International Journal of Interdisciplinary Innovative Research & Development (IJIIRD)

ISSN: 2456-236X

Vol. 04 Issue 01 | 2019

A survey-Enhancing ATM Security Using Biomertic

Ankita Arun Nandivadekar[1], Flavia Gonsalves[2]

[1, 2] Department of MCA MET ICS Bandra (W), Mumbai, Maharashtra, India

ABSTRACT

Growth in electronic transactions has led to increased demand for quick and accurate user credentials and authentication. Despite the countless advantages of an ATM scheme, ATM fraud has become more prevalent. In this paper, we provide an overview of the possible fraudulent activities which can be performed against ATMs and studies advised approaches to stop these sorts of frauds. To prevent these frauds, we would like to use some fool proof security solution that can be used with the existing technology. Biometric is a technology that can be merged with the current technology. Biometric Verification, System for Automated Teller Machine (ATM) will serve as an alternative to the current verification system that utilizes ATM cards and Personal Identification Number (PIN) to protect against fraud and efficiently eliminate the most widespread efforts to gain unauthorized access. With biometric technology, customers can gain access to their account through the smart card approach combined with biometric technology to automatically identify everyone using their individual physical or behavioural characteristics. The main aim of this project is to solve the problems that occur while using a PIN as the base of ATM verification system. These involve unauthorized access into financial accounts, stealing money. Thus, will improve the protection level for alternative money transactions.

Keywords-ATM, Biometric System, Identification, Recognition, Security System for ATM.

1. INTRODUCTION

As there is an increase in the facilities provided by banks so people are using these facilities for their economic activities. A customer who has a bank account can access the account from the ATM systems after receiving a PIN or a confidential bank password. By inserting the ATM card into the machine and entering a PIN number, you can easily complete the transaction, transfer funds, etc.

ATMs are located in different places and the customers can make basic transactions without the help of bank staff, due to this use of the ATM they are used widely. In Fig. 1, shows that in the year 2017 use of ATM machines is less as compared with the year 2016. In the year 2019, the use of ATM increases all most 50% with respect to the year 2015.

Normally, the purpose of authentication relates to reliable hardware equipment (ATM cards or tokens). The Personal Identification Number (PIN) of the cardholder sometimes is the only way to check the user's identity. There is a magnetic strip in every card that has all the information regarding the customer. The ATM machine scans, authenticates the card, and after verifying the customer's magnetic strip, card range, expiration date, as well as other necessary information.

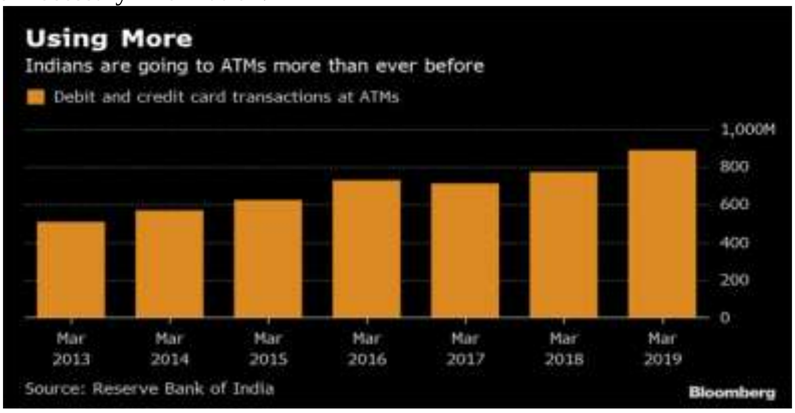

Fig. 1: Growth of ATM transactions in the world.

If these conditions are met, then the customer is allowed to perform the transaction. A PIN number is a crucial aspect used to secure information of customer’s Account, thus should not be shared with others. The crime which is happening related to ATM's is a serious issue so there is a need for ATM security. If any customer loses his/her card and the PIN number is known to the hacker. Then he can withdraw all the money in no time. So to avoid ATM related frauds there are various techniques which are secure while withdrawing money.

