



e-ISSN: 2319-8753 | p-ISSN: 2347-6710

IJIRSET

International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 11, Issue 6, June 2022

ISSN INTERNATIONAL
STANDARD
SERIAL
NUMBER
INDIA

Impact Factor: 8.118



9940 572 462



6381 907 438



ijirset@gmail.com



www.ijirset.com

Banking System Transaction with Hybrid Biometric Verification

Shraddha Madhukar Pawar, Prof. Devray R.N

Department of Computer, Vishwabharti Academy's College of engineering, Ahmednagar, India

ABSTRACT: In this modern world, almost everyone uses online platform which allow people to transfer and withdraw cash. This transaction if carried out through biometric authentication of every individual proves to be more secure. Biometric authentication refers to the automatic identification of a person by analyzing their physiological and/or behavioral characteristics or traits. Since many physiological and behavioral characteristics are unique to an individual, biometrics provides a more reliable system of authentication than ID cards, keys, passwords, or other traditional systems. A wide variety of organizations are using automated person authentication systems to improve customer satisfaction, operating efficiency as well as to secure critical resources. Now a day an increasing number of countries including India have decided to adopt biometric systems for national security and identity theft prevention, which makes biometrics an important component in security-related applications such as: logical and physical access control, forensic investigation, IT security, identity fraud protection, and terrorist prevention or detection. Various biometric authentication techniques are available for identifying an individual by measuring fingerprint, hand, face, signature, voice or a combination of these traits. New biometric algorithms and technologies are proposed, tested, reviewed, and implemented every year. The system aims to provide biometric authentication of fingerprint and face recognition for secure transaction for monetary in banks. Fingerprint authentication uses IoT technology for processing while face is scanned with deep learning for security and privacy towards transaction.

KEYWORDS: Face Recognition, Fingerprint, CNN, Banking, Biometric (Keywords)

I. INTRODUCTION

In financial sector, traditional method for transaction was authentication by signature of person. With advance of technology the card-and-PIN system are in use for any transactions, which works well, the cards also serve functions beyond the ATMs, as debit cards and as advertising for the banks. However, companies that make automated teller machines have found budding markets for the fingerprint technology where citizens already are accustomed to the use of fingerprints for general identification, such as ID cards they carry. Biometrics is certainly the most secure form of authentication. It's the hardest to imitate and duplicate. Thus, Biometric can be made best choice for identification and authentication of transaction. In modern days, everyone used to do banking like storing cash and withdrawing cash. The clients will be in line to extract cash from the bank. Traditional method for transaction was authentication by signature of person. The system is prone to fraud as signature of person can be impersonated to make the transaction in Banks. With advance of technology the card-and-PIN system are in use for any transactions, which works well, But carrying card everywhere and losing it becomes more dangerous. Such as may be theft, misplaced, duplicated, or forgotten; passwords may get distributed, unremembered, hacked or seen by some third party. Banks needed a good mechanism to manage protection for the clients to make the transaction in the banks. The system aims to provide biometric authentication of fingerprint and face recognition for secure transaction for monetary in banks. Fingerprint authentication uses IoT technology for processing while face is scanned with deep learning for security and privacy towards transaction. Paper is organized as follows. Section II describes about the related work done earlier for the system to be developed. Section III presents method used and algorithms used for the detection. Section IV presents experimental results showing results of images tested. Finally, Section V presents conclusion.

II. RELATED WORK

1. *Sharma, Risabh. "ATM Management System." (2021)*

In this paper, Decision-makers need to value a guaranteed level of security through biometric systems and the potential

for change which ensure that voters' thumbs during registration and voting days are properly placed on a fingerprint scanner, to Test verification should be done to verify the file[1].

2. *Kadam, Pankaj Anil, PradnyaPramodPatil, and SupriyaYogeshNaik. "Enhanced ATM Security based on Machine Vision."(2021)*

In this paper, The implementation of ATM security by using fingerprint also contains the primary verifying methods, which were inputting customer fingerprint, which is send by the controller and verified properly. The security Features were enhanced largely for the steadiness and reliability of owner recognition. The whole system was built on the fingerprint technology, which makes the system safer, reliable and easy to use. This will be most trusted and secure technology at electronic money transaction.[2].

