A Study of Possible Biometric Solution to Curb Frauds in ATM Transaction

Ahmad Tasnim Siddiqui
College of Computers & Information Technology
Taif University
Zip Code: 21974
Kingdom of Saudi Arabia

Mohd. Muntjir
College of Computers & Information Technology
Taif University
Zip Code: 21974
Kingdom of Saudi Arabia

Abstract - **In the modern growing world, the authentication and verification of a person is of more concern. It has always been the area to worry about the security and confidentiality of the consumers. In the complex and fast moving world it is not an easy task to maintain the authenticity and integrity of consumers. While getting money out of the ATMs, a PIN is required and if that PIN is hacked by someone then consumer can lose our money and other identities. To overcome from the current problem, banks and financial organizations can have a security solution which can combine the current technology with biometrics using physical characteristics like fingerprints, eyes and hands scanners to authenticate a person. It may prevent the ATM's frauds and can improve the security level of other financial transactions.**

*Keywords***:** **Biometric security, biometric ATMs, securing user's money.**

I. INTRODUCTION

Personnel identification is known as association of an identity with a person. It can be further divided into verification and recognition [1]. There many verification and identifications method available. But same is the case with fraud. There is also many fraudulent techniques available. Due to the emergence of ATM machines, customers were allowed a convenient way, round the clock, to carry out various transactions like withdrawal of money, deposit the money, check the account balance, and later features included to allow customers pay bills, transfer of money etc. By the invention of ATM technology which allows customers and business personnel's carry out the transactions using an ATM card or a debit card or a credit card. An ATM machine authenticates the card by reading and verifying the magnetic strip, card number, expiration date, and an already provided ATM PIN number. With the advancement of the technology there are also the advancement in hackers and criminal minded people around the world who identify and exploit to perpetuate fraud.

Biometric security is the science of authenticating physical characteristics e.g. fingerprints, eyes and hands to identify and authenticate a person and the products used in this system include fingerprint readers and retinal scanners. When you are considering biometric security, you want to have physical characteristics that are constant and do not change over time and are also difficult to fake or change on purpose. Biometric identity verification and authentication provides more and more monetary security and protection from identity theft and hacking personnel's. Passwords and PIN numbers are the major target to be stolen or revealed and afterward exploited by people with criminal mentality over the internet and also at banking and business networks. Switching from conventional security procedures to biometric physical access controlling eliminates the need for multi password system and different processes and integrates entire access control into one touch of the finger, scan of the eyes etc.

These days, security of financial and transactional data and identity theft protection are more of an issue rather than early years. Have you ever panicked because you lost your money folder, along with all of your credit cards and debit cards in it? Are you worried to bank through internet banking or online banking because of your information will be stolen, and also your money?

Biometrics technologies can be easily integrated with the financial organizations such as banks, ATM machines, at retail locations to be used with smart cards, credit cards and debit cards, and anywhere you may make a financial transaction. It will act on its own or in conjunction with your PIN to securely identify you as the owner of the card and the person who has access to the money being exchanged.

If a database of known person has been developed then it is possible to answer the question of the identity 'who are you?' The biometric of any unknown person can be compared against the database in a search. Their identity can be determined if their biometric has been entered onto the database on a previous occasion; this is much and more quick than a manual system. There should have high quality data needed if the database searches are to give accurate and instant results.

II. LITERATURE REVIEW

With the remarkable development of Information and Communication Technology (ICT), security of information is becoming more invasive in day by day life even as there are many ways and methods to hit on websites with this great development and improvement of information security. Phishing is one of the great threats to web authentication now days, where a phishing is a type of social engineering attack, by designing user's credentials by hoaxing the login page of any trusted well known web site. Spoofing or hoaxing of a bank's website is extremely popular among the hackers.

Internet banking requires attention to the development and implementation of some trustworthy security approach [13]. This requirement needs to design and develop an efficient technique that works efficiently by which consumers or users can be authenticated and granted access. By using biometric technology all types of fraud can reduce including phishing; spoofing etc. fraud prevention can be made easier, and also able to decrease the risk of identity theft. Biometric is making financial transactions more and more secure, safer for businesses personnel's and consumers both. These days when economy is going through uncertainty, many companies are realizing the benefits of investment to implement biometric technology. The money saved by doing so far more significant than the initial outlay, and for the peace of mind which is priceless.

There are many types of biometric scanning's e.g. face recognition, fingerprint identification, retina scan, vein geometry etc.

