International Journal of Trend in Scientific Research and Development (IJTSRD)
International Open Access Journal | www.ijtsrd.com
ISSN No: 2456 - 6470 | Volume - 2 | Issue – 6 | Sep – Oct 2018

# Secure E-Banking Using Bioinformatics

**Bilal Hussain Ch, Subayyal**
Research Scholars, Department of Computer Science and Engineering,
University of Engineering & Technology, Lahore, Pakistan

**ABSTRACT**
During the past decade e banking has emerged with enormous speed. The use of e banking and the application of e banking is now enormous these days. But the modern banking completely relies on internet and computer technology, the threats and the chances of breaching the security has also increased. We are totally dependent on the internet to carry out the transactions and the daily routines in the banks. Thus there is the immense need of increasing the security in the banking field. We have developed the system in which we have developed a secure banking system. We are using Finger print authentication device and the GSM module to carry out the functionalities of the system.

***Keyword:*** *Finger Print authentication device, GSM module.*

## I. INTRODUCTION

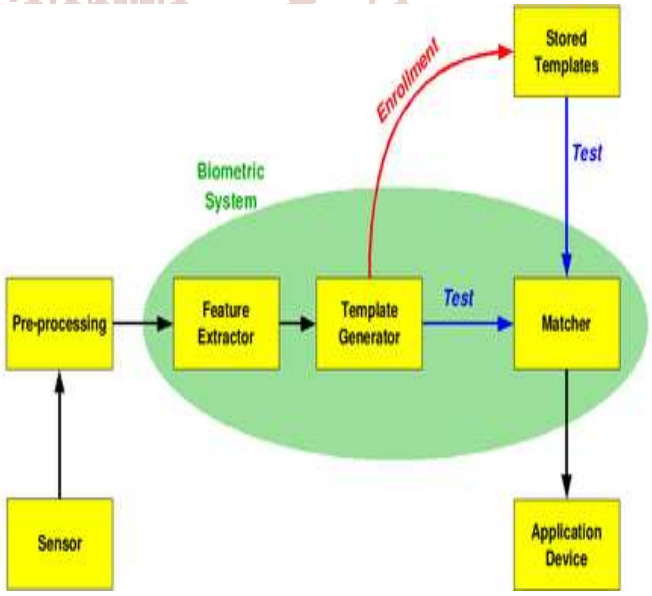
During the last decade the banking structure has been converted into the e banking system in which the daily routine work is being implemented using internet and advanced computer technology. Because of the immense need of the use of internet there is an immense threat of the hacking and disturbing the structure of the banking.

We have developed such a system that will ensure safety in to the present structure of the e banking. We have used a technique in which we are using a Finger print authentication device and the GSM module to enhance the security in the e banking system up to the next level.

Our proposed methodology is that when the user is ready to carry out the transactions and to perform some of the functions in his/her account he/she is required to authenticate himself/herself using Finger print authentication device.

The print of the user is matched with the one placed in the database, if the print matches a code will be send to the number of the user and the user is prompted to input the code received, if the code matches the one send by the system the user will allow to perform the transactions and make changes in the system. This process will ensure the security in the system to the next level.

In the first process in which the finger print is authenticated, we have used different MATLAB functions and schemes and algorithms for matching the print of the finger with the one placed in the database.




## II. EXISTING WORK IN CONTROL SYSTEMS

1. It is important for the banks to provide their Customers, a safe and secure access to their Accounts, sometimes hackers try to access the different user accounts by hacking the Automated Teller Machine. To prevent the Automated Teller Machine to be hacked by different hackers' finger

print scanner should be provided with each Automated Teller Machine. By providing Finger scanner with each Automated Teller Machine it will ensure after verifying that account was accessed by the original customer or by the specific person who had the access for that account. This will ensure security and will prevent from unauthorized access.

