All In One ATM System

[1]Ameya Bharote, [2]Pawansing.R.Patil, [3]Ravina chaudhari, [4]Shraddha Ghuge, [5]Ms.Prranjali Jhadhav

[1,2,3,4]Research Scholar, [5]Professor
Department of Computer Engineering
Matoshri College of Engineering and Research Centre, Nasik

***Abstract*: Every individuals has multiple bank accounts in different banks, people's need to carry multiple ATM cards for transaction, there may be different PINs for every account. In traditional system, ATM terminal customer recognition systems only rely on bank cards, security pin number, and such identity verification methods which measures are not perfect and functions are too single and at times there are incidents where we forget ours security PIN number, lose our cards, cards get stolen, stolen PIN numbers. To overcome the bugs in traditional ATM system, introducing a new ATM terminal customer recognition system, "All In One ATM system using Biometric and GSM Authentication". Biometric based fingerprint authentication technique is one of the most secure systems, unauthorized accesses are restricted, as this makes fingerprint a unique identification for everyone. This system also assures a secure GSM (OTP-One time Password) based transaction. Here the proposed system has no risk overhead in managing multiple account transactions and achieves high security as compare to the traditional ATM system.**

***Keywords*: ATM (Automated Teller Machine), PIN (Personal Identification Number), Multi-banking, Security, Biometric authentication**

1. INTODUCTION

ATM can be described as Any Time Money. We can get money at anytime anywhere only through ATM machines. To do the secure transactions we need biometric authentication. Biometric authentication is a growing and controversial field. Today biometric laws and regulations are in process and biometric industry standards are being tested. According to, there are three popular attacks against ATM: Skimming, PIN logging and Integrity violation. There are also attacks against mobile phone: Fake mobile apps installation, key logging software and grab PIN number during transmission. Besides that, an attack may also be a combination of both types of said attacks.

Information also can be exploited by a side channel attack. It is found that attackers try to get the

user's account information that stored on the magnetic strip present at the back side of ATM card. Password is the only identity that can use to authenticate the owner of ATM card. It means anyone can access the account bank through ATM machine as the password entered is correct. So, once the ATM card and password is lost or stolen by anyone, they can withdraw the money from that account easily without the problem of user authentication. Thus, it can see that the most serious issue raised in ATM card security is about user authentication. User authentication is important because it lead to the integrity violation of bank account information. It seems that this issue is worse as anyone can access all information stored when they entered the correct password towards accessing ATM card at ATM machine. Other than that, it is strongly emphasized that the security issues need technology improvements and better security policy as a countermeasure.

Amurthy and Redddy developed an embedded fingerprint system, which is used for ATM security applications. In their system, bankers collect customers' finger prints and mobile numbers while opening accounts, then customer only access ATM machine. The working of the ATM machine is such that when a customer place a finger on the finger print module it automatically generates every time different 4-digit code as a message to the mobile of the authorized customer through GSM modem connected to the microcontroller. The code received by the customer is entered into the ATM machine by pressing the keys on the touch screen. After entering it checks whether it is a valid one or not and allows the customer further access. Biometrics can be defined as measurable physiological and behavioral characteristic that can be captured and subsequently compared with another instance at the time of verification. It is automated methods of recognizing a person based on a physiological or behavioral characteristic.

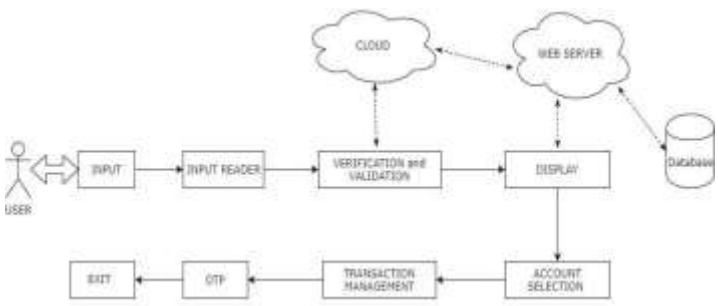

Fig1.Block Diagram of All in One ATM System

The architecture of the proposed system depicted in Fig[1]:

1. The working of system starts with reading input from user as a fingerprint of user. It will be read by fingerprint scanner. The input will be verified from the data stored in the database and gets validated.

The architecture of proposed system is divided into three different working modules, A) Working of Fingerprint Module B) Function of web Services C) Working of GSM module .

