Biometrics in Banking

Manjot Kaur Bhatia[1], Gunjan Dawar[2], Sanchit Sachdeva[3], Yash Bhasin[4]
[1]*Professor,* [234]*Research scholar,*
[1234]*Dept. of Information technology, Jagan Institute of Management Studies, Delhi , India*

Abstract- In the modern era of science, technology is shaping the world. The rapid growth in technology in the last two decades has changed the way we bank or operate in and out our day to day businesses. But with flexibility and easiness the new technology has added in our life, technology also brings added concerns for security of our data and identity.

To improve the state of current security measures used by banks for common facilities like ATM, we are here to discuss a proposal where we have to look beyond ATM PIN as authentication methods, as a PIN can be guessed, stolen and misused by fraudsters.

To overcome the challenge we are introducing a second factor of authentication, which is not only more secure than currently used one factor authentication(PIN based) but is hard to forge, steal and be misused with added hassle free operation. The second line of defence we are talking about is the Biometrics Authentication.

In this paper we are discussing, how we can improve the efficiency of the biometric system by setting proper thresholds to maximize the efficiency and accuracy of the biometric system for authentication. As we answer the above question, we discuss the challenges that are present in the current system and how we are proposing to increase the efficiency of the biometrics authentication.

The first part discusses the challenges with biometrics and degradation of the biometrics sensors over time and how it reduces its efficiency to work properly as an authentication device, with added constraints of a quick and time bound transaction.

The second part of the proposal emphasize on how we can improve the security, efficiency and speed of the system. The system handles the performance and speed issue by introducing few constraints such as, if the user wants to change PIN or withdraw an amount greater than the maximum threshold amount set or performs more transactions in a day than the maximum transaction threshold for the day set by the bank, in such case the user has to provide his biometrics identity to complete the transaction process. On the other hand if the user wants to simply know the account balance or print a mini transaction there is no need to go through the biometric authentication system.

Keywords- Access Control; Biometric; Fingerprint Verification; Constraint based Biometric

I. INTRODUCTION

Biometric technology provides us with a quick and efficient system for user authentication. A typical biometric setup uses a set of sensors, a database and a working algorithm that matches the input from the sensors against the images in database[1]. One of the main benefit of using BAS is that it leave the user from the hassles of learning complicated passwords. Another benefit they offer is they cannot be forgotten or lost.

BAS has their advantages and disadvantages too, as a password can be made complex remembered and will be stored in the memory of the user in a best case scenario, but the biometrics cannot be hidden from the world, they are public and are very susceptible to attacks[2].Also, stolen biometrics can be passed down to collect confidential and private information of their owners, such as an ethnic group, medical diseases, and genetic information or to practice unlawful activities. Due to such problems, it has become very important there is need to develop privacy maintaining BAS i.e. a biometric authentication system which can alleviate aforesaid security and privacy threats mentioned.

A successful attack can have a drastic effect on the life of the user. A stolen password can be changed at the will of the user but a compromised biometric cannot be. So the storage of centralized database of the biometrics also has great security implications and the measures might not be cost effective.

In this paper we are providing with the insight of use of Biometrics in the BankingSector especially ATMs (Automatic Teller Machines) that have made it easier to carry out all the crucial banking tasks easier and less complex and less time consuming.The first section provides an insight towards what lead to write this paper. The use of fingerprint scanner in ATM. The sensor is exposed to different conditions such as sweaty hands, dusts and oil which affects the sensitivity of the sensor to capture accurate information for sample verification. There will be instances where someone needs to withdraw only a small amount or just balance inquiry and there is a long queue of people behind him, so the algorithm should be smart enough to bypass biometric authentication in such cases. To skip this problem we propose a system which introduce where one has to enter one's biometric details only in case when the transactions are above a certain threshold. The threshold variable will be true in combination of certain condition like the number of transaction is more than k=5 for example in a day, or the net amount withdrawal is more than l=10000 or both are true. It will also ask for the biometric authentication

in case it detects the location abnormality or multiple invalid pin requests.

The proposed system provides additional security at ATM as the bank can enforce maximum number of transaction or maximum amount can be withdrawn by any unauthorized person.

The second section throws light on the technology. The third section describes the background of the biometrics and how biometrics works. The fourth section envelops the current problems of the system in a broad perspective, the problems includes some theoretical implementations and the problems faced by agencies implementing biometrics worldwide. The fifth section provides us a solution to the current biggest problem faced by biometric system in banking and the last section throws light on the future scope of biometrics.