2. As banking system is shifting toward online banking system where they always need internet to send and receive information .some criminal hackers try to hack different user accounts through internet if they successfully access some accounts, then it results in the form of big loss for the customer and for the banks also. So it is necessary that the customer should be securely identified before each login to the accounts for this purpose different technologies should be used for safe and secure access to the account and for the identification of the customer.
3. ATM is the electronic telecommunication device used for transaction. It can be accesses by anywhere for cash with draw, deposit money and transfer funds, but no proper authentication is used. So there is need to securely identify the person before accessing the account so therefore face recognition should be used that will ensure the authorized access to the account was made , otherwise user will not be able to login if face recognition process was not completed.

## III. Hardware used in the system

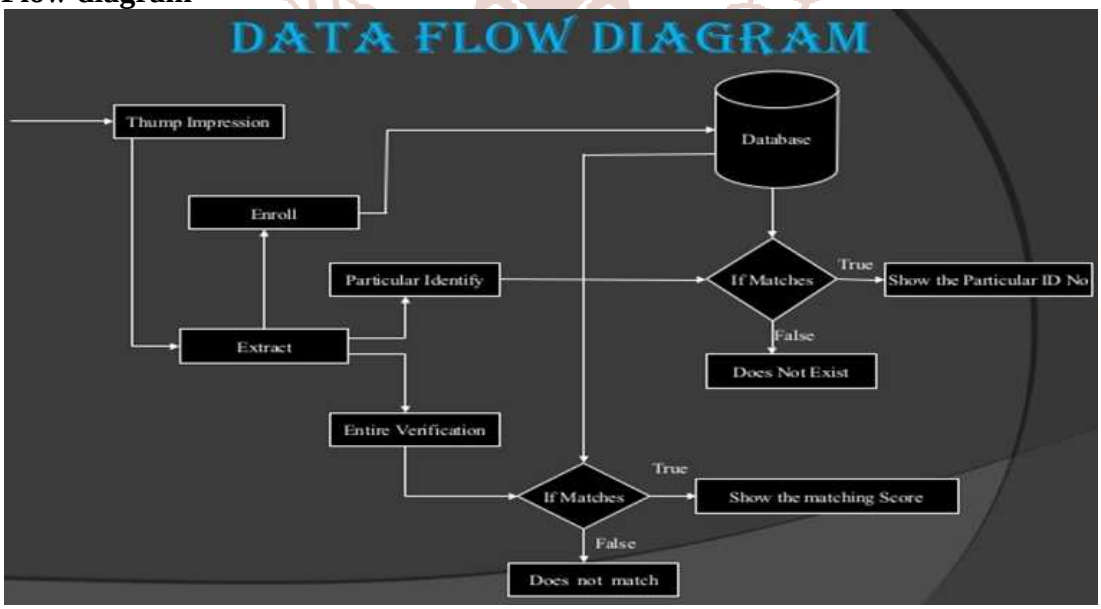
The hardware implemented in the system are finger print authentication device and the GSM module. Both the modules have vital and different importance in the system.

Finger print authentication device:

