Transactions Using Bio-Metric Authentication

[1]Dr.D. Thamaraiselvi, [2]Sankaramanchi Seshadri Sarma, [3]Ponguru Praveen Chandu

[1]Asst.Professor, Dept. of Computer Science and Engineering, SCSVMV University, Tamil Nādu, India
[2]Dept. of Computer Science and Engineering, SCSVMV University
[3]Dept. of Computer Science and Engineering, SCSVMV University

---

Abstract - *In previous ATM systems, mostly personal identification number (PIN) is used to verify authentic users which are not secured, and it is very easy to copy. Sometimes thieves have a very strong way to steal our account information, that's why a biometric verification system can be a firm solution. This paper aims to provide a more secure method using biometric features. PIN verification is combined with face recognition in our proposed method to identify a customer during an ATM transaction. Facial data is verified using the Haarcascade Frontal algorithm. To assure security while doing transactions through a swipe machine, the client will confirm the transaction through Facial technology's approval message. In both cases, the Face will be identified through a Camera. If any illegitimate person tries to use the card it will automatically be blocked by the system and detailed information will be sent to the customer through Mail. Hence, this proposed method will provide more advanced security by identifying and reducing fraud.*

***Key Words*: ATM, Bio-metric, face, Transaction, card**

1. INTRODUCTION

The faster improvement of information and communication engineering has affected every aspect of human life in recent years. Therefore, the way of dealing with banking activities has also been changed. ATM is an automatic technique that enables the customers to do economical transactions like swift cash out, fund transfer, balance inquiry, savings withdrawal from anywhere anytime without the aid of a branch representative or teller. To access the account from ATM systems, customers need to hold a debit or credit card on that bank account. Today to pay shopping bills, phone, electricity, gas bills and many more people prefer debit or credit cards most of the time as these cards make sure immediate and simple access to their accounts. A swipe machine also known as electronic data capture (EDC) is used to do this type of transaction. To pay for the things or to complete the transaction, users just need to swipe the debit or credit card through the machine. All customer data is encoded into the magnetic strip on the card and before completing the transaction machine reads the magnetic strip to verify card no, date of expiration, and other features of the customer. Personal Identification Number (PIN) is an important aspect of both ATM and EDC security schemes as it is usually applied to protect the monetary information of a user from illicit access, but only PIN has not been able to make sure the security of the transactions. Bio-metric features can be a solution to this kind of problem. Among all biometric features, a face is recognized as a secured and proven technique. A person's individuality is defined by characteristics and relationships.it can be used as an authentic identification process. In this regard, our proposed method is based on biometric features and message authentication technology to improve security. Here, face identification is checked along with PIN verification to recognize the genuine user during an ATM transaction. Since it is impossible to replicate biometric features like face, to solve the authentication problem, this proposal can be a good solution. During shopping or payment through a swipe machine, the client will get a confirmation Mail through SMPT technology on his/her Mail ID which is registered with the bank to approve the transaction. To identify the illegitimate/fraudulent customer in both cases, the location will also be tracked using a GPS modem during the transaction. This will help to reduce the possibility of abduction and redouble the security of ATM and swipe machine

2. LITERATURE SURVEY:

Balvir proposed a model of designing an embedded system to improve ATM security. Serial communication is managed by the system to scan the cardholder's database, which then immediately generates messages to the mobile of the authorized users through the 89C51 microcontroller-connected GSM module. The main purpose of the paper proposed by Bharati M Nelligani is to make practical and effective usage of embedded systems and advanced technologies to design a smart ATM security system. In this paper, an IR sensor is used to realize the appearance of the card owner and face to identify and verify the legal customer. A variety of sensors and cameras are used to capture security-related information which is further analyzed and dispatched to the central main server to experiment. Utilizing this information obtained from different ATMs, a statistical vulnerability test will be done by the system, and vulnerability software is assigned to all ATMs. The proposed scheme focuses on saving time and solving a very sensitive issue of the system. If the users want to know their balance, then also they need to go through the verification system. This model proves that fraudsters will never gain any advantages from the system. Hence, the security will never be compromised. Increase the safety of electronic money transfer via EDC an embedded fingerprint technique with PIN has been introduced. It's a design to secure swipe card transactions by applying bio-metric features like facial identification with traditional PIN. There

are a variety of methods to raise the safety of the transaction using a bio-metric recognition system. In this given model PIN is completely replaced with a biometric system such as facial, e-fingerprint, retina, and so on