To make a transaction secure and identify the authorized person various techniques are introduced by the ATM system. In biometric technique, there are various methods like face recognition, fingerprint recognition, etc. which have been designed to enhance the security of ATM, but there are various challenges in those techniques. This paper focuses on the security of the ATM system and its various techniques which makes the ATM secure to use.

2. LITERATURE REVIEW

2.1 Atm Frauds In India

In Fig. 2, shows that in the year 2018 fraud of ATM card happens in India. IN 2019, due to a booming scene of the crime, India is estimated to surpass the United Kingdom and become the second-most targeted country behind the undisputed leader, the US, for payment card fraud. Also from statistics on cybercrime compiled by the cybersecurity firm Gemini Advisory, approximately 3.2 million Indian payment cards were posted for sale online and compromised in 2018, which was a huge jump from last year, when information for about 800,000 Indian payment cards only was reported on cybercrime forums.

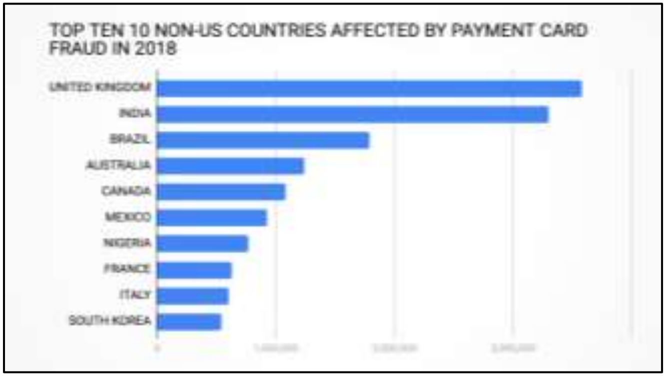

Fig2: Payment card fraud statistics for 2018

The immediate attention that India is receiving makes sense. It is predicted that the country will overtake China by 2024 to become the highest populated country. India's economy is expected to exceed the UK economy by the end of the year. Coupled with a middle-class boom in India and efforts by the government to digitize the country, more and more Indians now have a payment card. But equivalent investments in payment card protection from the banking sector did not accompany this unpredictable rise in valid payment cards. Indian banks stay simple to hack, e-banking solutions are plagued by safety faults, and the ATM network is not subject to the same close monitoring as all the other countries ATM networks, which improves cyber attacks and economic fraud. For beginners, the underestimated ATM network of the country is now the area where most associations will attempt using skimmed cards to cash out stolen money. “Threat actors in the dark web have earlier suggested India as an ideal place to use ATMs to cash PIN information from different compromised European cards," Gemini Advisory Researchers Stas Alforov and Christopher Thomas said during a study conducted yesterday. As Indian banks don't employ modern anti-fraud systems, there is a huge demand for Indian payment cards as they can be easily cloned and cashed out en-masse. Realization on the behalf of cyber-criminal organizations has led to a rise in Indian payment card selling prices of 150 percent, which Alforov and Thomas have now observed are in huge demand. An Indian payment card now has an average price of $17 (approx. 1,177.73 Indian Rupees) from a median price of $6.90 in 2017 (approx. 478.02 Indian Rupees). Gemini observed that the attention of cybercriminals has also been noticed by the Indian financial sector.

2.2 Biometric

Biometrics is the scientific term used for body measurements and calculations. It relates to metrics belonging to human characteristics. In computer science, verification of biometrics has been used as a way of identifiable data and can be monitored. It is additionally utilized to recognize people in bunches that are beneath reconnaissance. Biometrics in respect to natural sciences has been examined and connected for numerous eras and is to some degree essentially seen as "biological statistics."

Verification is the act of building up or affirming something (or somebody) as true, that claims made by or approximately the thing are genuine. Any physical or behavioural biometrics of human beings can be used as a biometric trademark, the length which fulfils necessities.