- **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. This system analyzes specific features that everyone's face has like the distance between the eyes, width of the nose, position of cheekbones, jaw line and chin to only name a few.
- **Fingerprint Identification** – 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. This will not work properly in few industries like automobiles where workers hands are not so cleaned and are always dipped in oil or grease.
- **Geometry of Hand** – This will work in insensitive working environments. It does not require very clean hand conditions and uses a small dataset. It is not measured as intrusive and often used in industrialized environment.
- **Scan of Retina** – There is just no recognized way to duplicate a human retina and, as far as it is known, 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 but this is still a standard approach in military and government organizations.
- **Iris Scan** - 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.
- **Vein Geometry** – 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.
- **Signature Biometrics** – This is easy to gather and is not actually intrusive.
- **Voice Analysis** - This method of security biometric can be implemented and tested without the person's awareness. Even though it is easier to forge by using a soundtrack but it cannot be done by trying to reproduce another person's voice.

There are still the concerns of fingerprint spoofing or creating fake biometrics, but it is definitely easier to clone a card number, as it is now a day's practiced.

In different countries, biometrics technology (fingerprint authentication to be precise) has been successfully used to combat ATM fraud by financial institutions such as the Western Bank in the USA, Barclays Bank in the UAE, Groupo Financiero Banorte in Mexico, Banco Falabella in Chile etc [2].

According to Harris & Spence, 2002, banks are gradually more threatened by the outflow of all secure and personnel information which can be offered to their competitors. Additionally, Banks also want assurance that information resources such as the security system, software code, trade secrets, architectures, designs and algorithms are not getting out [14].

According to reports [3], in developing countries like Nigeria, ATM fraud appear to be committed by typically persons who are linked to bank officers who are very easily able to provide pin numbers and other significant information essential to perform such type of crimes. With the use of biometric security along with the traditional technologies, such type of fraudulent incidents can be prevented and minimized. Biometrics can be used as an extra added layer of authentication and authorization process which ensures that even with the correct pin information and in control of another person's ATM card, a cheater will not be able to perform any transaction since the biometric features of every human being is unique.

The uninterrupted usage of services such as the ATM will rely to a certain extent on public observation and self-belief that it is safe and secure to use it for day by day transactions which includes cash withdrawals, payment of bills, prepaid phone recharge and top up, and a lot of other transactions which at the time can only be performed out by actually going to the local bank [4].

III. INVESTING IN BIOMETRIC SECURITY SYSTEM

Now days biometrics technology is becoming cheaper and cheaper for both in its application and usage. Financial organizations need to spend more money in this technology and they should promote as a way of securing business transactions, across the counter and at the same time while using the ATM. To provide security for performing transactions in this manner, financial organizations can offer more and more services at the ATM which can produce more profits and cut down on the cost of services offered from counter to counter [5]. If financial institutions are providing different type of services at the ATM centers they can reduce the load at the bank counters. This will be an advantage to the organizations because they will definitely get return in providing 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 [6]. 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.

With the advancement of such technologies, banks and other financial organization 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.

After combining advanced technology with the observations and effective procedures remarkable success can be obtained 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 [9].

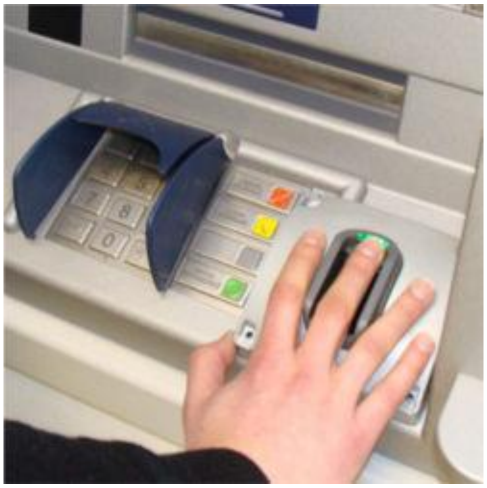

Fig. 1. Biometric (Fingerprint scanner) ATM. (Image Source: http://cacm.acm.org/news/95831-biometric-atm-gives-cash-via-finger-vein-scan/fulltext*)*

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.

When our ATM card and PIN is connected with biometrics then our data is safe and less at risk. From the security point it can be said 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 consumers 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 [10].

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 [7].

Working of Iris scanning is the most accurate verification of biometrics. In iris scan first of all, the entire pattern is recorded to the system and after that comparison check is performed to test the genuineness of the person. If the pattern matches the person is considered to be genuine. The image given below explains the process of IRIS scanning.

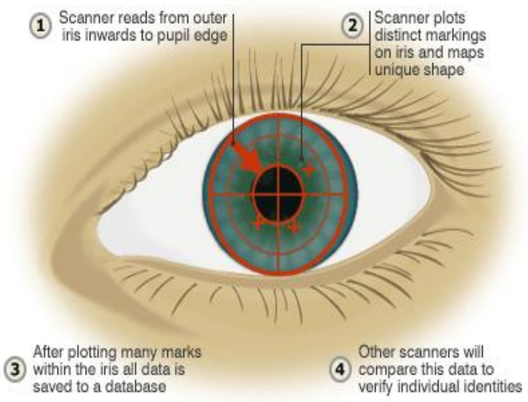
1 Scanner reads from outer iris inwards to pupil edge
2 Scanner plots distinct markings on iris and maps unique shape
3 After plotting many marks within the iris all data is saved to a database
4 Other scanners will compare this data to verify individual identities

Fig. 2. Process of IRIS scan (Image Source: http://news.bbc.co.uk/2/shared/spl/hi/guides/456900/456993/html/nn3page1.stm)

After taking the picture using camera, the computer matches for:

1. The center of the pupil
2. The edge of the pupil
3. The edge of the iris
4. The eyelids and eyelashes etc.

After finish this, it analyzes the every pattern in the iris and converts them into a code. Iris is normally a secure and covered structure and it doesn't usually changes time to time. Iris scanning is very much used in high security zone around the world.

