FINGERPRINT BASED ATM SYSTEM

1G. Vishwas, 2G. Prudhvi Raj, 3N. Shreya , 4Mr. B. Ravi Raju
123B.Tech Students, 4Assistant Professor
Department of Information Technology,
ANURAG GROUP OF INSTITUTIONS, Hyderabad

ABSTRACT

The main aim of this project to provide secure banking system, by taking fingerprints as authorized identity at ATM/banks. The purpose of the project is to provide a secured and reliable environment to the customers for their banking transactions by providing a unique identity to every user using the FINGER PRINT identification technology.

Identification and verification of a person today is a common thing; which may include door-lock system, safe box and vehicle control or even at accessing bank accounts via ATM, etc which is necessary for securing personal information. The conventional methods like ID card verification or signature does not provide perfection and reliability. The systems employed at these places must be fast enough and robust too. Use of the ATM (Automatic Teller Machine) which provides customers with the convenient banknote trading is facing a new challenge to carry on the valid identity to the customer. Since, in conventional identification methods with ATM, criminal cases are increasing making financial losses to customers.

Fingerprint Based ATM is a desktop application where fingerprint of the user is used as a authentication. The finger print minutiae features are different for each human being so the user can be identified uniquely. Instead of using ATM card Fingerprint based ATM is safer and secure. There is no worry of losing ATM card and no need to carry ATM card in your wallet. You just have to use your fingerprint in order to do any banking transaction. The user has to login using his fingerprint and he has to enter the pin code in order to do further transaction. The user can withdraw money from his account. User can transfer money to various accounts by mentioning account number. In order to withdraw money user has to enter the amount he want to withdraw and has to mention from which account he want to withdraw.The user must have appropriate balance in his ATM account to do transaction. User can view the balance available in his respective account. The system will provide the user to view last 5 transactions.

I.INTRODUCTION

1.1 OVERVIEW

Biometrics is the art of science and technology of measuring and analyzing biological data. If biometrics refers to technologies that measure and analysis human body characteristics, such as DNA, fingerprinting, eye retina and irises, voice pattern, facial pattern and measurement for authentication purposes. Biometrics identifier method provides several advantages over the traditional method and current method used in our daily life. Basically concentrate on two function one is for identification and other verification. A modern ATM is typically made up of the devices like CPU to control the user interface and devices related to transaction, magnetic or chip card reader to identify the customer, Pin pad, secure crypto-processor generally within a secure cover.

Display to be used by the customer for performing the transaction, function key button, record printer to provide the customer with a record of their transaction, to store the parts of the machinery requiring restricted access- vault, housing for aesthetics, sensors and indicators. In this modern era there are many people using ATM. Fast development of banking has various advantages and disadvantages.

The main objective of this system is to develop an embedded system, which is usedfor ATM security applications. In these system, Bankers will collect the customer finger prints while opening the accounts then customer will only access ATM machine. Theworking of these ATM machine is when customer place finger on the finger print module itdisplays the name of the customer on the LCD connected to the micro controller. If the user does not have a account activated by a fingerprint initially it does not allow the user to do transactions. Nowadays, using the ATM (Automatic Teller Machine) which provides

customers with the convenient banknote trading is very common. However, the financial crime case rises repeatedly in recent years; a lot of criminals tamper with the ATM terminal and steal user's credit card and password by illegal means. Once user's bank card is lost and the password is stolen, the criminal will draw all cash in the shortest time, which will bring enormous financial losses to customer. How to carry on the valid identity to the customer becomes the focus in current financial circle. Traditional ATM systems authenticate generally by using the credit card and the password, the method has some defects. Using credit card and password cannot verify the client's identity exactly. In recent years, thealgorithm that the fingerprint recognition continuously updated, which has offered newverification means for us, the original password authentication method combined with the biometric identification technology verify the clients' identity better and achieve the purposethat use of ATM machines improve the safety effectively.

II.EXISTING SYSTEM

We are using ATM's in our country for all our banking activities. An automated teller machine (ATM) is an electronic telecommunications device that enables customers of financial institutions to perform financial transactions, such as cash withdrawals, deposits, transfer funds, or obtaining account information, at any time and without the need for direct interaction with bank staff. On most modern ATMs, customers are identified by inserting a plastic ATM card (or some other acceptable payment card) into the ATM, with authentication being by the customer entering a personal identification number (PIN), which must match the PIN stored in the chip on the card (if the card is so equipped), or in the issuing financial institution's database.