- Universality-Everyone ought to have the biometric trademark.
- Distinctive-The impact of the trademark should be sufficiently unique for any two people.
- Permanence-Trademark ought to be enough invariant over a time allocation.
- The collectability-the biometric trademark should be measurable with a few identifiable verification gadgets.
- Performance-Refers to the level of exactness and speed of confirmation of the structure, the advantages required to wrap up the specified certification level, and the operational and characteristic fragments that affect the precision and speed.
- Acceptability-Indicates how many people in their normal day-to-day lives will accept the use of a precise biometric identifier (trademark).

The biometric identifier can be separated into two sorts on either physiological characteristics or behavioural characteristics. The physiological identifier includes facial expressions, fingerprint, iris recognition, vein recognition, retina scanning, voice recognition, and DNA match. By verifying this the user can be identified. The behavioural identifier includes the user to act with recognition of typing patterns and walking gaits and gestures.

2.3 Type of Biometric

2.3.1 Physical Biometrics

Physical identifiers are used for immutable and device independent.

2.3.1.1 Fingerprints Recognition

Fingerprint recognition is most widely being used as a security purpose in computer-aided and personal identification. Unique finger impression recognition is utilized in voting, examination, operation of bank accounts, etc. They are also used for controlling access to highly secured places like offices, equipment rooms, banks, law enforcement agencies, hospitals, and clinics, schools, and colleges, gym and fitness centres. The fingerprints of any person remain the same throughout life and no two fingerprints are ever the same. But for this to work precisely, it requires clean hands without having any wounds to their fingers or else it'll be able to identify.

2.3.1.2 Facial recognition

Face recognition system is a biometric computer application able to identify or verify a customer through the comparison and analysis of patterns from a digital image. Present systems for facial recognition deal with face prints and 80 nodal points on the human face can be recognized by these systems. Nodal points are mainly endpoints used to evaluate factors on a person's face, along with the length and width of the nose, the angle of the cheekbone, and the depth of the eye socket. A technique of facial recognition is a software program that investigates or confirms an individual from a photograph or a video from a database source automatically.

In favourable circumstances, these systems use face prints to precisely recognize these systems currently focus on smartphone applications that include the intended purpose for personal marketing, social media, and image tagging. Social networking sites like those of FB use face identification software to tag users in photos. This software also improves the personalization of marketing. For instance, billboards are designed with an integrated software system that acknowledges the quality, gender and calculable age of onlookers to deliver targeted promoting.

2.3.1.3 Iris recognition

Iris recognition is a technique of biometric identification that uses pattern-recognition techniques which supports high-resolution pictures of the irises of associate individual's eyes. The iris is captured via associate coral imaging method, which identifies the iris from the pupil of the eye. The image is then derived from an analysis of the detail within the triangular network of the iris. The technology of Iris recognition requires camera technology, with subtle infrared brightness, decreasing the peculiar reflection of the convex cornea to build photographs of the depth-rich, complicated iris structures. These images region unit born-again into a digital figure to provide mathematical illustrations of the iris that generate a unique useful identification of a person. These algorithms were used to effectively debut of the technology in conjunction. An iris recognition algorithm first needs to examine the iris and pupil's relatively concentrated external circular borders in an eye photo. The pixel group that only covers the iris is then transformed into a bit pattern and This preserves the important data for a statistically relevant comparison between two iris photographs. In the scenario of Daugman's algorithms, a conversion of the Gabor wavelet is used to separate the camera into excellent signal noise.

2.3.2 Behavioral Biometrics

Behavioral statistics is usually used for confirming an individual. They are often divided into the following types: keystroke recognition and talker identification.

2.3.2.1 Keystroke Recognition

It is very important for reducing fraudulent exercises like inappropriate mail and untrustworthy typewritten. Keystroke recognition as the name recommends measures the person’s writing designs. Computers utilizing keystroke acknowledgment code will decide the improper exercises and pushes the message to authorized individuals to require appropriate action.