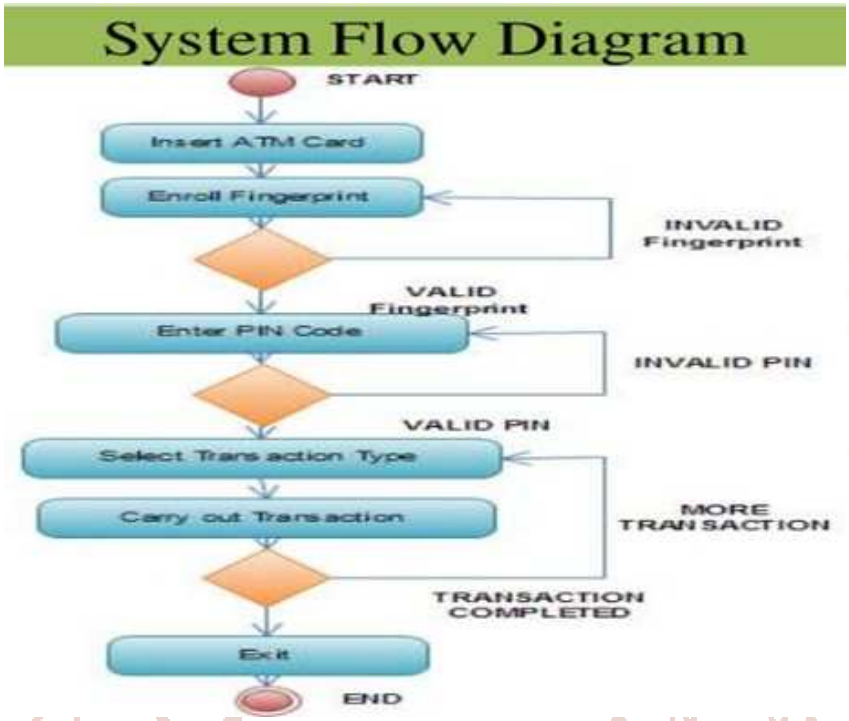
The device is used to authenticate the user and authentication process occurs every time the user wants to make changes in the account or to with draw or to submit funds in the account.


We are using the GSM module which has the functionality to send the code message to the user to after the authentication phase. The user has to enter the code in the given field to perform the transactions and the if the code entered by the user matches with the one send by the system the user will be given the perform the transactions.