II. RESEARCH BACKGROUND

The modern society is significantly wrapped with technology all around. With digitization of banking and rapid increase in advancements in technology, there is a need to include every section and corner of the society in the fabric of modernisation. One such example is exclusion of rural India where a significant population is illiterate in the banking system. More than 70% of Indians depend on agriculture; 60% of industries are agro based; 50% of national income is contributed by rural sector and the agricultural sector is the largest foreign exchange earner to India. Such an essential and key sector is neglected by financial institutions and especially by the banks.

With ever increasing threat of identity theft and cyber terror, he challenges that are In front of the banking fraternity to expand their activities in the rural world are the security of the accounts and money of the account holders.

People from rural area mostly are illiterates so filling and making them understand banking procedures are tough in nature and processing time for each and every application forms, forms takes long time.

Also the use of thumb prints in place of signatures make the identification of person more difficult as there is a high chance of error when matching thumb impressions with naked eyes.

To increase the efficiency and security of banking system, biometrics offers a huge potential in making banking simple and quick.Biometrics replaces the signature system and provides a frictionless authentication process through thumb prints.

However, combining the desire for user-friendliness with the need to improve security is a tough balancing deed. With the rapid gain of momentum of biometrics in banking, it is equally becoming an area of great interest for cybercriminals. The security of the apps and systems, supporting these mechanisms, are jeopardized.

III. LITERATURE REVIEW

Biometrics is a term consists of two words bio and metrics which means biological characteristics of humans.

Each individual has a unique biometrics due to which they can be used for the authentication purpose[3].

The authentication process is a multi stage process such as measurement, signal processing, pattern matching and decision making.

Scanning the image of user characteristics, measuring and matching it against a database is part of biometrics. It involves capturing the image of the finger of the user and mathematically modelling it to extract features and store in a digital format so it can be used later for matching. The performance of the biometric system is measured with the following factors.

False Match Rate - It is the rate by which the biometric system the incorrect images in the database to the input image from the scanner. It is possible that an incorrect template is matched in the database as a genuine template hence increasing the fault match rate of the system. It is used to measure the rejected data percentage in the system. It is a critical parameter for the efficiency of the system.

Receiver operating Characteristic- It is a balance between match rete and reject rate and is measured by setting a threshold to find the match template. The threshold defines the minimum percentage of characteristics it must match to call it a true match or reject an input. If the threshold is set low, the number of rejections will be low but the accuracy of the system is compromised, but if it is too high the rejects increases and speed reduces hence decreasing the efficiency of the system.

Equal error rate (EER) or **Crossover error rate** (CER): Defines as the rate at which the system takes the sample or rejects the sample is called equal error rate. The less the rate the better is the system. It can be used to measure the performance of the system. The rate can be calculated from the ROC curve.

Failure to enroll rate (FTE or FER): It is the rate by which the system rejects the input, the low quality input can make system to reject more.

Failure to capture rate (FTC):The rate at which the system failed to capture the metrics of the user even when the input is successfully submitted in the system.

Template capacity: The maximum number of different unique templates that can be stored in the system.

IV. WORKING OF BIOMETRIC SYSTEM

The biometric system consists to two parts, data and identification. Together they make biometric system.

The system works in two phases. The first phase consists on enrolling the user in the biometric database.

Scanning : The first step of enrolment consists of scanning the biometric feature of the user.
Processing : The second step consists of processing the scanned image in the database. The processing consists of several steps like Noise removal, Color correction etc and converting into a format which can be stored digitally.
Storage: The processed image is then stored in a secured cloud, where it can be accessed by ATM via bank servers for verification.The enrolment is a time consuming and aone-time process hence does not possess a challenge.
The second phase is the identification phase. The identification phase is done in multiple steps which are listed below.
Scanning - The first step includes the scanning of the user fingerprints at the machine.
Transmission - The transmission over a secure line to the database server that hosts the biometric truth data.
Signal Processing- This process prepares the scanned image for matching by removing noises and distortion.
Data Extraction - The process extracts features from the processed image to obtain more precise data and reduced size.
Template creation - With the extracted features a template is created with some set of properties to make comparison fast and accurate.
Matching - Returns a value true or false depending on the match of template with the image stored in database.

