International Journal of Innovative Research in Advanced Engineering (IJIRAE) ISSN: 2349-2163
Issue 07, Volume 8 (July 2021) https://www.ijirae.com/archives

FINGERPRINT AND FACE RECOGNITION BASED ATM SYSTEM USING RASPBERRY PI

Kavyashree S*
PG Student, Dept of ECE, JSS Science and Technology University
Karnataka, India
kavyakavyasuresh@gmail.com
Supreetha M
Dept of ECE, JSS Science and Technology University
Karnataka, India
supreetha.manjanna@sjce.ac.in

Publication History
Manuscript Reference No: **IJIRAE/RS/Vol.08/Issue07/JLAE10087**
Research Article | Open Access
Peer-review: Double-blind Peer-reviewed
Article ID: IJIRAE/RS/Vol.08/Issue07/JLAE10087
Received: 20, July 2021
Accepted: 23, July 2021
Published Online: 30, July 2021
Volume 2021 | Article ID JLAE10087 | https://doi.org/10.26562/ijirae.2021.v0807.008
Kavyashree &Supreetha (2021). FINGERPRINT AND FACE RECOGNITION BASED ATM SYSTEM USING RASPBERRY PI.IJIRAE::International Journal of Innovative Research in Advanced Engineering, Volume VIII, 190-198.
doi: https://doi.org/10.26562/ijirae.2021.v0807.008
Editor-Chief: Dr.A.Arul Lawrence Selvakumar, Chief Editor, IJIRAE, AM Publications, India
Copyright**:** ©2021 This is an open access article distributed under the terms of the Creative Commons Attribution License; Which Permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited

Abstract: ATMs (Automatic Teller Machine) are becoming widely used in today's world because they are easy to use and offer convenience. However, today's ATM technology comes with some security risks such as the theft and misuse of cards, the possibility of losing a card, and forgetting PIN numbers. A growing number of frauds committed against automatic teller machines over the last decade motivated us to use biometrics to ensure the accuracy and security of personal identification. In this paper, we describe a biometric fingerprint and face recognition system that can replace ATM cards and PINs. The transaction is successful when fingerprint, OTP, and face match. If the fingerprint does not match, the customer is guided to enter the aadhaar number. Similarly, if face matching fails, the customer is given an option to answer the question. Here aadhaar number and correct answer to the question must be entered correctly to proceed. Aadhaar number entry and question & answer options are mainly provided for those who are unable to access the system because of damage to their physical attributes (finger and face).
Keywords: based; recognition; fingerprint; face; atm; aadhaar

I. INTRODUCTION

Systematic identification of people using their biometric characteristics is known as biometrics. The unique biometric traits used for identification can be an iris, fingerprint, handwriting, face or voice. A biometric identification system is rapidly gaining popularity due to its higher security level in comparison to traditional identification systems. It is considered reliable and accurate to use biometric systems. Using biometric techniques, similarity can be measured between the user's physical attributes and the recorded biometric traits.

Through 24x7 self-banking, the ATM has become a banking hub. Due to the excess use of ATMs, their numbers have increased as well as more fraudulent attacks were launched against them. In order to overcome this, it is necessary to integrate biometrics in ATM systems. The fingerprint and face recognition technologies find application in many different fields such as bank locker security, human-computer interaction, military base station security, criminal identification and cybersecurity among others. These features prevent unauthorized access to the user's account through filched or counterfeit cards. It is not sufficient to have a card to access the account since the person is also required to proceed with the transaction. As a part of the system presented here, two biometrics (fingerprint and face) are used as fraud detection tools to identify multiple types of illicit ATM attempts. A biometric recognition framework is used in the proposed system to make ATM transactions more secure. For smart ATM access, we are using a raspberry pi microcontroller. The transaction process starts with the capture and matching of a fingerprint and then the user enters a four-digit security code (OTP) sent to their mobile number through twilio.

Upon entering a valid OTP (One Time Password), the system proceeds to identifying the user's face. The customer can withdraw the cash after their face ID matches the database image. In case the account holder's fingerprint or face get injured due to some accident and can no longer recognized by the system, the aadhaar number and question and answer choice is provided to access the system.