3. PROBLEM STATEMENT:

In the existing system, we use a debit or ATM card at an ATM Machine or POS machine, Customers can withdraw cash from accounts, make a deposit or transfer money from one account to another or perform any other functions which are not highly secured

4. PROPOSED METHOD:

In this proposed system, not only the valid cardholder is allowed only by the knowledge of the account holder anyone can enter the ATM by using the account holder's ATM card. If any unauthorized person is inserted ATM card, their picture with one OTP will be sent to account holders mail, only after entering that OTP in the system it will allow the user to withdraw the money.

5. ADVANTAGES:

1. It is very secure compared to credit or debit card payments.
2. Very fast transactions would take place in less than a second.
3. We can transact at most of the places just with Face

6. METHODOLOGY:

In our proposed system, once the consumer inserts the card into an ATM, the card reader reads the information stored on the magnetic stripe of the card and then passes it to the host processor for confirmation. The host processor communicates with the bank database to get detailed account information. If everything is okay, then the customer is asked to press a 4-digit PIN which is then compared with the PIN encrypted into the magnetic stripe on the card. Here, authentication is done by verifying both personal identification numbers (PINs) and matching the face. If PIN verification is okay, then the customer's facial image is scanned at the ATM terminal and verified using Haarcascade Algorithm features which are the best face recognition algorithm. After that, EFT (electronic fund transfer) occurs from the customer's account to the processor's account, and a code of approval is sent to the ATM to withdraw cash. Each useful information must be provided to affect the transaction. If a face doesn't match the first time, the customer will get two more chances to match the face. But if the face is invalid consecutive three times, then to make sure whether the customer is valid or not, the system will ask him/her for date-of-birth and phone number. If the information is okay means the customer is legal, but if the information is wrong then the system will understand that an illegal user is trying to access the account. Therefore, it'll block the card. After blocking the card, the system will automatically inform the customer about the corruption along with details such as device number, So, the customer will be able to take the necessary steps.

7. ALGORITHM:

Step-1: Start

Step-2:user Stands Infront of a Machine

Step-3: reads the Face Data of the user

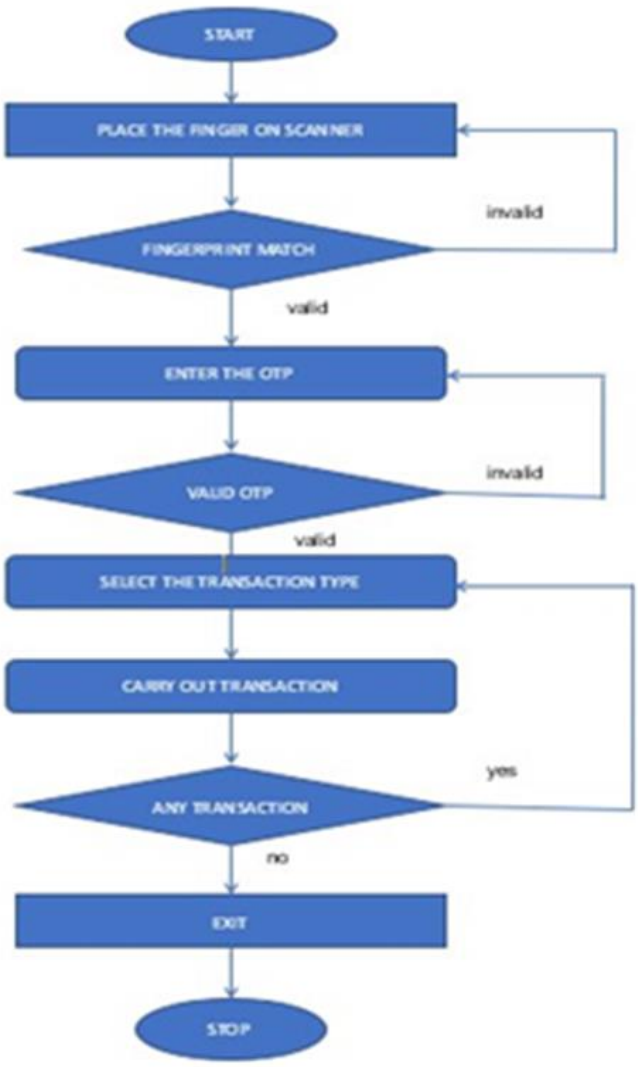
Step-4: if the face matches with the bank database it continues with transaction type

