A Succinct Analysis of Applications and Services Provided by ATM transaction using fingerprint technology

[1]Zenith Mohanty, [2]Sangram Rout

[1,2]Department of IT, C.V. Raman College of Engineering, Bhubaneswar
mohantyzenith@gmail.com[1], sangramrout007@gmail.com[2]

Abstract -This paper deals with solutions related to ATM (Automated teller machines) security. Fingerprinting technology is rapidly progressing and it offers lots of opportunities to the users. The main objective of this method is to make ATM transactions as secure as possible. The fingerprint concept is chosen because it provides availability, reliability and uniqueness with high accuracy. The system verifies fingerprint images with saved fingerprint and gives accurate fingerprint result that if it is valid or invalid to the user who uses the ATM machine. In this way we can improve and enhance the security of ATM system to control increasing crime circle of ATM.

Index Terms—**Accuracy, ATM (automated teller machine), Reliability, Uniqueness**

I. INTRODUCTION

Biometric technology is an art of technology for measuring and analyzing biological data. For example, it may analyze any biological data such as DNA, fingerprint, eye retina etc. In ATM machines, particularly biometric technology can be used in the form of fingerprinting technology in order to detect and verify fingerprinting images and produce the accurate result. This method provides several advantages over traditional or old method and current method that is used in our daily life. Basically this fingerprint technology focuses on two basic functions. One is identification and another is verification.

In fingerprinting technology users fingerprints are scanned using biometric technology and then this are stored in the database. All fingerprints are unique in themselves. A normal fingerprint consists of lines and spaces. This lines are called ridges and the spaces in between the lines are called valleys. This fingerprint system is easy to use and most suitable for everyone. Fingerprint is a unique identity of any user.

II. PRESENT ATM SYSTEM

In present ATM systems, customers do their transactions from ATM by inserting a plastic ATM card with a magnetic stripe that contains unique identification number and some security information such as expiry date. This unique identification number is called PIN. PIN is a 4 digit number which is generated by any bank. PIN is very easily remembered and is also changeable according to

the user so that an attacker would need to guess an average of infinite times to get the correct PIN. In the present system user have to insert plastic ATM card to the ATM machine. If the pin is found correct the user is allowed to do transaction. If pin is found wrong, then system again asks for pin number until a correct pin is not entered (allowed maximum up to 3 times).

III. ATM SYSTEM USING FINGERPRINT TECHNOLOGY

The objective of this system is to use fingerprints in ATM system.

The main difference between this system and present ATM system is that, this system is more relaxing and easier than present ATM system because in this system, there is no need to remember 4 digit pin number for any access. Here, we just have to place finger on the fingerprint scanner and if the user is an authorized, he is permitted to do the transaction. Fingerprint generates a code as SMS to user mobile number, which is used for validation purpose. If the code entered by user is valid, then user performs transaction on the basis of it.

There are two main phases of proposed ATM system. They are

1) Enrolment/Scanning phase

2) Authentication/Checking phase

Enrolment/Scanning phase

Enrolment phase is also known as registration phase. In this phase, the user scans its fingerprint using the fingerprint scanner and stores into the database.

Authentication/Checking phase

In authentication phase, an individual is checked or verified by matching the test image provided by him with the stored image(fingerprint image that is stored in the database) i.e. it is checked that he is who claims to be.

Detailed working of ATM system using fingerprinting technology is as follows:

Data collection unit: data collection unit is a unit which collects data in form of user fingerprints and stores it into the database or to the main server. This unit generate a byte for every storing newly added user fingerprint. If the fingerprint is placed on the sensor then definitely data collection unit will generate a byte which will range from 0x00 to 0xFF. But if no finger is placed then, it will return code which is "0xFF" (it means in case of error).

Image pre-processing unit: after the scanner scans the fingerprint of the user, it takes the input image of the fingerprint for pre-processing. In pre-processing unit the input image of fingerprint can be called as test image. So in pre-processing unit, basically test image (which is in analog form) is converted into digital form. If quality of the digital image is good, it is then converted into a template (it is a kind of pattern).

Data storage unit: this unit stores the template that are generated from pre-processing unit into the database. The template are that are to be stored into the database are of size 512 bytes (approx.).

Search unit: in search unit, search function is called while placing finger on the sensor. In this unit, once a search function is called then existing memory is checked and if matching is found, this search function returns a matching ID.

Decision unit: this unit decides whether user of the input is an authorized user or not. This is only possible thorough image comparison. The input image is compared with stored image in database. This stored image and needed image is compared and needed resolution is 500dpi (dots per sec). If image comparison is satisfied, unit decides that the input is authorized user.

Transaction unit: if the decision unit decides that the user of input is an authorized user, then transaction is carried out successfully.

Empty unit: this unit calls a function called as empty function. This function is called after the transaction is completed successfully. This function empty the database containing fingerprints stored in it.