II. LITERATURE SURVEY

One time passwords and face recognition are used to increase the security of accounts and protect user privacy. With the technology used for face recognition, each face serves as a code for facilitating machine identification. It eradicates the possibility of fraud due to theft and duplication of ATM cards. Furthermore, the OTP which is generated randomly, eliminates the need for the user to memorize PINs, as it acts as it's own PIN [1].

In today's world most of the bank customers desire to use ATMs for their money transactions due to it's ease of use nature. But there is a security risk in today's ATM technology like theft and misuse of cards, chance of losing a card and forgetting PIN number. So to reduce all these problems, authors in paper [2] proposed a new generation ATM system which is based on facial recognition and here they have replaced ATM cards with RFID tags. An embedded ATM camera has been used for face detection in this system by using a new computer vision framework. If an illicit person is detected, the corresponding user will get an alert message.

In [3] authors developed an embedded system used for ATM security. ATM crimes have increased significantly over the last few years. ATMs use PIN numbers to identify individuals and these PIN numbers are strictly confidential. Yet hackers are highly likely to hack PIN numbers, personal information, and much more. In order to diminish these problems, a system has been created in which input was provided to the microcontroller by a RFID card, and a GSM module transmitted messages including three replies (yes, no, action) to the legal client's mobile phone. If the user responded as 'YES', then transaction will be successful. If the response is 'NO', then transaction will terminate and if the response is 'ACTION', then the card will be blocked. In paper [4] an ATM system that incorporated both fingerprint authentication and GSM authentication to enhance security was proposed. In [5] the ATM transaction was enhanced in security through the usage of the Advanced Encryption Standard algorithm. [6] an ATM system which uses the face to identify the user was described. Here Principal Component Analysis was used for facial recognition and OTP for transaction security.

Modern society relies heavily on ATMs. If the PIN number is forgotten or the card is damaged, it is difficult for user's to retrieve money. This scenario encourages the use of biometric validation rather than using a PIN or ATM card. Here, the Fingerprint and Face ID are preferred to high priority. Identification of user's fingerprint and a verification of his or her face are performed, and authentication is given to the appropriate user. Raspberry pi microcontroller is used for the prototype of the system [7]. In paper [8], blockchain technology is being applied to IOT to improve cash logistics and ATM operations in terms of transaction stability, privacy, security and so on. [9] presents a new generation of multi-level security system for ATMs using Arduino UNO. As ATMs have become easily accessible and easy to use, their usage has increased significantly in recent years.

Although this system reduces human effort and makes their lives easier, it lacks the security that would guarantee their safety. So in this paper, a new level security system has been proposed which uses face recognition concept to detect the unauthorized user.

III. PROPOSED SYSTEM

A. Hardware Design

In this proposed system we have proposed a new concept through face recognition and finger print to strengthen the security of the conventional ATM model. A block diagram of a proposed ATM security system based on fingerprinting and face recognition is presented in Fig.1. In this system, finger print and face image of the individual are used for validation purpose. When a person is enrolled in the program, the fingerprint module captures their fingerprint and compares it to that of an authorized user. As soon as the fingerprint is matched, an account holder receives a code via text message, which is sent by Twilio account interfaced to the Raspberry pi. After the OTP is entered correctly, person's face image is compared to database image. When both the recognition schemes match with a same single individual, access for that account will be provided. And also the entry of aadhar number and question answer possibility is given to user, in case the user's finger or face are damaged and couldn't access the system.

In this case, Raspberry Pi microcontroller controls the process. The Fingerprint scanner Id and face Id are searched in a database where the other details of the user account will be stored. The raspberry pi microcontroller performs the search operation in the database and sends the necessary information to a display device. Python face-recognition module and Open CV libraries are used for the process of recognition, verification and identification of face images. The fingerprint libraries are used for the above-mentioned process for fingerprints. The program for the process is coded in python.