Using an ATM, customers can access their bank deposit or credit accounts in order to make a variety of financial transactions such as cash withdrawals, check balances, or credit mobile phones. ATMs can be used to withdraw cash in a foreign country. If the currency being withdrawn from the ATM is different from that in which the bank account is denominated, the money will be converted at the financial institution's exchange rate.

III.PROPOSED SYSTEM

We are using ATM's in our country for all our banking activities. An automated teller machine (ATM) is an electronic telecommunications device that enables customers of financial institutions to perform financial transactions, such as cash withdrawals, deposits, transfer funds or obtaining account information, at any time and without the need for direct interaction with bank staff. In our proposed system we are introducing finger print sensor in which when a user scans their finger, if that user is valid or not.

A biometric authentication system seems to be an excellent solution to authentication problems; however biometric authentication has some weaknesses.

Biometrics is a rapidly evolving technology that is being widely used in forensics, such as criminal identification and prison security, and that has the potential to be used in a large range of civilian application areas. Biometrics can be used to prevent unauthorized access to ATMs, cellular phones, smart cards, desktop PCs, workstations, and computer networks. In automobiles, biometrics can replace keys with keyless entry devices.

There are two main objectives of this paper, as follows: - 1. To integrate the fingerprinting in access control for ATM system. 2. To purpose a framework for the ATM system using fingerprint verification.

IV.LITERATURE REVIEW

System analysis is the performance management and documentation of activities related to the life cycle phases of any software namely:

- The Study Phase
- The Design Phase
- The Development Phase
- The Implementation Phase
- The Testing Phase

Software Analysis starts with a preliminary analysis and later switches on to a detailed one. During the preliminary analysis the Analyst takes a quick look at what is needed and whether the cost benefits. Detailed analysis studies in depth all the cornered

factors, which builds and strengthens the software.

SRS

SRS (Software Requirement Specification) is a document that completely describes what the proposed should do, without describing how the software does it.

Performance Requirements

1) The operation time should be small and the throughput should be high.
2) It should produce timely and accurate result.

Software Quality Attributes

i) **Maintainability** – Since it is directly associated with the database, so there is very little maintainability problem with this application.
ii) **Easy to Learn –** Since there are less number of forms, this application is very easy to learn with user-friendly screens.
iii) **Flexibility** – This application is very much flexible for future enhancements.

Hardware Requirements

- System : Pentium IV 2.4 GHz.
- Hard Disk : 40 GB.
- Floppy Drive : 1.44 Mb.
- Monitor : 15 VGA Colour.
- Mouse : Logitech.
- Ram : 512 Mb.

Software Specifications

- **Operating System:** Windows
- **Coding Language**: Python 3.7

V.MODULES

Most biometric technology systems use the same basic principles of operation. First, a person must be registered, or enrolled, on the biometric system.

1. Enrollment:

The process by which a user's biometric data is initially acquired, accessed, processed, and stored in the form of a template for ongoing use in a biometric system is called enrollment. Subsequent verification and identification attempts are conducted against the template(s) generated during enrollment.

2. Presentation:

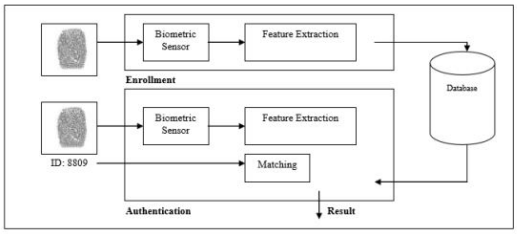
Presentation is a process by which user provides biometric data to an acquisition device-the hardware used to collect biometric data. Depending on the biometric system, presentation may require looking in the direction of a camera, placing a finger on a platen, or reciting pass phrase.

3. Biometric data:

The biometric data users provide in an unprocessed image or recording of a characteristic. The unprocessed data is also referred to as raw biometric data or as a biometric sample. Raw biometric data cannot be used to perform biometric matches. Instead, biometric data provided by the user during enrollment and verification is used to generate biometric templates, and in almost every system is discarded thereafter. Thus Biometric systems do not store biometric data-systems use data for template creation. Enrollment requires the creation of an identifier such as a username or ID. This identifier is normally generated by the user or administrator during entry of personal data. When the user returns to verify, he or she enters the identifier, and then provides biometric data. Once biometric data has been acquired, biometric templates can be created by a process of feature extraction.