The databases are stored on cloud. Web services give access to all the bank accounts of user.

Table: Biometric Device Comparison

Biometric Technology	Accuracy	Cost	Devices required	Social acceptability
Iris Recognition	High	High	Camera	Medium-low
Facial Recognition	Medium-Low	Medium	Camera	High
Voice Recognition	Medium	Medium	Microphone, Telephone	High
Fingerprint	High	Low	Scanner	High

There are different techniques for biometric. They are mainly Iris Technology, facial recognition, voice recognition, fingerprint, palm technology, signature recognition, etc. In our system we use fingerprint biometric technology/device because it provide high accuracy, low cost as compare to other techniques or device.

A. Working Of Fingerprint Module

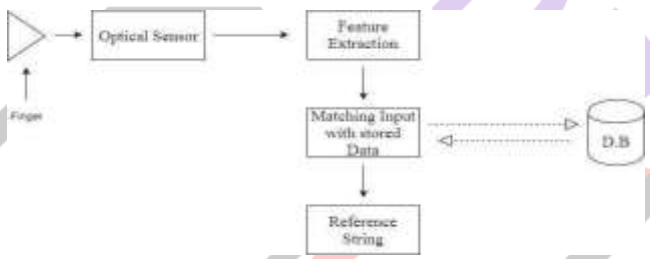

Fig.2 fingerprint sensor

In fig[2] Fingerprint scanner reads the data through the optical scanner sensor and authenticates it with the enrolled data in the database on the cloud. If authentication is successful it provides a UID. Using UID fetches the detail information from the bank database. In author on cloud we can securely handle critical data by the use of biometric fingerprint this helps to use here cloud technology.

Fingerprint scanner used for scanning is optical scanner. It basically performs two tasks:

- Takes the image of the fingerprint.
- Determines whether the design of new fingerprint image matches the previously stored image.

One of the key aspect or major factor which need to consider, quality of the finger image. Factors affected to the quality of image are

- Skin Conditions: - Dryness, Wetness, Dirtiness, Temporary or Permanent Cuts, Bruises, etc.
- Sensor Conditions: - Dirtiness, Noise, Size and User co-operation.

Once the fingerprint is validated the system requests web services for the account details of the user. The details of all the bank accounts of user are displayed for the further transaction.

The following table gives the detailed information of fingerprint Scanner devices.

Fingerprints Devices	**Devices/Technology used**	**Performance**	**Cost**
Optical scanner	Scanner	High	Less expensive
Ultrasonic scanner	Sensors	Slow	Expensive
Capacitive scanner	Capacitors	medium-low	Expensive

B. FUNCTION OF WEB SERVICES:

Web services play important role of carrying data between cloud and bank database & gives it to the machine that is used for establishing as an interface for the users.

C. WORKING OF GSM MODULE:

The account details of user are stored on cloud in centralized manner. The account details of all the bank accounts of account holder are displayed. User needs to select one of the bank accounts for the transaction. If user wants to transfer the money or debit the money from account he will get OTP on registered mobile number. The GSM module generates OTP for enforce authenticate transaction from the bank side.

This OTP needs to be entered for the transaction to be carried out. Once the transaction is completed system will get back to homepage.

2. LITERATURE SURVEY

A survey, as a comparative case study is given in Table I. It deliberates the Biometric techniques in enhancing the security for ATM transaction and other system.

TABLE I: Literature Review Table

Sr.No.	Title of the Papers	Technology / Method	Advantages	Drawbacks
1.	A Self Banking Biometric M/C with Fake Detection Applied to Fingerprint and Iris along with GSM Technology for OTP [5]	RFID, Biometric and GSM	1. Trusted Authenticati on 2. Increases the security 3. High accuracy	May be GSM module or network failure occurs
2.	A Constraint-based Biometric Scheme on ATM and Swiping Machine [13]	Electronic Data Capture (EDC)	1.Durability of sensor 2.Securityan d Reliability	Time consumption, noise and sensor issue

3.	Biometrics in Human-Machine Interaction[3]	Human-Machine interface technologies , decision making techniques	1.provide decision making support to system 2.high accuracy	System needs to be sensitive to cultural differences, facial expressions.
4.	Biometric Quality: A review of fingerprint, iris and face [6]	QA Algorithm	Strong Performance	More noise created.
5.	Short Term Face Recognition for Automatic Teller Machine (ATM) Users [7]	Magnetic stripe for data storage	1.Data can be Altered if Necessary 2.Inexpensive	Breakable, data can be Destroyed
6.	ATM terminal Design is based on fingerprint recognition.[8]	ARM 9,GSM,Gabor filter Algorithm and Direction Filter	1. Stability And Reliability of Fingerprint Characteristics .2. Security	Fingerprint image contains a lot of noise, thus it is time consuming.
		Algorithm, Embedded System.	features were enhanced.	