IJIRAE:: ©2014-21, AM Publications, India - All Rights Reserved

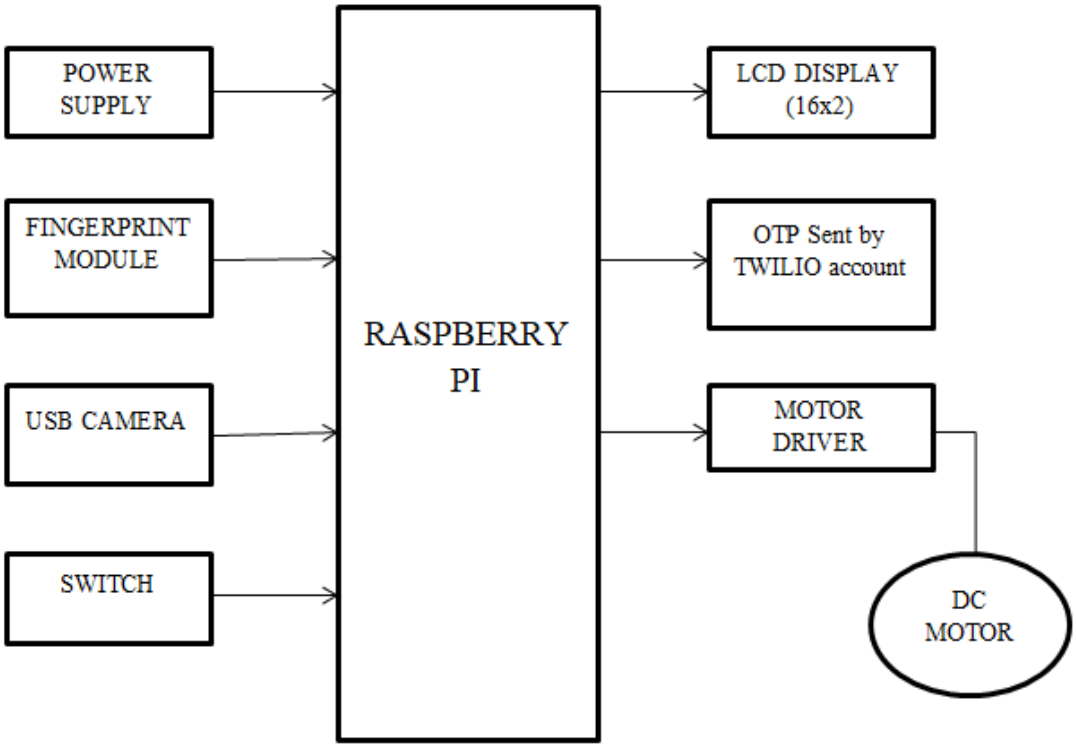

Fig.1. Block representation of Proposed system

1) Raspberry Pi

It is an ATM-card-size single-board computer, which is of low cost. Because of its modularity and open design, it finds widespread use across a number of fields including weather monitoring, security systems, and tracking systems. Its adoption of HDMI and USB devices makes it a common choice for computer and electronic hobbyists.

2) USB Camera

A USB webcam is a device which is used to take videos and pictures connected to microcontroller through USB port. It has very high flexibility and low manufacturing cost. These USB cameras offer very good resolution in spite of low cost. In this project USB camera is used to identify an authorized user.

3) Fingerprint Module

It is a sensor used to identify authorized person. It is mainly used for security purpose. A wide variety of devices, such as mobile phones, access control systems, computers, electronic locks and security safes utilize it. This module includes a large number of commands for doing tasks such as enrolling, verifying, and identifying fingerprints, reading and writing fingerprint template files and retrieving fingerprint images among others.

In this project, fingerprint module plays a major role. Although face recognition is part of this proposed system, the fingerprint has a much greater impact. Imagine a scenario with twins, leaving the image collapsed because of the same face. In such cases, fingerprints assist in identifying the account.

B. Software Design

1) Raspbian OS

The Raspberry Pi Foundation developed Raspbian OS as an operating system for the raspberry pi. It is designed especially for the raspberry pi models and it delivers excellent performance and stability.

2) Image Processing

To improve the quality of an image or to extract required information from it, digital image processing can be used. Image processing is applied in the fields of medical, color processing, video processing, transmission and encoding, remote sensing and so on. By using this, the algorithm can be applied to a much wider range of input data types, which gets rid of problems created during processing, such as noise and signal distortion.