4. Feature extraction:

The automated process of locating and encoding distinctive characteristics from biometric data in order to generate a template as called feature extraction. Feature extraction takes place during enrollment and verification-any time a template is created. The feature extraction process includes filtering and optimization of images and data in order to accurately locate features. For example, voice-scan technologies generally filter certain frequencies and patterns, and finger-scan technologies often thin ridges present in a fingerprint image to the width of a single pixel. Since quality of feature extraction directly affects a system's ability to generate templates, it is extremely important to the performance of a biometric system.



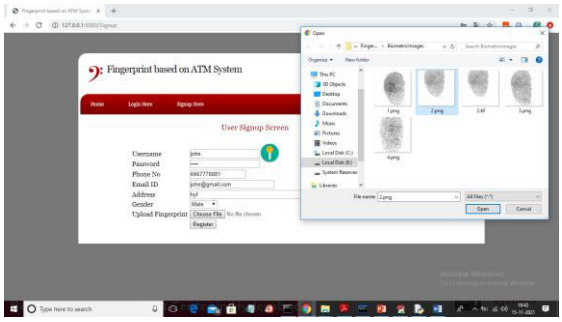
VI.OUTPUT

All existing banking applications are authenticating users based on PIN NO or password but this technique is not secured so in propose online banking application we are authenticating user based on his finger print. To implement this project we have designed following modules

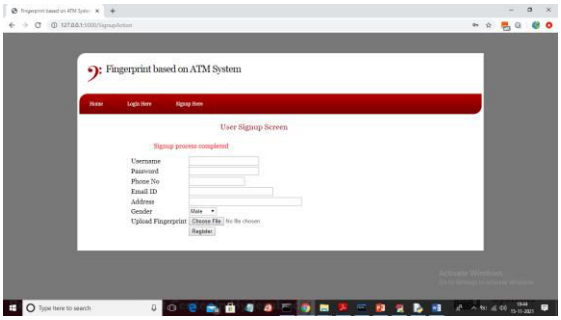
1) Signup: using this module user can signup with the application by using username, password and finger print image. All signup details will be saved in MYSQL database
2) Login: using this module user can login to application by entering username, password and finger print image given at signup time to authenticate himself
3) Deposit: after successful authentication user can deposit amount and it will added to his account
4) Withdraw: using this user can withdraw amount if sufficient balance available
5) View Balance: using this module user can view available balance

First create database in MYSQL by copying content from 'DB.txt' and then paste in MYSQL

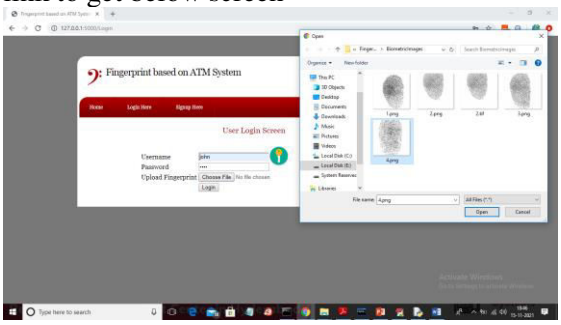
To run project double click on 'run.bat' file to start python FLASK server



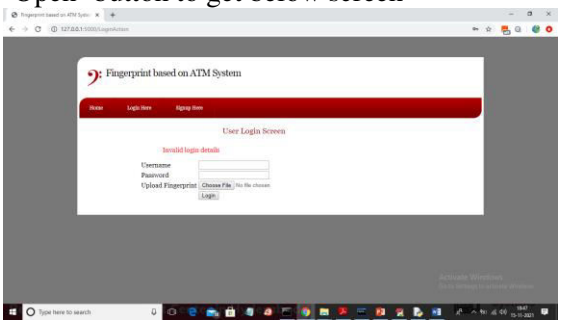
In above screen fill all signup details and then choose finger print image and then click on 'Open' button to load image and to get below screen