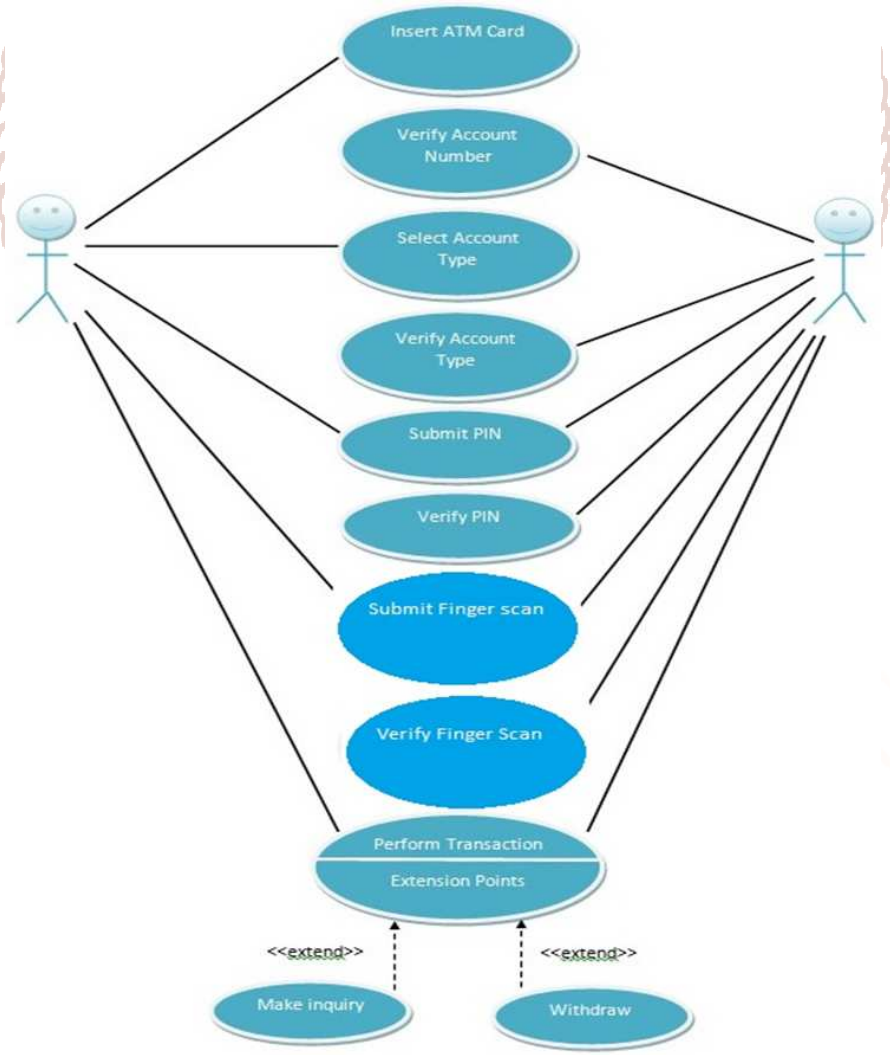
## IV. Data Flow diagram



**System flow diagram**:-



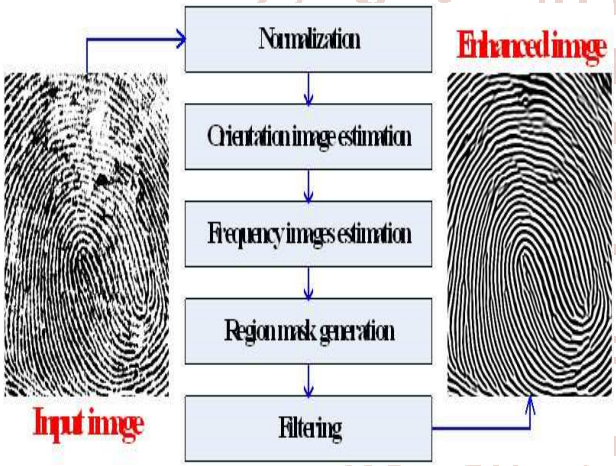

**Use Case Diagram:-**



**Explained View of the system:-**
In our system we have used the methodology which consists of three phases. Now we will explain the entire structure and the working of the system.

**Registration phase:-**
In this phase the user is registered. This is the first phase. When the user wants to open an account in to the bank, the user is required to give his/her finger impression to register himself / herself. Besides setting up the PIN password the user is also registered on the basis of the finger print impression. The user is asked to place the finger three times on the finger print scanner to get the fair good and clear image of the finger.

Besides this we have used other MATLAB functions and also created some of them to enhance the image and to place in the database. We have used Normalization techniques and frequency distribution techniques and orientation image estimation and the region mask distribution.




**Authentication Phase:-**
In this phase the user is authenticated. This process is done by matching the finger print impression of the user with the finger print impression saved in the database. In this phase only the registered user can enter. When the user is registered the PIN number is given to him/her also with account number and the account password. In this phase the user enters the ATM booth enter the account number. Enter the account type. Verify type. Enters the pin. Then the PIN is verified. Then comes the use of the Finger print authentication device. The user submits the impression of the finger and that impression is checked with the one placed in the database. If the impression matches the one placed in the database the user is allowed to access the account and perform the activities. If not the user will be blocked and will not be allowed to access the account and perform the transactions.

**GSM code generation phase:-**
This phase is used for enhancing and ensuring the security in to the system to the next level. When the user is authenticated the system will send the code to the number given by the user at the time of the registration. The user is then prompted to enter the code in the required field. Then the code is checked with the code send by the system, if the code matches, the user is fully authorized to access the account and perform the functionality. If the code does not matches the user is blocked to perform the functionality and will not be authorized.

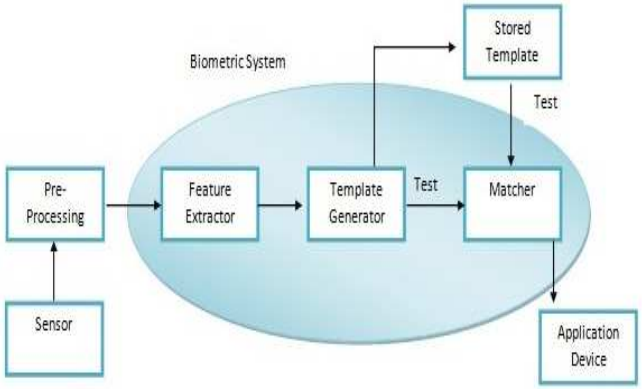



Fig. Working of Biometric Authentication

**Benefits of our proposed methodology:-**
The benefits of proposed system are:-

**Fairness:-**
Our system will introduce fairness in the e banking process to next level. As the methodology proposed by us is nearly impossible to break. So it will introduce fairness in the electronic banking process.