According to the Biometrics Institute Industry Survey 2012, the Adoption rate of Biometrics in day by day life replaced Biometrics at the Border in terms of the improvement expected to be of maximum significance over the next coming years. This was the case overall, in both ANZ and Europe and amongst both consumers and suppliers [8]. The table below shows the adoption of biometrics:

I. TABLE 1 – ADOPTION OF BIOMETRICS

Most significant development in future	**2011-2012**	**2010-2011**	**2009-2010**
All respondents (208 in 2012)	Adoption of Biometrics in Everyday life	Biometrics at the Border	Increased User Acceptance
ANZ (94 in 2012)	Adoption of Biometrics in Everyday life		
Europe incl. UK (61 in 2012)	Adoption of Biometrics in Everyday life		
Users (100 in 2012)	Adoption of Biometrics in Everyday life		
Suppliers (78 in 2012)	Adoption of Biometrics in Everyday life		

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. Biometric security has more improved security and safety features than the conventional security methods.

- 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; banks and other institutions 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. FINANCIAL & TRANSACTIONAL SOLUTION PROVIDERS

There are many big companies in the market who are providing biometric solutions at various level of security. Some of them are: **Aware Inc.** Aware Inc. is a big security solution provider for biometrics systems. It provides software components and applications to verify the user's identity. The products and services provided by Aware Inc. include software, finger print reader, facial recognition system etc. It provides the functionality given below [11]:

- Fingerprint and facial image auto-capture
- Image QA and compliance assurance
- Certified 1:1 fingerprint matching
- Standard-compliant data formatting and validation
- Service-oriented workflow server platform

Cogent: This is a leading provider of Automated Fingerprint Identification Systems, or AFIS, and other fingerprint biometric solutions to corporations, law enforcement agencies, governments and other organizations around the world.

Cross Match Technologies: This is also a leader in providing biometric identity management systems, applications and enabling technologies to law enforcement agencies, governments, and businesses globally. It offers biometric technologies which are capable of mobile, wireless or stationary that encompasses fingerprint, iris scanning technology, palm and full-hand scanners, facial recognition systems, biometric software, document readers and other related services.

MorphoTrak: It provide complete solution including development, manufacturing & integration of biometrics and identity management solutions to serve the needs of civil identification, law enforcement, driver control, facility/IT security, border control and access control. This is recently named Biometrics Company of the Year by Frost & Sullivan, a business consulting firm.

NEC: A well known leader in the field of biometrics technologies has developed few finest automated methods for verification and identification. NEC provides the best and most advanced biometrics solutions for government, law enforcement, commercial and civil applications. NEC has int4roduced some of the world's most complex identification system for the government and other organizations. NEC provides products and services like Finger Scanners, Fingerprint Readers, Hand Readers & Middleware / Software, Border Control / Airports, Smart Cards, Consumer / Residential Biometrics etc.

VII. BIOMETRICS AT BANKS 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.

According to the President & CEO, Axis Software, "They are using scanning and matching algorithms that are approved by FBI. They 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 [16].

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 [15].

VIII. FUTURE OF BIOMETRIC TECHNOLOGY

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 [12]. 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.

IX. CONCLUSION

These days 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 consumers 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] Use Biometrics To Tackle ATM Fraud, URL: http://www.thenigerianvoice.com/nvprint/15393/2/use-biometrics-to-tackle-atm-fraud.html

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

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

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

[8] Biometrics Institute Industry Survey 2012, www.biometricsinstitute.org

[9] HITACHI VeInID documents, URL:

[10]

http://www.hitachi.eu/veinid/documents/hitachi_vein_16pp.v6.pdf

[11] ATM Marketplace, URL:

http://www.atmmarketplace.com/article_print/129761/ATM-security-in-Asia-moves-to-veins

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

[13] Future of Biometrics technology, URL:

http://www.articlesbase.com/tools-and-equipment-articles/what-is-the-advantage-of-biometric-security-products-2398403.html

[14] D. Hutchinson & M. Warren. "Security for Internet banking: aframework", Logistics Information Management, Emerald GroupPublishing Limited, 16(1), pp.64 – 73, 2003.

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

[16] India's First Bio-ATM From Axis , URL:

http://www.cxotoday.com/story/indias-first-bio-atm-from-axis/

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