3 MATHEMATICAL MODEL

System = { I, S, i, o, s, f }

S = { S1, S2, S3, S4, S5, S6, Si, Si1, Si2,… , Sin }

Where,

I = initial state (user). S = states.

i = set of inputs. o = set of outputs.

s = success of operation. f = failure of operation

4. PROBLEM STATEMENT

Every individual has multiple bank accounts in different banks, people need to carry multiple ATM cards for transaction, there may be different PINs for every account. At times it happens that we forget ours PINs, lose our cards, cards get stolen, stolen PINs such scenario are faced in our daily life, so to overcome these problem, "Design One Touch Multi- banking Transaction System using biometric and GSM authentication" is proposed.

5. CONCLUSION

In the proposed card-less multi-banking Transaction ATM system, replaces the traditional ATM system. It has advantages such as saves manufacturing cost of cards and overcomes drawbacks of the traditional system like carrying multiple cards, losing of card, losing PINs, remembering multiple PINs, fraud calls related to ATM card, etc. and provides high security by using authentication like fingerprint and OTP system; therefore making it easy to use multiple bank account transaction in a single touch.

REFERENCES

[1] A. K Jain, K Nandakumar, and A Nagar, "Biometric Template Security," 2008, ACM, , DOl.10.1155/2008/579416.
[2] Mohsin Oza, Dr.D.R.Kalbande, "Enhanced Security for ATM machine with OTP and facial recognition features,"International Conference On Advanced Computing Technologies and Applications(I CATA- 2015).
[3] W. A. Shier, S. N. Yanushkevich "Biometrics in Human- Machine Interaction," The International Conference On Information and Digital Technologies2015.
[4] http://biometrics.pbworks.com/f/comparisontable.png Last seen 02 Sept2017
[5] Joyce Soares, A. N.Gaikwad "A Self Banking Biomtric M/C with Fake Detection Applied to Fingerprint and Iris along with GSM Tech. for OTP," International Conference on Communication and Signal Processing, April 6-8, 2016,India.
[6] Joyce Soares, A. N.Gaikwad "A Self Banking Biomtric M/C with Fake Detection Applied to Fingerprint and Iris along with GSM Tech. for OTP," International Conference on Communication and Signal Processing, April 6-8, 2016,India.
[7] Yun Yang , JiaMi, "ATM terminal design is based on fingerprint recognition," 978-1- 4244-6349-7/10/$26.00 ©201 0 IEEE
[8] https://www.bayometric.com/fingerprint-reader-technology- comparison/Last seen 02 Sept2017.
[9] Joyce Soares , A.N.Gaikwad, "Fingerprint and Iris Biometric Controlled Smart Banking Machine Embedded with GSM Technology for OTP," 2016(ICACDOT) Shweta Singh, Akhilesh Singh, Rakesh Kumar, "A Constraint- based Biometric Scheme on ATM and Swiping Machine," 2016 International Conference on Computational Techniques in Information and Communication Technologies(ICCTICT).
[10] Iwasokun Gabriel Babatunde, Munda Josiah Lange, Akinyokun Oluwole Charles, Dehinbo Johnson Olumuyiwa, "Experimental Study of Thumbprint-Based Authentication Framework for ATM Machines," Science and Information Conference 2014 August 27-29, 2014 | London,UK.
[11] Shimal Sri Das, Debbarma Jhunu (2011), "Designing a Biometric Strategy (Fingerprint) Measure for Enhancing ATM Security in Indian E-Banking System," Ibidapo, O. Akinyemi, Zaccheous O. Omogbadegun, and Olufemi M. Oyelami (2010), "Towards Designing a Biometric Measure for Enhancing ATM Security in Nigeria eBanking System,"International Journal of Electrical & Computer Sciences IJECS-IJENS Vol: 10 No: 06, pages68-73.