3) Python

In this project, we have written a program code in python language which is a high level, interpreted and general purpose programming language. It's language design greatly enhances readability and control statements syntax making programming and development much easier. The dynamic nature of the program enables it to support automated memory management, which is extremely useful for object-oriented programming in real-time.

IJIRAE:: ©2014-21, AM Publications, India - All Rights Reserved

4) Twilio

Twilio messaging is an Application Program Interface, which permits software developers to perform many communication tasks through it's web service APIs, such as making phone calls, sending texts, and receiving voicemail messages. In this project, we are using twilio messaging to send OTP to the authorized user.

IV. IMPLEMENTATION

Currently, ATMs are accessible and convenient for most customers. At present, ATMs display instructions on the screen which a user reads to interact with the ATM. Once the user has read the LCD instructions, he or she can operate the ATM using the keypad. Despite this, the existing system has a number of disadvantages such as requiring a user to carry the ATM all the time and also having many security risks. Therefore, we developed a system that enables us to use ATM machines without ATM cards but with more security.
The flowchart in Fig. 2. illustrates how the methodology is implemented.

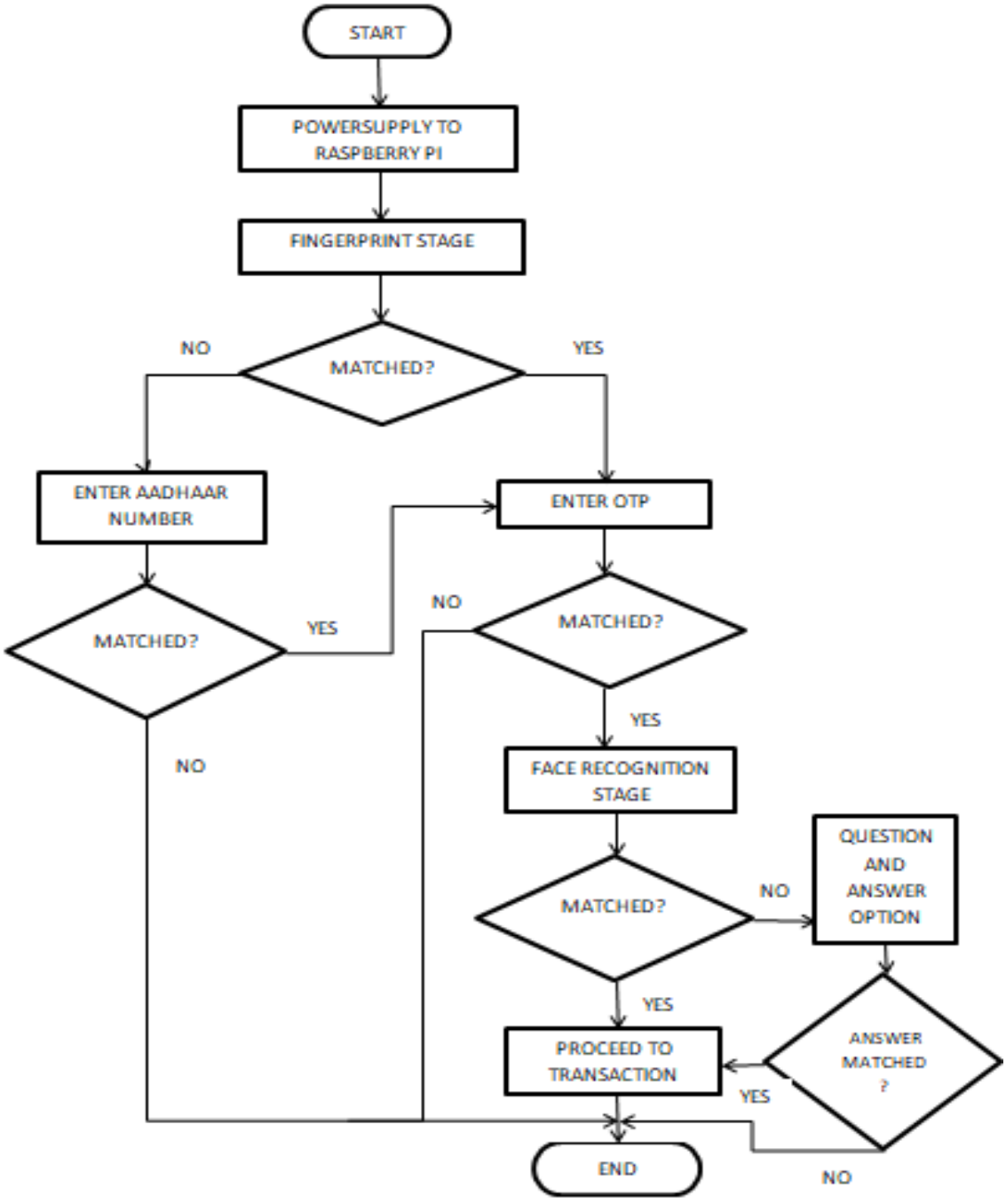

Fig.2. Flowchart of proposed system

In this approach, the raspberry pi microcontroller serves as the controlling module and it is the brain of the device.

Step1: Initially we store the fingerprint and image of the account holder in database.

Step2: The transaction process begins with capturing and matching fingerprints. When the controller detects a genuine user, it will display the message "FINGER MATCHED" on the LCD.