V. PROPOSED SYSTEM

Problems with current Biometric System
Working with Biometric system has some issues and limitations with the input of the sensor that scans the fingerprint, like speed, accuracy with time and failures.
For working of fingerprint scanner the user has to put his fingers on the scanner again and again. Touching the sensor again and again degrades the working capability and accuracy of the system. As every user has to give biometrics irrespective of cleanliness of their hands, the dust and oil from the figers degrades the biometric system and hence hampering the capability of the sensor to work at its maximum efficiency to scan the image. With decreasing efficiency the rate of failure increases rapidly making the service unusable that requires biometric authentication.Here we apply our concept to the ATM machines to improve the efficiency of the biometric system.

Solving the sensor issue
The continuous use of the sensor can degrade the sensitivity of the sensor and will increase the false positive rate. A lot of customers scans fingers with oily and dusty hands to make enquiry and withdrawals at the ATMs, thus decreasing the efficiency of the system. To solve the issue we can introduce a constraint based biometrics system that will require smart use of biometric sensors for ATM and reduce the number of times biometric authentication is used and thus improving speed and efficiency of the system, resulting in improved and secure services at the ATM.
We apply a constraint at the use of biometric in the ATM machine. The user has to authenticate his biometrics credentials only when the withdrawal amount is greater than the maximum safe amount defined by the bank or the number of transactions is more than the maximum number of transactions for the day or the user wants to change pin. So in case a fraudster want to perform a transaction with a very large amount or repeated attempts the bank will be alarmed and the access can be blocked, saving money and fraud. The threshold numbers will be updated by the bank on a daily basis and will be updated for the user in each attempt, hence improving the security of the system and making an efficient use of the biometric system. The added constraint not only smartly limits the use of the biometrics but also improves the speed and efficiency of the whole system.

Working of the system
In the system we are proposing, we are adding an additional layer of security without modifying the existing system solving the issue of sensor efficiency over time.
When the user uses a system which is equipped with the biometric sensor, the user first enter the ATM card and follows the required 4 digit PIN procedure. The ATM pin is verified against the database of the bank and after successful verification, user is asked for the banking options. If the banking request is not critical, such as balance inquiry or printing on Mini statement, the request is fulfilled. If the security is critical such as amount withdrawal or pin change the request is then forwarded to our proposed algorithm for further process. Once the user enters this mode the min_transaction count of the algorithm is incremented with 1 and user is prompted to enter the amount. If the user enters the amount and the amount is less than the safe threshold set by the bank and also the maximum transaction threshold by the bank, the transaction is completed and the cash is dispensed by the machine. But if the request amount is more than the threshold user is asked for the biometric verification. After the successful verification of the biometrics against the database, the transaction is completed and the cash is dispensed.
The transaction count threshold is reset every 24 hours to enable ease of banking for the users.
Here is an algorithm representing the above procedure.

Initial Conditions:
currentTransactions=0 (reset to 0 at 0:00hr)
constantmaxCashLimit
1) readatm details and enter pin
2) verify user with pin and card number
3) if user authentication fails goto (10)
else

Ask user for balance enquiry, cash withdrawal or pin change
a) if selected cash or pin change go to (4)
b) if selected balance enquiry goto (9)
4) currentTransactions+=1 //(update the transaction for today)
5) Ask user for amount
6) IF (amount<maxCashLimit) AND (currentTransactions< 5)
a) goto (9)
b) Else goto (7)
7) Ask user for biometric authentication
8) IF biometric matched
a) GOTO (9)
b) Else ACCESS DENIED
9) ACCESS GRANTED
10) End Transaction

Here is a C implementation of the above algorithm:
Case 1: When user tries to enter an invalid PIN.

```
Reading ATM detail....
Enter your card number:1234

Please enter your PIN:98732

Invalid pin try again:
Please enter your PIN:43287

Invalid pin try again:
Please enter your PIN:23980

Card unacceptable, not a valid user(end Transactions)
```

Case2: Change PIN.

```
1.PIN change
2.Cash Withdrawl
3.Balance Enquiry
 choose your option:1

 enter the new PIN:2378

 your PIN has been changed:
 Do u wish to continue:_
```

Case 3: IF (amount<maxCashLimit) AND (currentTransactions< 5):

```
This is your transaction number:1
enter the amount you wish to withdraw:1000

your transaction is in progress:(please do not go back)
Now your Account Balance is:149000
do u wish for another transaction,if(press 1)
```