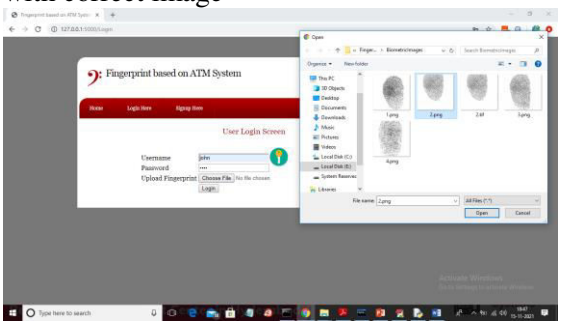
In above screen after pressing 'Register' button we will get message as 'Signup process completed' and now click on 'Login Here' link to get below screen



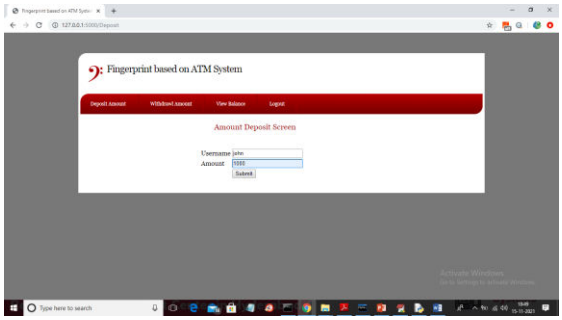
In above screen I am login and selecting wrong finger print as '4.png' and then click on 'Open' button to get below screen



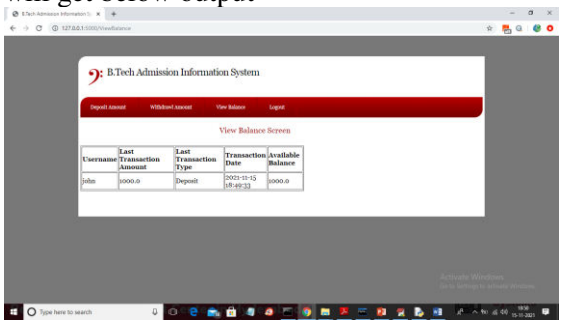
In above screen login is failed and now login with correct image



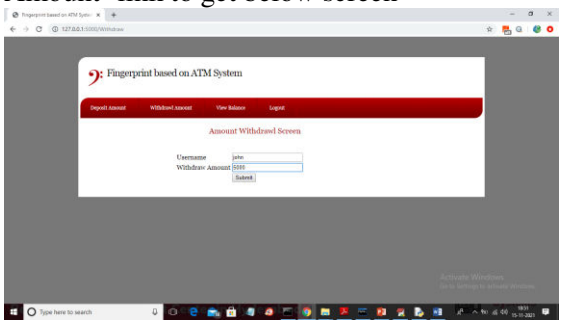
In above screen now i am uploading correct image and press 'Login' button to get below output



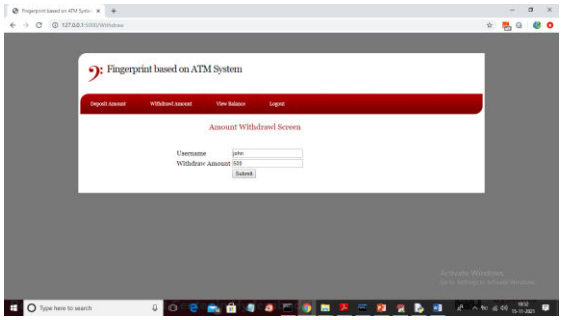
In above screen username will display in default and now enter some amount and press 'Submit' button to complete transaction and will get below output



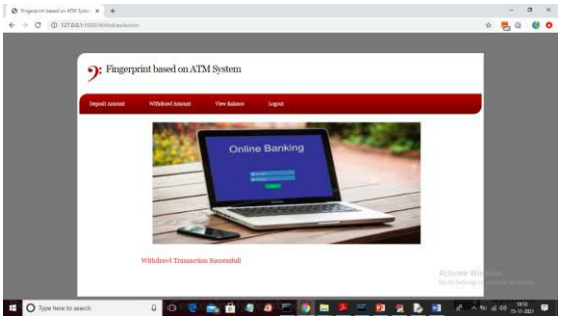
In above screen deposit transaction is displaying and now click on 'Withdrawl Amount' link to get below screen