Step 3: Subsequently the fingerprint is matched, an account holder receives a 4 digit OTP via text message which is done through Twilio account interfaced to the Raspberry pi. If the OTP has been entered correctly, the LCD will display a message such as "OTP MATCHED", if not the current process will get terminated.

Step 4: After the OTP is matched, image of the user is captured with the USB camera. When the face recognition match with a same individual in the database the transaction process will begin, if not the system control goes to question and answer option block. Once the correct answer is given to respective question the user can withdraw money.

Step5: If the fingerprint is not matched in step 2, the system asks for aadhaar number. After the correct aadhaar number is entered the flow continues from step 3(Enter OTP), if not the current process will terminate.

Incase the user's finger or face are damaged due to some accident or age issues and couldn't access the system, the idea of aadhar number and question answer possibility given to user is very helpful.

V. RESULTS AND DISCUSSIONS

The proposed system is composed of raspberry pi 3 model, fingerprint module, USB camera, LCD display, motor driver, DC motor and switches. Fig. 3., shows the project model.

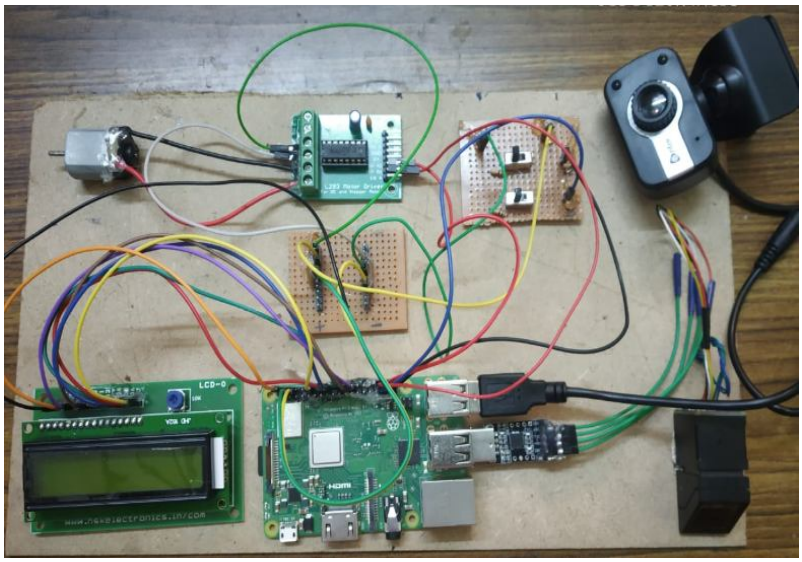

Fig.3. Project Model

In this project we are considering three cases.

Case 1: When both fingerprint and face matched.

The process of transaction starts with taking fingerprint of an individual and matching that with the data stored in database. If the fingerprint matched, the LCD will display a message such as "FINGER MATCHED" as shown in Fig. 4.

Fig. 4: Message displayed on LCD when fingerprint matched

After the fingerprint is matched, the controller will decide that he/she is an authorized user and four digit security code (OTP) is sent to their mobile number through twilio account interfaced to the Raspberry Pi as shown in Fig. 5.

