prints, voice; facial characteristics etc. by verifying your biological or physical characteristics you can authenticate yourself very easily just like your signature on a check.
- Signature biometric security verifies the way the user signs his name. In this technique the speed and pressure applied by the user is measured. This type of verification is done normally in transaction related operations.
- In every type of biometric security verification, the finger print is used heavily. It is still playing a most important responsibility in biometric security system. When the user's or approved person's finger print is entered into the security system only he or she is able to access the computer or can proceed to a secure region. Biometric devices verify every time you try to enter. So, they are allowing only authorized people to proceed and hence reducing the chance of frauds up to negligible level.

VI. USAGE OF BIOMETRICS IN INDIA: CASE STUDY

A Pune, India, based technology company, Axis software, has developed Bio-ATM, which is a biometric based automated teller machine for banks and other financial organizations which controls biometric technology to allow safe and secure ATM transactions. This is the first time in India's history that any company has developed such type of ATM machine. The Bio ATM provides an option to the traditional card and pin based authentication ATM systems [13].

According to the President and CEO, Axis Software, "We are using scanning and matching algorithms that are approved by FBI. We can also offer iris recognition, palm scanning etc if required. According to the Axis software there ATMs are suitable for all popular Switch Protocols as well as popular middleware; anybody can even replace

existing machines with the Axis Bio-ATM without a problem."

In India, first movers in the biometric ATMs include ICICI Bank, Punjab National Bank (PNB), United Bank of India (UBI), CITIBANK, Bank of India (BOI), and so on. Punjab National Bank (PNB) installed its first biometric ATM system at a village in Uttar Pradesh (UP) to help uneducated and semi-educated consumers to perform basic ATM operations through voice assistance and fingerprint recognition. The bank is planning to serve more than 30,000 villages, 15 million households, and 80 million people. PNB is aiming to open around 100,000 biometric ATMs by the end of 2013 [14, 15].

The second largest bank of India, ICICI Bank also came up with IIT Chennai with the aim of launching a biometric ATM-based pilot project in Andhra Pradesh at Guntur district. ICICI was the first bank in India who launched a biometric ATM in May 2005 at Guntur district of Andhra Pradesh. ICICI Bank introduced a biometric enabled smart card in 2006, which allows banking transactions to be conducted on the field. United Bank of India (UBI) has moved one step ahead and launched a solar-powered and voice-enabled biometric ATM in rural areas of Ludhiana district of Punjab. This ATM provides support for both biometric and PIN-based transactions and consumes much less power than the usual ones as it is operated by solar energy [16].

In India there is National ID (UID) program running, which is called as Aadhaar. Currently this is the biggest biometric database in the world. It is a biometric technology based digital identity. This can be instantaneously verifiable online at the point of sales/service (PoS), at anytime, from anywhere, in an electronic way. According to the Wikipedia source, currently there are approximately 500 million people (5 billion fingerprints, 1 billion iris images, 500 million face photos) registered with approximately 6 peta byte of database size. The programme is for every Indian national and hence it is expected to reach 1.25 billion people in coming years, with 15 PB of database size and over 200 trillion biometric matches per day [18]. According to the Infosys co-founder *Nandan Nilekani*, who has also the prime role behind the project, says Aadhaar is on track to enroll about 60% of India's people by the end of 2014. It is till now the fastest, largest and the most accurate biometric database in the world. These days most of the Banks are willing to implement the biometric authentication and authorization of customers, linking all of them to the existing Aadhaar database, in a phased manner. According to Mohan V Tanksale, chief executive, Indian Banks' A ssociation (IBA), "We are not averse to it (biometric verification). We are open to do it in a phased manner". But the move will be welcomed, if implemented, would enable biometric authentication and verification of credit cards, debit cards at PoS (point of sale) terminals as well as in all ATMs. Biometric authentication and verification has been a contentious problem with banks, that's why they had migrated from magnetic strip cards to comparatively safer chip and PIN-based cards to cope with the frauds. Some banks have already started working on biometric authentication. All banks would have to think about the cost to reconfigure software and equip each and every branches, ATMs and also PoS terminals with biometric readers [20].