Case 4: IF(amount>maxCashLimit) AND (currentTransaction>5):

```
your transaction is in progress:(please do not go back)
Now your Account Balance is:120000
do u wish for another transaction,if(press 1)3

This is your transaction number:3
enter the amount you wish to withdraw:30000

you need to go through the process of Biometrics:

place your thumb on the sensor for the biometrics verification:

                    ...ACCESS GRANTED...
your transaction is in progress:(please do not go back)
Now your Account Balance is:90000
```

Case 5:IF(Biometric doesn't match):

```
your transaction is in progress:(please do not go back)
Now your Account Balance is:80000
do u wish for another transaction,if(press 1)1

This is your transaction number:5
enter the amount you wish to withdraw:1000

...ACCESS DENIED...
```

Case 6:checking current Balance.

```
 Do u wish to continue:1

1.PIN change
2.Cash Withdrawl
3.Balance Enquiry
 choose your option:3

 your Account current Balance is:80000
```

VI. FUTURE SCOPE

Biometrics is unique and it is seen as the next thing in the authentication process, as it provides an extra and reliable barrier to the existing technologies. Therefore there are intensive research work going on in the field of biometrics to include it in different technologies like smartphone.
The future of biometrics is more secure and reliable with metrics like DNA matching and iris scanning. DNA profiling is a technology that maps unique characteristics of a person and map that into a machine readable form.
DNA are unique and provides a great security barrier but it has its own limitations and usage with current technologies.
However, there is quite a high probability that the progress of technology arises which in the near future will bring up DNA profiling to the computer world.

VII. CONCLUSION

At its early days, current biometric technology dominates over the orthodox password and other authentication schemes.In respect of security biometrics shows vulnerabilities as the efficiency of sensors degrades over time, the communication line may be not secure and the threat of storing the identification profile of so many users in one place is itself a task for security. Also with current technologies it is quite possible to surpass the biometric identification with the use of some advanced tools.Hence to design a biometric system it must include the vulnerabilities the system adds to the overall closed loop of banking.
The system proposed in this paper aims at solving a key problem of scanner degradation over time with smartly limiting the use of biometric sensor, which in terms increase security for important tasks and reduce hassle for non-trivial task.
The user does not have to go through the biometric for knowing balance or get a mini statement from the ATM. If the user wants to withdraw cash but has not crossed the safe threshold limits for the number of transactions for the day and amount of transaction in each transaction. The user will be asked for the biometrics analysis only when he wants to withdraw a big amount of cash or the number of transactions crosses more than five for the day or each time the user wants

to change PIN. It not only saves time but adds an additional layer of security to the system and prevents bank users from frauds.

Along with the constraints we can also include the ideas proposed in the following papers to enhance performance and speed of matching results[5] [6] [7] [8] saving times of customers and banks.

Many banks have already implemented concept of Biometric in their ATMs [4] now they only need to add a condition to adopt this constraint-based scheme to their system with solving issues related to fingerprint biometric

To properly use biometrics for everybody's benefit, an intelligent approach would be used to prepare the users mentally and psychologically about the new technology, and make further improvements to the technology itself.

VIII. REFERENCES

[1]. "Biometrics: Overview". Biometrics.cse.msu.edu. 6 September 2007. Archived from the original on 7 January 2012. Retrieved 2012-06-10.

[2]. "What is Biometrics?". Biometrics Research Group. Michigan State University. Retrieved 10 November 2017.

[3]. "Characteristics of Biometric Systems". Cernet. Archived from the original on 17 October 2008.

[4]. A. T. Siddiqui, "Biometrics to control ATM scams : A study," International Conference on Circuit Power and Computing TechnologyICCECT, pp. 1598–1602, 2014.

[5]. S. Barman, S. Chattopadhyay, D. Samanta, S. Bag, and G. Show, "Anefficient fingerprint matching approach based on minutiae to minutiaedistance using indexing with effectively lower time complexity,"International Conference of Information Technology IEEE, pp. 179–183, 2014.

[6]. U. Jayaraman, J. Viswanthan, A. K. Gupta, and P. Gupta, "Minutiaebased geometric hashing for Fingerprint database," InternationalConference on IntelligentComputing, (ICIC -12), July 2012.

[7]. R. Boro and S. D. Roy, "Fast and robust projective matching forfingerprints using geometric hashing" In Proceedings of the 4th IndianConference on Computer Vision, Graphics and Image Processing, pp.681-686, 2004.

[8]. R. S. Germain, A. Califano, and S. Colville, "Fingerprint matching usingtransformation parameter clustering," IEEE Computational Science andEng., vol. 4, no. 4, pp. 42-49, 1997.