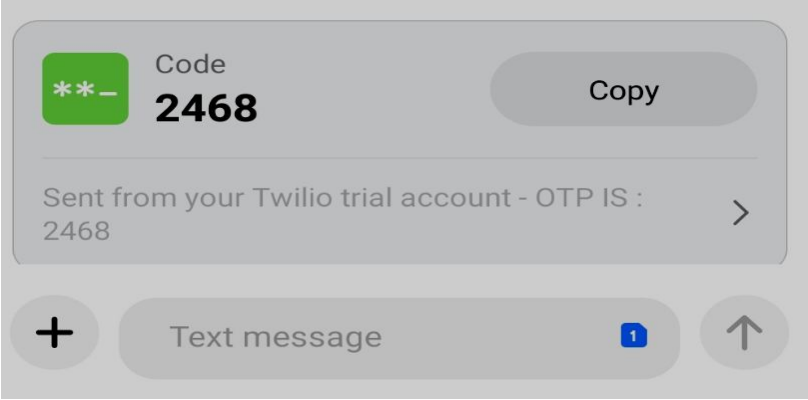

Fig. 5: OTP sent by twilio account

If the OTP has been entered correctly, a message will display on the LCD such as “OTP MATCHED” as shown in Fig. 6. If the OTP entered is not valid, current process will get terminated and goes back to initial (fingerprint) stage as shown in Fig.7.

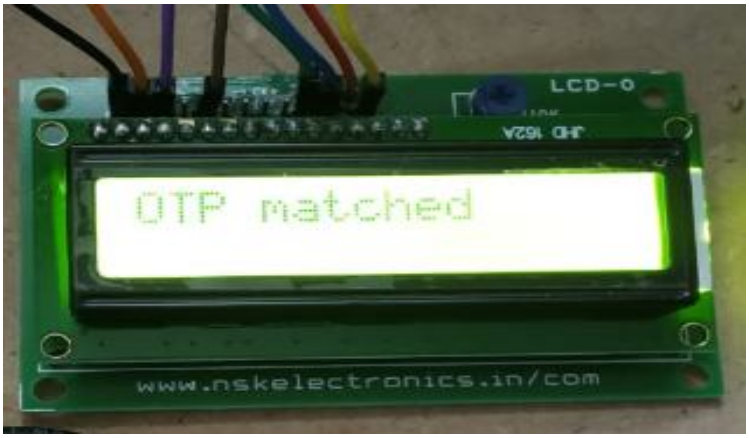

Fig. 6: Message displayed on LCD when valid OTP has entered

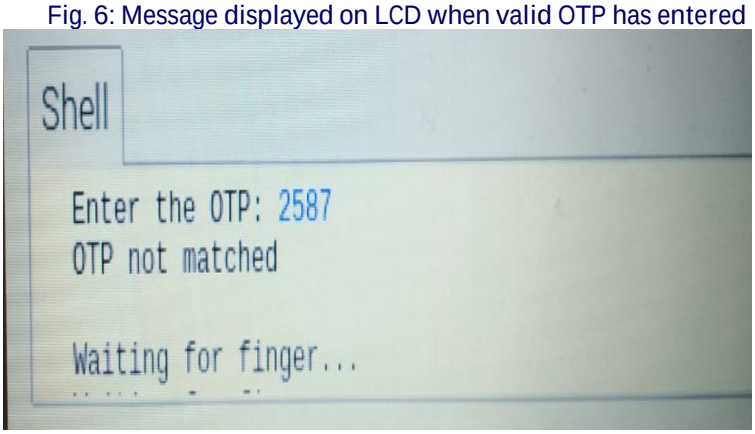

Fig.7. OTP not matched

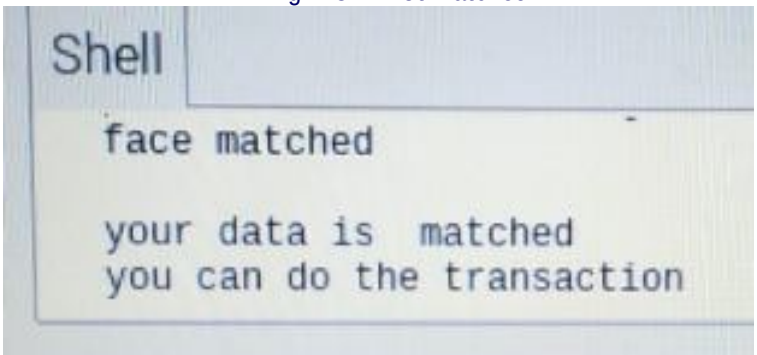

Fig. 8: Face matched

Once the OTP is matched, the control flow goes to face recognition part. Here, person's face image is compared to database image. If the face is matched then the transaction is successful as shown in Fig. 8.