Step-5: else it rejects the transaction

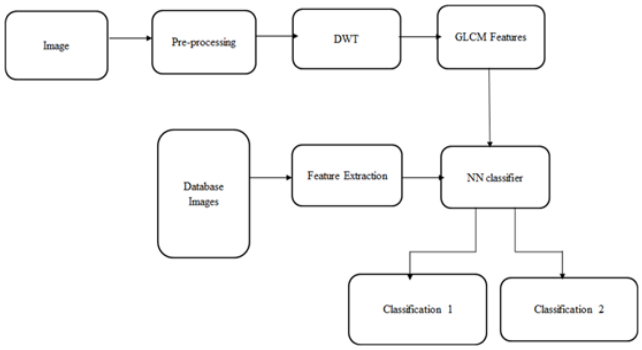
Step-6: continues with the transaction or rejection

Step-7: Stop

8. FLOWCHART:



9. BLOCK DIAGRAM:



10. BLOCK DIAGRAM CLASSIFICATION:

Web camera is connected to the raspberry pi to capture the image, if some person enters the ATM, cameras get triggered and capture the image of that person, to compare with the database.

11. PROJECT DESCRIPTION:

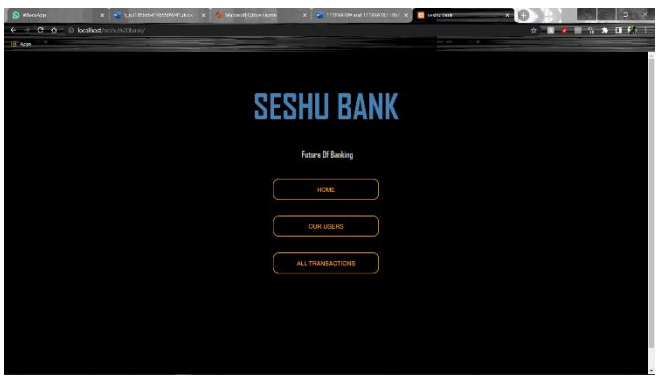
This project consists of a raspberry pi module and a camera to scan the facial data of the customer in Infront of the ATM.

12. WORKING:

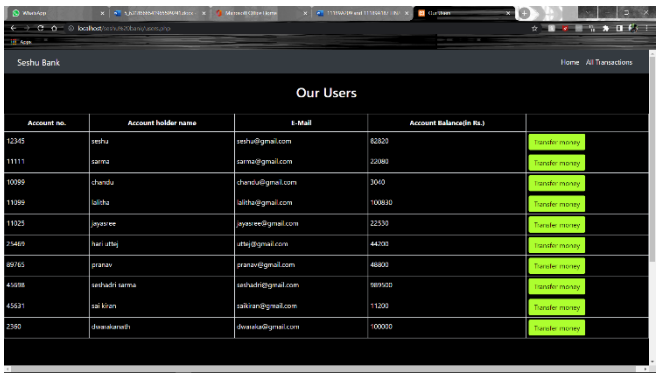
1. When a customer places a card on any pos/ATM or at any merchant
2. It will scan the face details and decodes the data entered by the bank
3. Now it will search the decoded data in the particular bank's database.
4. If the details of the face and details in the bank database are matched
5. Then it will debit the certain amount entered by the merchant
6. And the transaction will show successful
7. If there is a mismatch in details, It will be a failed transaction and This process will just complete in seconds.