VII. FUTURE OF BIOMETRIC TECHNOLOGY

It's never easy to predict anything in the area of development of technology. But further growth and development of biometric technologies will significantly the complete system significantly. These technologies are surely not to just put to use in making the business easier, additionally they will perform the accurate invigilation and authentication. Hope it will not be hindering the development of these techniques [19]. There are concerns about the basis of Biometrics that Biometrics are not secret, Biometrics cannot be revoked, Biometric traits are not always invariant, Biometrics have secondary uses, How reliably unique the biometrics are [17]? Although biometric technologies are mainly being used for verification and authentication purposes in a various situations they are growing and rising en route to be extensively used in future. In near future, biometrics is going to be integrated more and more in e-business activity, e-commerce and access to homes, access to cars and even cell phones. Apple has already started biometric access in its iPhone 5S model. One of the most important changes in ATM technology could be the scanning of cheque and automatic deposit into the account. There are some more technological innovations which assure for extensive usage of biometrics technology in future [11]. They are:

Access control using facial recognition: Presently there are many biometrics security devices which are using 3D infrared facial recognition system to recognize the identity of a person which requires a person to come close enough to be authenticated. But in near future this technology may be more advanced and strengthened by making the identification of a person easier and even few feet far from the camera.

Facial recognition passive observation: In this type of biometric system, a camera will be place to monitor entrance of any building and it'll spot any unknown or unauthorized individual under few seconds and then transfer the alert to the security control room and security in charge on duty in real time.

VIII. CONCLUSION

As we can see that security concerns have risen to very high levels as terrorism and other unseen dangers are around which cause huge damage to human life and intellectual property. To safeguard against all these high quality technical attacks and intrusions we need equally sophisticated biometric security systems. Biometrics security system has revolutionized the way people generally perceive security. The only hurdle to deploy these seemingly fool-

proof security measures is people's acceptance. Once issues and objections like invasion of privacy, undue physical harassment etc. are sorted out, biometrics security products will have more acceptance from people and will work out as the most effective security system ever. Biometric systems along with the existing systems and technology can produce a very well protected system where consumer can have rest from all their worries related to the money theft, identity theft etc.

REFERENCES

[1] Anil K. Jain, Ruud Bolle, Sharath Pankanti, Biometrics: personal identification in networked society

[2] Traceless Biometric Technology, URL: http://innovya.com/tag/atm/

[3] Use Biometrics To Tackle ATM Fraud, URL: http://www.thenigerianvoice.com/nvnews/15393/1/use-biometrics-to-tackle-atm-fraud.html

[4] http://www.thenigerianvoice.com/nvnewsthread2/15393/6/

[5] http://www.arabianbusiness.com/index.php?option=com_pressreleases&view=detail&Itemid=77&pr_id=6507

[6] BBC "Biometrics Technology", URL: http://news.bbc.co.uk/2/shared/spl/hi/guides/456900/456993/html/

[7] Biometrics Institute Industry Survey 2012, URL: www.biometricsinstitute.org

[8] HITACHI VeInID documents, URL: http://www.hitachi.eu/veinid/documents/hitachi_vein_16pp.v6.pdf

[9] ATM Marketplace, URL: http://www.atmmarketplace.com/article_print/129761/ATM-security-in-Asia-moves-to-veins

[10] Find Biometrics, Global Identity Management, URL: http://findbiometrics.com/solutions/facial-recognition/

[11] Future of Biometrics technology, URL: http://www.articlesbase.com/tools-and-equipment-articles/what-is-the-advantage-of-biometric-security-products-2398403.html

[12] L. Harris & L. J. Spence. "The ethics of e- banking". Journal of Electronic Commerce Research. VOL. 3, NO. 2,2002

[13] India's First Bio-ATM From Axis , URL: http://www.cxotoday.com/story/indias-first-bio-atm-from-axis/

[14] http://www.business-standard.com/article/finance/pnb-to-open-100-000-biometric-atms-by-2013-109121400053_1.html

[15] Siddiqui, Ahmad Tasnim; Muntjir Mohd.; A Study of Possible Biometric Solution To Curb Frauds in ATM Transaction, IJASCSE, November 2013

[16] http://www.infosys.com/FINsights/Documents/pdf/issue10/financial-transactions.pdf

[17] M. Fahim Zibran, Biometric Authentication: The Security Issues, Technical Report #2012-02, University of Saskatchewan, Canada

[18] Ayhan EMRE, Biometric Security Technologies

[19] Wieslaw Bicz, Future of biometrics, Whitepaper available at http://www.optel.pl/article/future%20of%20biometrics.pdf

[20] M Allirajan, "Banks for gradual introduction of biometric verification", article available at http://timesofindia.indiatimes.com/city/coimbatore/Banks-for-gradual-introduction-of-biometric-verification/articleshow/45590601.cms

[21] Ahmad Tasnim Siddiqui and Mohd. Muntjir, "A Study of Possible Biometric Solution to Curb Frauds in ATM Transaction", IJASCSE, Volume 2, Theme based issue 3, 2013.

[22] Ahmad Tasnim Siddiqui " Biometrics to Control ATM scams: A study", ICCPCT-2014, IEEE Conference, pp. 1598 – 1602, Mar 2014.