Case 2: When face is not matched.

After the OTP is matched, if the face recognized does not match with the image stored in database, a question and answer choice is given to user as shown in Fig. 9. Once the correct answer is given to respective question the user can withdraw money. This facility is very useful to those whose face is damaged due to any accident and system couldn't recognize him/her.

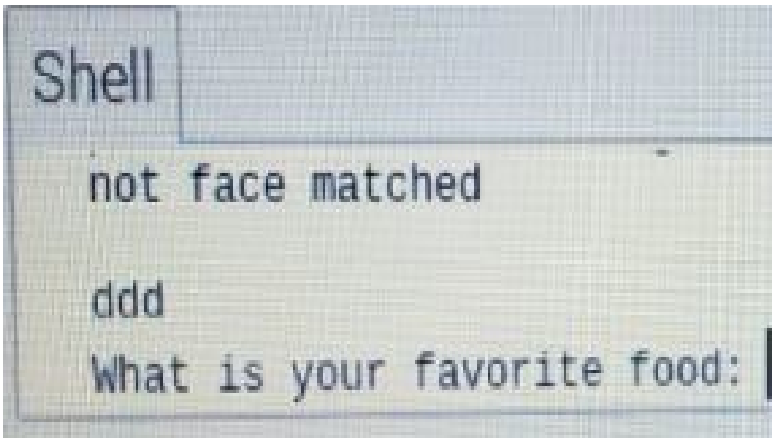

Fig.9. Face not matched

Case 3: When fingerprint is not matched

The process starts with fingerprint matching, if the fingerprint does not matched, the system asks to enter an aadhaar number as shown in Fig. 10. If the person enters the correct number the system flow goes to OTP part and it continues with the face recognition part. If the aadhaar number not matched, the current transaction will get terminated and goes back to initial (fingerprint) stage as shown in Fig.11.