Flow chart of ATM system using fingerprint technology is shown as follows:
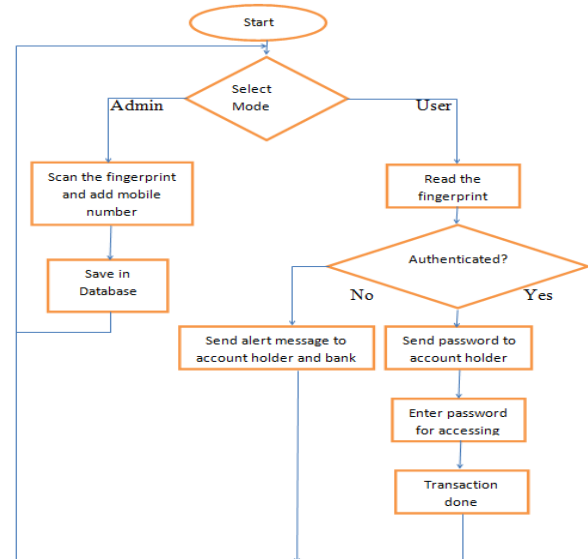

IV. METHODOLOGY

The ATM user access any banking transaction on the basis of the following methodology.

Any banking institution first asks to an individual to choose any 4 fingers of their hands according to the assigned 4-digit PIN number. When the ATM holder goes to the ATM system first the system asks user to position their 4 fingers on the fingerprint scanner (According to the fingerprinting technology).

First of all the user position its first finger which indicates the first digit of the pin number. Then the system verifies whether fingerprint that is scanned for first digit of the pin number is correct or not. If the match is found correct then the user is allowed to position second finger on the fingerprint scanner which indicates the second digit of the pin number. Same rule can be applied for the second finger also. If the second fingerprint is matched then the user is allowed to position the third finger which indicates the third digit of the pin number.

Similarly the user registers its third finger for third pin digit verification. If the match is found correct then user is allowed to place its fourth finger which indicates the 4th digit of the pin number. And at last if this finger is found correct then finally the user is permitted to withdraw any amount (up to the given withdrawal limit) from the ATM system. So this is the methodology how the user access any banking transaction from ATM system. For example, in the following figure we can see how a user have chosen its fingers according to the 4-digit pin number 1204. According to the following figure first of all the user will place its first finger for first pin digit verification i.e. 1. If first fingerprint is matched then user will place its second finger for second pin digit verification i.e. 2. If this fingerprint is matched then user continue to follow the same procedure until all the fingerprints are matched i.e. 0 and 4. Now finally the user is allowed to withdraw its

desired amount and successfully complete the banking transaction.
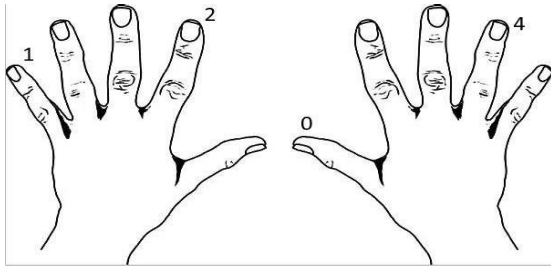
V. ADVANTAGES OF ATM USING FINGERPRINTING

1. Fingerprinting technology in ATM provides accuracy because identical matches of fingerprints are nearly impossible.

2. The image template of scan fingerprint requires less memory.

3. Implementation of this system provides more security to ATM transaction and improves authentication.

4. The fingerprints are never lost or forgotten.

5. The system is easy to install, less time consuming and mostly approved biometric system.

VI. DISADVANTAGES OF ATM USING FINGERPRINT

1. More awareness is required: Users need to know how to position their finger, face and eye. If the user itself is not aware of this modern technology then due to this lack of knowledge it may become difficult for the user to access any banking transaction from ATM.

2. Expensive: Fingerprint technologies are available in $100 range but still majority of technologies are closer to the $500.

3. Affected by environment and disease: In some situations, in the case of fingerprints technology cold or moist hands for fingerprint scanners can block the devices. So this may lead to some bad impact on fingerprinting ATM systems.

VII. SYSTEM DESCRIPTION

In order to implement the fingerprint technology we need to deploy following hardware components.

1. Microcontroller (LPC2148)

2. Fingerprint module (FIM3030)

3. GSM modem

4. User Interface

5. Power supply
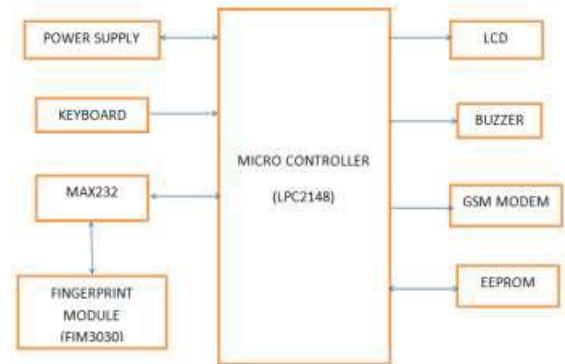
VIII. CONCLUSION

The implementation of ATM security by using fingerprint recognition is a vital step as well as it is very difficult. For security purpose and to have a control over criminal records it is necessary to bring fingerprint system into our present era. Fingerprint have unique features and characteristics that do not change for whole life and are different individually. The whole system designed by using this fingerprint technology makes its very reliable, secure and easy to use.

REFRENCES

[1] Dhiraj Sunhera "Fingerprint based Biometric ATM authentication system", International journal of engineering inventions.

[2] Sneha Ramrakhyani, Manisha Meshram, Lata Chandni, Rasjanli Gothe, Parul jha "Fingerprint based ATM system: survey", International journal of innovative research in science, engineering and technology.

[3] Namrata, Dr Sukhvir "Review paper on enhance the ATM security using fingerprint recognition", International journal of computer science and mobile applications.

[4] V.Ajantha Devi, A.Priyanka "the evolvement of ATM using fingerprint", International journal of computer science Trends and Technology.

❖ ❖ ❖