2.3.2.2 Voice Recognition

Voice is an additional physiological attribute, as a result, everyone has different speak, but voice recognition is mainly based on the study about how good a person speaks. Sound confirmation focuses on the vocal factors that deliver voice rather than on the sound or discourse pronunciation itself. The sound quality depends on the dimensions of the vocal tract, mouth, nasal cavities and the other voice processing mechanism of the human body. It does require any simple mic or cheap hardware. Input sound is seen as non-invasive. The technology needs additional hardware by using existing microphone Other Techniques

2.3.2.3 Signature Recognition

Signature recognition could be a style of the biometric methodology used to analyze and live the physical activity of sign language just like the pressure applied, stroke order and also the speed. Some bioscience area unit used to compare visual pictures of signatures. Signature recognition is often operated in 2 other ways, like static and dynamic.

Consumers write their own signatures on the document in static mode, digitize it through a camera or related optical scanner. this technique identifies the signature that examines the shape. This system identifies the shape of the signature. Customers draw their signature in dynamic mode on a digitizer tablet that gives the signature in real time. Another option is that by gaining suggests of stylus-operated PDAs. A couple of biometrics also works with capacitive screen smartphones where customers can sign using a finger or a written signature. This type of recognition is additionally referred to as “on-line”. So, this is all about biometric sensors which can be used by several organizations to increase the level of security and protecting their information and copyrights as well.

Some other available techniques to identity verification are described below.

2.3.3 Palm-print

Palm-print verification is a slightly completely different implementation of the fingerprint technology. Palm-print scanning uses fingerprint scanning-like optical readers. If their size is much larger and this can be a restricting factor for the use in mobile devices or workstations.

2.3.4 Hand Vein

Hand vein pure mathematics is predicated on the actual fact that the vein pattern is distinctive for numerous people. The veins under the skin absorb infrared radiation and So have a darker pattern on the picture of the infrarot camera's side. The hand vein pure mathematics remains within the stage of analysis and development. One such system is factory-made by British Technology cluster. The device is named Veincheck and uses a template with the dimensions of fifty bytes

2.3.5 Thermal Imaging

This technology is similar to the hand vein pure mathematics. It additionally uses an infrared source of light and camera to provide a picture of the vein pattern within the face or within the wrist joint

2.3.6 Ear Shape

In law enforcement applications where ear markings are spotted in crime scenes, the recognition of people by ear form is used. It remains to be seen whether this technology will advance to access control apps. An ear form verifier (Optophone) is created by a French company ART Techniques. It is a handset type of telephone with a lighting unit and cameras capturing two ear images.

2.3.7 Body Odour

The body odor biometry relies on the actual fact that just about every human smell is exclusive. Sensors capture the smell from body parts that are non-intrusive such as the back of the hand and the smell. Each human smell is made up of chemicals known as volatiles. They are extracted and converted to a template by the system. The use of body odor sensors brings up the privacy issue because the body odor carries a major quantity of sensitive personal info. It is doable to diagnose some diseases or activities within the last hours by analysing the body door.

3. MATERIALS AND METHODS

The survey's target population was customers and employees of some Indian business banks. The customers and students were randomly selected.

The tool used for this research was a survey of 16 things made by the researchers. The questionnaire items were obtained from a comprehensive literature study and an oral interview. There are three segments of this tool. The first segment identifies the profile of the survey participants. The second segment investigates with the use and reliability of ATM by survey participants. The third segment investigates the biometric trait reliability. The survey's 200 duplicates managed the return of 167 usable duplicates. That was a return rate of 82 present. This research was conducted for over two months.