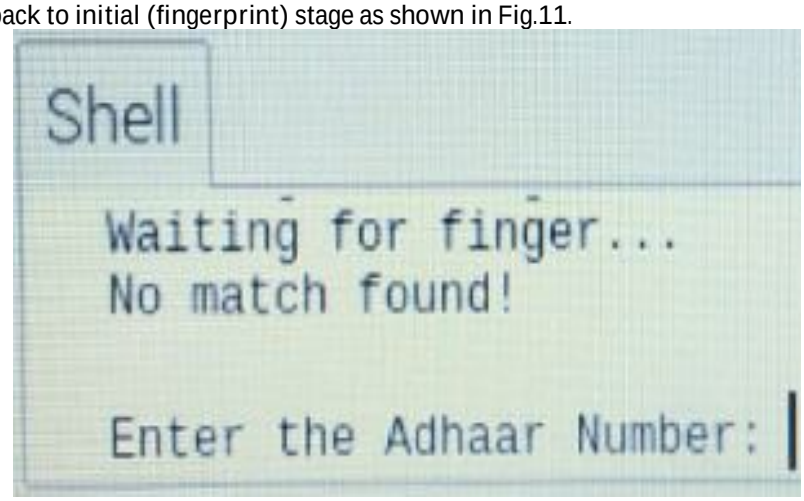

Fig. 10: Fingerprint not matched

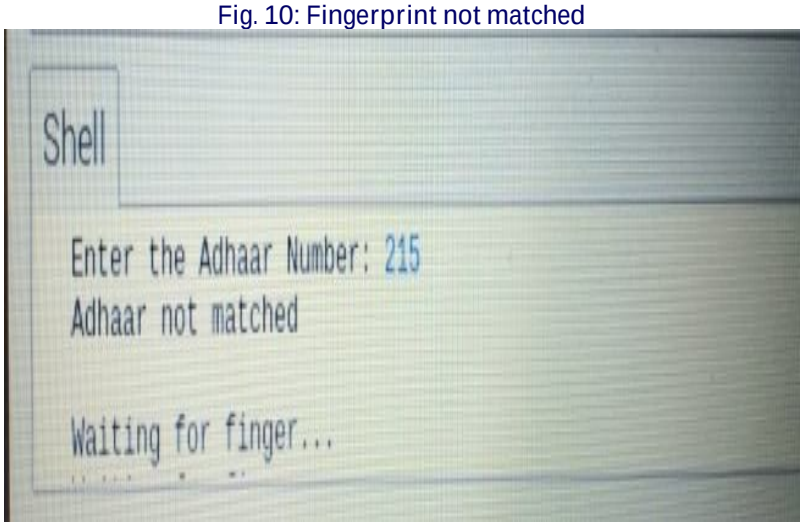

Fig. 11. Aadhaar number not matched

VI. CONCLUSIONS

Using biometric data as a PIN has enhanced the trustworthiness and security of ATM transactions. Incorporating OTP into the system increases security and eliminates the need to memorize PINs. Furthermore, the concept of entering aadhaar number and answering a question, when the physical characteristics of the user are damaged and they are not able to log on to the system is extremely helpful. The system is embedded with embedded technology, which ensures that it is non-invasive and user-friendly. This model can be used in bank lockers security, criminal identification, security systems in R&D labs, military base station security and so on. In future, compare to other forms of biometric identification facial recognition may be more difficult, so it will be possible to develop a more accurate algorithm. Optimally we can replace facial recognition with iris or retinal recognition if it is less expensive.

REFERENCES

1. Anil K. Jain and Arun Ross. Introduction to Biometrics. In Anil K. Jain, Patrick Flynn, and Arun. A. Ross, editors, Handbook of Biometrics. Springer US, 2008.
2. Dr. S Sasipriya, Dr. P Mayil Vel Kumar, S Shenbagadevi, “Face Recognition Based New Generation ATM System”, European Journal of Molecular and Clinical Medicine, Vol.7, Issue 4, 2020.
3. Mrs.S.P.Balwir,Ms.K.Katole, Mr.R.D.Thakare, Mr.N.S.Panchbudhe ,Mr.P.K.Balwir,"Secured ATM transaction system using microcontroller”, International Journal of Advanced Research in computer science and software engineering, Vol.4,Issue4,April 2014.
4. Khatmode Ranjit P, Kulkarni Ramchandra V,”ARM7 Based Smart ATM Acess and Security System Using Fingerprint Recognition and GSM Technology”, International Journal of Emerging Technology and Advanced Engineering ,Vol.4,Issue 2,Feb. 2014.
5. Fakir Sharif Hossian, Ali Nawaz, Khan Md. Grihan,”Biometric Authentication Scheme for ATM Banking System using AES Processor”, International Journal of Information and Computer Science, Volume 2 Issue 4, May 2013
6. Mohsin Karovaliya,Saifali Karedia,Sharad Oza, Dr.D.R.Kalbande, ”Enhanced Security for ATM machine with OTP and facial recognition features”, International Conference on Advanced Computing Technologies and Applications(ICATA-2015).
7. Dr.G. Ranjitham, Senthamilarasu Manoharan, Vetrivelu Murugesan, Sree Sabaresan Ravi, “Face Recognition and Fingerprint Based New Generation ATM”, International Journal of Innovative Science and Research Technology, Volume 3, Issue 3, March – 2018
8. L. Denis, T. Krishnakumar, M. Karthikeyan, S. Sasipriya, “IOT based architecture for banking cash logistics and ATM operations with sensors based networks”, International Journal of Scientific and Technology Research, 9(2), pp. 2071-2076, Jan. 2020.
9. S.K. Sangeetha, K Ganaga Gayathi, S Gowtham and Bhuvaneshwaran , “New generation multilevel based ATM security system”, in IRJET, vol.7, Issue 4, April 2020

IJIRAE:: ©2014-21, AM Publications, India - All Rights Reserved