13. OUTPUTS:

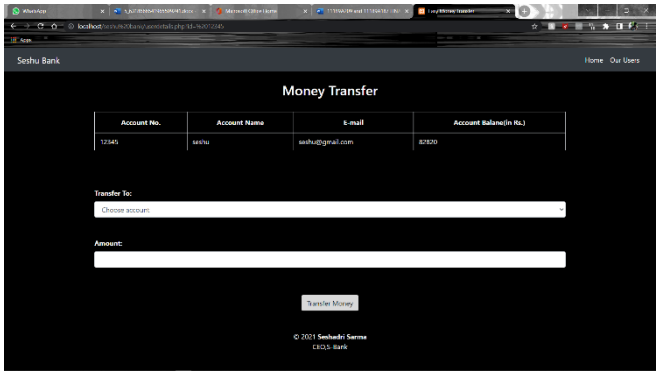
HOMEPAGE:



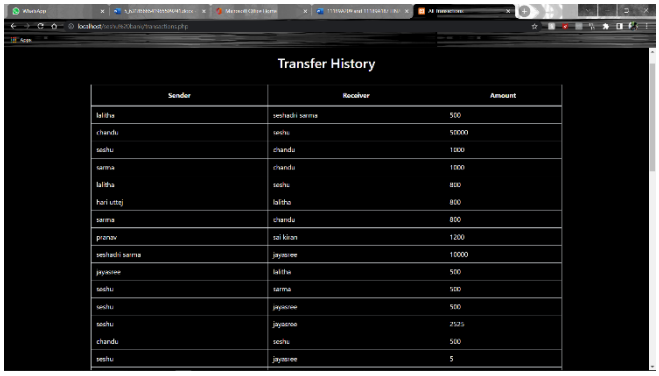
OUR USERS:



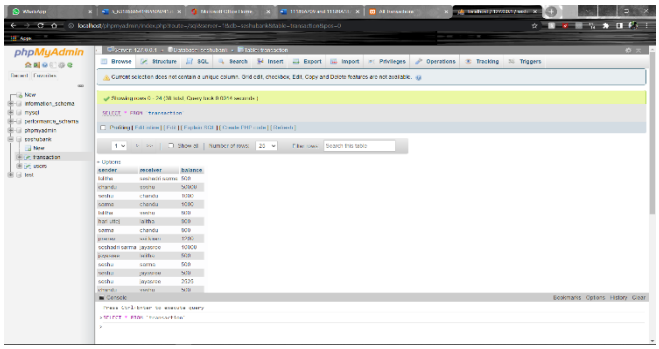
TRANSACTION PAGE:

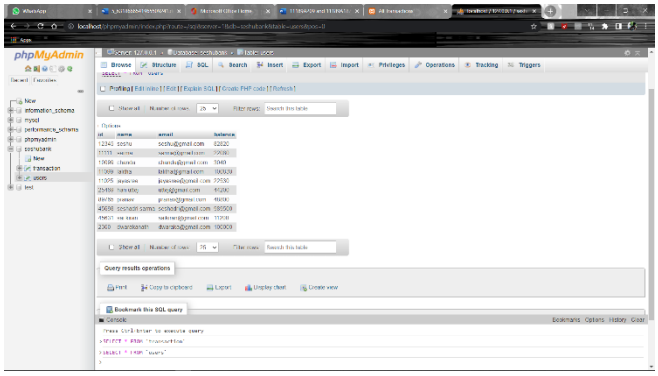


TRANSACTION HISTORY:

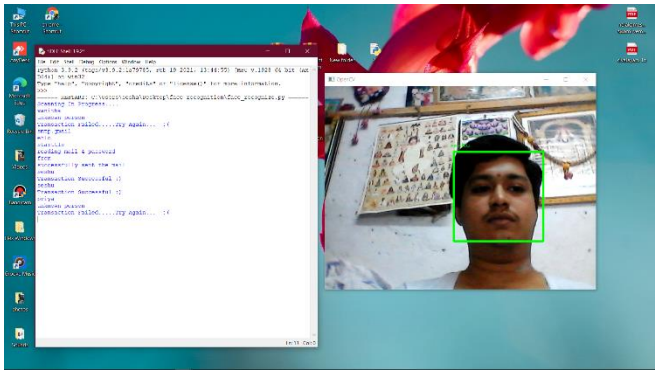


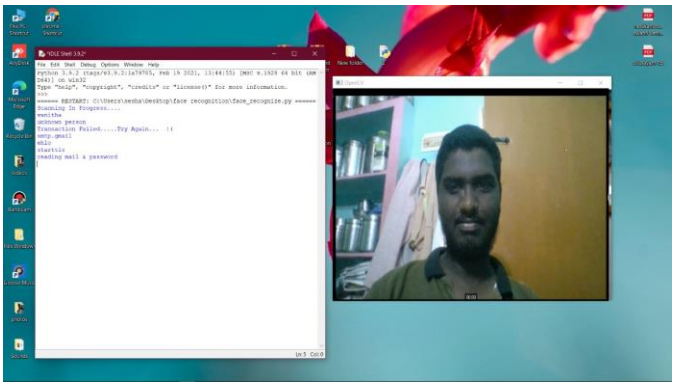
DATABASE:



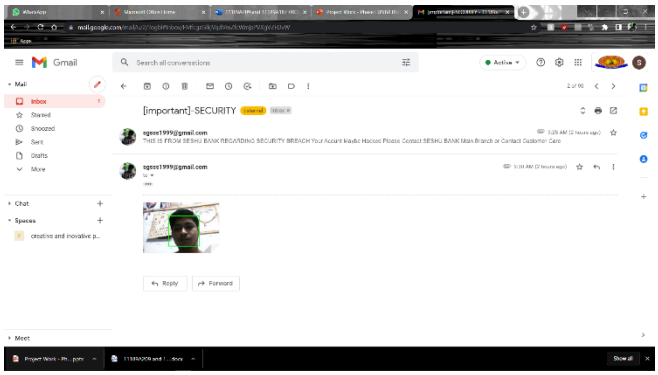


FACE RECOGNITION:





MAIL IMAGE:



14. CONCLUSION:

The growing result of electronic transactions increases the demand for making more secure and reliable transaction systems. Yet money theft, identity theft is becoming a threat in the banking system. So, it's very important to determine the authentic user properly to safeguard against all kinds of technical attacks and intrusions. By combining biometric and mail authentication technology along with the existing systems our proposed model can produce a very effective and well-protected methodology to increase both ATM and swiping machine security. But it can't predict the breach in security before the occurrences which are also very important. We plan to build a real-time monitoring system along with an enhanced security system based on more bio-metric features like iris patterns, retina scan, signature biometrics, etc., and an efficient message authentication algorithm.

REFERENCES

1. Onyesolu MO, and Ezeani IM, "ATM Security Using Fingerprint Bio-metric Identifier: An Investigative Study," International Journal of Advanced Computer Science and Applications, 2012, Vol. 3, no.4, pp. 68–72.

2. Daniel Peralta, Mikel Galar, Isaac Triguero, Oscar Miguel-Hurtado, Jose M. Benitez, and Francisco Herrera, "Minutiae filtering to improve both efficacy and efficiency of fingerprint matching algorithms," Engineering Applications of Artificial Intelligence, June 2014, Volume 32, Pages 37-53

3. S.P. Balwir, K.R. Katole, R.D. Thakare, N.S. Panchbudhe, and P.K. Balwir, "Secured ATM Transaction System Using Micro-Controller", International Journal of Advanced Research in Computer Science and Software Engineering, April 2014, vol. 4, no. 4, pp. 1358-1362.

4. Bharati M Nelligani, Dr. N V Uma Reddy, and Mr.NithinAwasti, "Smart ATM Security System Using FPR, GSM, GPS", International Conference on Inventive Computation Technologies (ICICT), 26-27 Aug. 2016.