The items in this tool were analysed using illustrative measurable methods The primary details were obtained from diaries, internet readings and courses. Expert's judgments were used to determine the validity of the survey things in the questionnaires. All the items in the questionnaire were face-validated by two experts. Items wording has also been confirmed for clarity. For irrelevance, two items in the questionnaire have been removed while three ambiguously worded items have been reorganized to represent clarity. The two experts observed the items appropriate for administration on the subjects after the corrections.

4. RESULTS AND DISCUSSION

Presentation of the overview of the results in terms obtained (Tables I – III). Table I indicates the participant's profile. Participant's age group was 20-60 years. The questionnaire was attended by 40 men and 34 women.

Table I. Profile of Participants

No	Profile	Description
1	Age	20-60 years old
2	sex	34:40
3	Bank account and ATM card	Respondents own different types of account depending on the bank, bank products and types of services rendered.

At least one type of bank account is held by each participant. Each member owns no less than one type of financial balance that focuses on the bank, the items offered and the bank's benefits. This succeeded in ATM being launched and the services it offers. The use and reliability of ATM are shown in Table II.74 Respondents who speak to a few customers and staff of a few banks and speak to 82% of the population use the ATM while 54 present of the population is yet to use the machine. One or the other form of ATM fraud is known to 77% of the population. Most of the Indian banks are constantly improving their customers on ATM fraud and taking steps to prevent it.74% of the population considers ATM transactions to be too dangerous. This required 66% of the population to say they will keep going to use ATM. Due to machine-related security issues. As a result, 60% of the population preferred a third authentication rather than using the ATM and PIN cards. And this population believed that ATM security will be improved dramatically with the infusion of biometric traits to the current ATM and PIN cards.

Table III illustrates the biometric character's reliability and popularity. Biometric fingerprints are known to 74 present of the population. By adding fingerprint technique into the current ATM card and PIN, 78 present of the population strongly trusted that the ATM would provide better safety.

Table II. Use and reliability of ATM

	Question	Responses		total	Percentage (%)	
		yes	No		Yes	No
1	Do you use an ATM card?	73	1	74	98	1
2	Do you find pin secured while using ATM card?	49	25	74	66	33
3	Since how long are you using ATM card?					
	a) Less than a year	4			5	
	b) More than one year, less than 3 years	10			13	
	c) More than 3 years	59		74	79	
4	Have you ever heard of any ATM fraud?	57	17	74	77	22
5	Are ATM transactions becoming risky?	55	19	74	74	25
6	Will security concerns make you stop using ATM?	34	40	74	45	54
7	Do you prefer higher security for ATM?	71	3	74	95	4
8	Will you discontinue the utilization of ATM as a result of the	49	25	74	66	33

	safety problems related to it?					
9	Would you like a 3rd level security aside card and PIN?	45	12	74	60	16
10	Have you detected of biometry as a method of authentication?	58	16	74	78	21
11	Do you suppose the utilization of biometry will improve ATM security?	73	1	74	98	1

Table III. Reliability of biometrics characteristics

Q.no	Question	Response	Percentage (%)
1	Please indicate that one or a lot of the subsequent biometric technologies you've got used before.		
	a) Fingerprint	35	47
	b) Voice	4	5
	c) Palm	2	2
	d) Face	10	13
	e) Retinal	7	9
	f) Iris	4	5
	g) Signature	5	6
	h) Gait	2	02
	i) None	5	6
	Total	74	100
2	How often do you use biometric technology?		
	a) Always	25	33
	b) Often	15	20
	c) Sometimes	30	40
	d) Seldom	4	5
	Total	74	100
3	Biometric technology increases security in general.		
	a) Strongly agree	7	9
	b) Agree	52	70
	c) Neutral	13	17
	d) Disagree	1	1
	e) Strongly disagree	0	0
	Total	74	100
4	Which banking channels uses biometrics in your organization		
	a) Internet Banking	17	22
	b) Telephone Banking	6	8
	c) ATM	20	27
	d) Banking in the Branch	30	40
	e) Community Banking	1	1
	Total	74	100
5	In which banking channel does one assume statistics works well?		
	a) Internet Banking	23	31
	b) Telephone Banking	7	9
	c) ATM	18	24
	d) Banking in the Branch	26	32
	e) Community Banking	0	0
	Total	74	100
6	Which of the biometrics the characteristic will provide better security when united with the ATM cards?		
	a) Fingerprint	27	36
	b) Iris	11	14
	c) Face Recognition	14	18
	d) Signature	5	6
	e) DNA	4	5
	f) Retina	7	9
	g) voice	6	8
	Total	74	100