**Uniqueness:-**
We have defined uniqueness in our system. Every user has the unique identity because of the unique finger print. No user would be allowed to access the account of any other user.

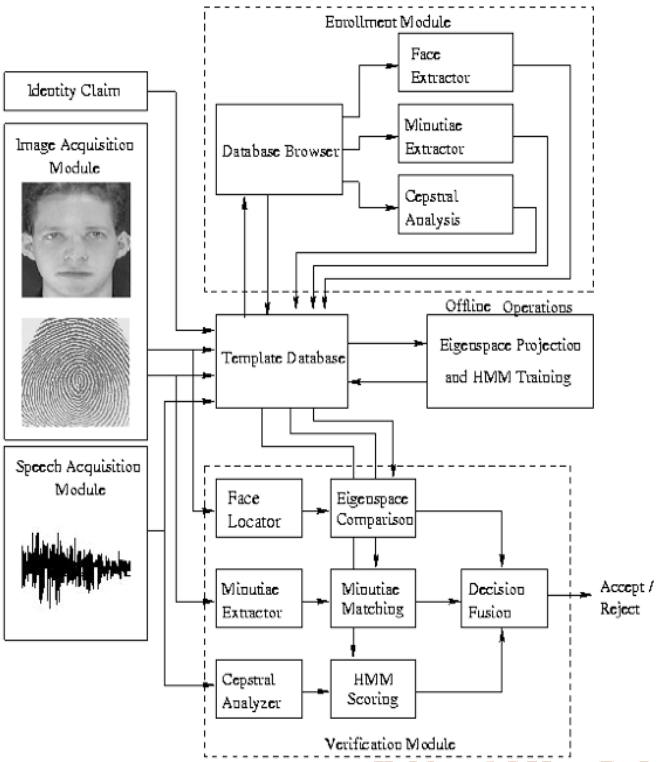
**Privacy:-**
We have paid special attention to privacy in our system. The privacy of the user will be maintained on all conditions.

**Accuracy:-**
Our methodology is accurate. We have introduced accurate and dependable devices in the system. They will provide the most accurate result is all conditions.

**Efficiency:-**
Efficiency is the important factor that we have considered.

**Conclusion:-**
We have developed a system which can be implemented in the e banking system. We have used advanced security techniques. We make the use of the finger print authentication device and the GSM module.

**Future work:-**
For the future various biometric techniques can be implemented to enhance the security in the system.




Face detection and the voice recognition techniques can be used to enhance the security.

**References:-**


1. Ratha, Nalini K., Jonathan H. Connell, and Ruud M. Bolle. "Enhancing security and privacy in biometrics-based authentication systems." *IBM systems Journal*40.3 (2001): 614-634.
2. Jain, Anil K., et al. "An identity-authentication system using fingerprints."*Proceedings of the IEEE* 85.9 (1997): 1365-1388.
3. Jain, Anil K., et al. "Filter bank-based fingerprint matching." *Image Processing, IEEE Transactions on* 9.5 (2000): 846-859.
4. Liu, Simon, and Mark Silverman. "A practical guide to biometric security technology." *IT Professional* 3.1 (2001): 27-32.
5. Gullman, Lawrence S., Eric Edwards, and Norman Fast. "Biometric token for authorizing access to a host system." U.S. Patent No. 5,280,527. 18 Jan. 1994.
6. Zhang, Lin, et al. "Online finger-knuckle-print verification for personal authentication." *Pattern recognition* 43.7 (2010): 2560-2571.
7. Council, Federal Financial Institutions Examination. "Authentication in an internet banking environment." *Financial Institution Letter, FIL-103-2005. Washington, DC: Federal Deposit Insurance Corp. (FDIC). Retrieved March* 18 (2005): 2005.