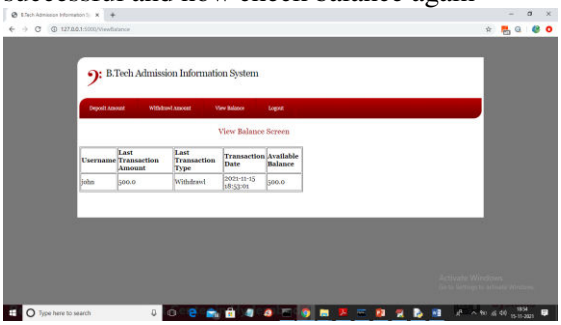
In above screen I am withdrawing amount larger than available amount to get below screen



In above screen 500 is withdrawing and press 'Submit' button to get below screen



In above screen withdraw transaction successful and now check balance again



Now in above screen available balance is 500. Similarly you can perform N number of transaction

VII.CONCLUSION

In today's modern world, autonomous systems play an important role in our day to day life. As the social computerization and automation have drastically increased, it can be seen evidently where the number of ATM centers increases rapidly. Most civilians use ATM's regularly. A good example can be a financial transaction, ease of money exchange etc. So there exists an important factor called security.

The security features were enhanced largely for the stability and reliability of owner recognition. The whole system was built on the fingerprint technology which makes the system safer, reliable and easy to use. As we know that fingerprint are the most acceptable biometrics all over the world in identifying a person. Some government in the world are still implementing fingerprints technique to identify their citizens and the criminal from the scene of crimes in forensic work.

A lot of criminal's tamper with the ATM terminal and steal customers' card details by illegal means. Once users' bank card is lost and

the password is stolen, the users' account is vulnerable to attack. Traditional ATM systems authenticate generally by using a card (credit, debit, or smart) and a password or PIN which no doubt has some defects. The prevailing techniques of user authentication, which involves the use of either passwords and user IDs (identifiers), or identification cards and PINs (personal identification numbers), suffer from several limitations.

REFERENCES

[1] Pranali Ravikant Hatwar and Ravikant B Hatwar, BioSignal based Biometric Practices,
International Journal of Creative Research Thoughts, Vol. 1, No. 4, pp. 1-9, 2013.

[2] Edmund Spinella, Biometric Scanning Technologies: Finger, Facial and Retinal Scanning,
Available at:https://www.sans.org/readingroom/whitepapers/authenticati on/biometric-scanningtechnologies-finger-facial-retinal-scanning-1177.

[3] Gu J, Zhou J, Zhang D.A combination model for orientation field of fingerprints. Pattern
Recognition, 2004, 37:543-553.

[4] N. Selvaraj and G. Sekar, A Method to enhance the Safety Level of the ATM banking industry
using AES Algorithm, International Journal of Computer Applications, Vol. 3, No. 6, pp. 5-9, 2010.

[5] A. Haldorai and A. Ramu, Security and channel noise management in cognitive radio
networks, Computers & Electrical Engineering, vol. 87, p. 106784, Oct. 2020.
doi:10.1016/jcompeleceng.2020.106784

[6] A. Haldorai and A. Ramu, Canonical Correlation Analysis Based Hyper Basis Feedforward
Neural Network Classification for Urban Sustainability, Neural Processing Letters, Aug. 2020.
doi:10.1007/s11063-020-10327-3

[7] J. Yang N. Xiong, A.V. Vasilakos, Z. Fang, D. Park, X. Xu, S. Yoon, S. Xie and Y. Yang A
Fingerprint Recognition Scheme supported Assembling Invariant Moments for Cloud
Computing Communications, IEEE Systems Journal, Vol. 5, No. 4, pp. 574-583, 2011.

[8] J. Leon G. Sanchez G. Aguilar, L. Toscano, H. Perez and J.M. Ramirez, Fingerprint
Verification Applying Invariant Moments, Proceedings of IEEE International Midwest
Symposium on Circuits and Systems, pp. 751-757, 2009.

[9] LO Gorman Overview of Fingerprint Verification Technologies, Information Security
Technical Report, Vol. 3, No. 1, p. 21-32, 1998.

[10] G.B. Iwalokun O.C. Akinyokun, B.K. Alese and O. Olabode Fingerprint Image Enhancement:
Segmentation to Thinning, International Journal of Advanced computing and Applications,
Vol. 3, No. 1, pp. 15-24., 2012.