The results of the biometrics comparison analysis survey are provided in Fig.3. Gain a great response and success in this survey among all the biometrics fingerprint system. The outcome indicates that there is a large margin between the use of fingerprints to recognize other biometrics such as the face, palm, iris, voice and signature.

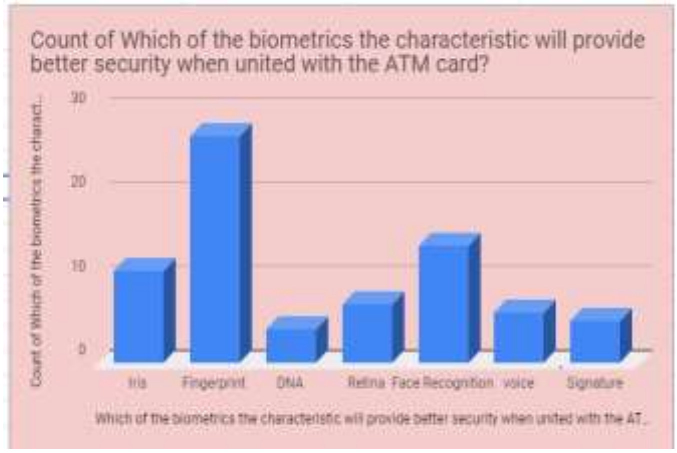

Fig3. Comparison survey on biometrics

The following reasons for the common use and acceptability of fingerprints for safety enforcement or control:

1. Fingerprints have a wide variation as there are no identical prints for two people.
2. Fingerprints have high degree of consistency. The fingerprints of a person may change the scale, but not the relative appearance, which is not the case with other biometrics.
3. Fingerprints are left whenever a surface is touched by the finger.
4. Small and cheap fingerprint capture devices are available.
5. Fast computing hardware available.
6. High identification rate and speed devices available that satisfy the requirements of many apps.
7. Network and Internet transactions are explosively increasing
8. The increased awareness of the need for user-friendliness as an essential component of reliable protection.

5. CONCLUSION

As we can see, security concerns have increased as terrorism and other invisible risks around which human life is seriously damaged. The existing system is not secure to carry out cash transactions, data, and funds for customers. We need similar advanced biometric safety systems to protect against all these high-quality technical threats and intrusions. Using biometric, various techniques can be used to distinguish the characteristics of the individual. This paper describes a high-level system for modifying current ATM systems using biometric fingerprints recognition as security protocols. We have been able to build a biometric system to improve the ATM's security characteristics for the Indian banking system's efficient banking transaction. This system will definitely reduce the rate of fraudulent activities on the ATM machines when fully deployed so that only the registered owner of a bank account access card.

6. REFERENCES

[1] “India is shutting down ATMs even as people use them more”, May 15, 2019

[2] Catalin Cimpanu “India expected to surpass the UK for second place in payment card fraud”Zero Day-April 19, 2019 04:20 GMT (09:50 IST)

[3] Moses Okechukwu Onyesolu, and Ignatius Majesty Ezeani, “ATM Security Using Fingerprint Biometric Identifer: An Investigative Study,” International Journal of Advanced Computer Science and Applications · April 2012

[4] Nisha Bhanushali, Meghna Chapaneria, “Fingerprint based ATM System“, Journal for Research ,Volume 02,Issue 12, February 2017 ISSN: 2395-7549