3. *Aldakheel, Eman Abdullah, and Mohammed Zakariah. "MOBILE DEVICES AND CYBERSECURITY ISSUES AUTHENTICATION TECHNIQUES WITH MACHINE LEARNING." (2021)*

Cybersecurity is the most important and hot research topic, especially at this time. As people are getting more dependent

on digital systems and critical and sensitive information's are stored on these digital devices. There is an advantage of using these devices and gadgets. Still, at the same time, there is a risk of getting attacks on these sensitive files, be it money or essential transaction information for business dealings like customer information for a business. In this study, various security threats have been discussed, mainly for mobile devices. First, the harmful effects of using mobile phones concerning the attacks on these devices have been discussed. After that, authentication techniques are discussed, which show the various methods being applied to safeguard the mobile devices from intruders for malware attacks[3].

4. *IYAW, OG, EI IHAMA, and PCI IGBINIGIE. "THE NEED FOR A BIOMETRIC SYSTEM FOR CLASSROOM ATTENDANCE."(2021)*

In this paper we employ a computerized facial recognition attendance monitoring technique which will enable the

department to properly ascertain the academic strength of each student in terms of student regularity to classroom lectures and commitment to classroom learning, and generate reliable student attendance report stored in a secured database. The software was developed using Visual Basic.Net which connects the text field to database and MySQL was used for the database design.[4].

5. *Tait, Bobby L. "Aspects of Biometric Security in Internet of Things Devices." 2021.*

This paper provides detailed insight into the general mechanisms utilized for biometric application in Internet of things

devices. The mechanisms and internal working of these biometric technologies presented in this paper are focused specifically on the applicability in IOT devices. IOT devices incorporates various scanners and sensors to allow the IOT device to biometrically interact with a human being. These scanners and sensors were primary designed to facilitate and ease user interaction with the IOT device in an effort to make the day to day usability of the IOT device faster and easier if you may. It must be noted that every biometric technology has certain strengths, but indeed, also certain noteworthy shortcomings. It is often these shortcomings that get exploited in a security subversion attempt. This chapter introduces and discusses the various biometric technologies used in IOT devices. Attention is given to the software and the hardware aspects of each biometric system. The generic working of these biometric technologies is presented. Attention is given to legacy biometric technology implemented on IOT devices, currently used biometric technology implemented on IOT devices, and finally, possible future biometric applications of biometric technology destined for IOT devices. In conclusion practical examples of biometric subversion on IOT devices such as fingerprint, facial and voice biometric subversion and hacking, will be investigated, discussed and evaluated[5].

6. *Multi-scale feature extraction for single face recognition.*

Single sample face recognition has always been a hot but difficult issue in face recognition. The existing methods solve

this issue from selecting robust features or generating virtual samples. By considering selecting robust features and generating virtual samples simultaneously, the paper proposes a multi-scale support vector transformation (MSSVT) based method to generate multiscale virtual samples for single image recognition. The methods to solve problems are divided into two categories. One is to look for and select features that are robust to the number of samples, from the point of view of feature selection, such as PCA and 2DPCA. But when each person has only one face to be trained, the feature information extracted from the feature extraction algorithm will also be very limited, resulting in a bad recognition performance. The other is to generate multiple virtual samples from the point of view of the extended sample, thus reducing the impact of the sample size.[7].

III. PROPOSED METHODOLOGY

The system proposes a hybrid approach to use fingerprint and iris scan for authentication. The system applies fingerprint

scanner with MFS100 hardware device for authentication for fingers. The system uses deep learning technology for scanning face. Secure authentication for monetary transaction in banks is done with same.

A. Modules

- Account Register

- Account is Created in Bank.
- Biometric is Registered.
- Image is captured .
- Fingerprint is Registered. -Request Transaction
- Transaction is Requested.
- Face Detection is detected.

1. Locate one or more faces in the image and mark with a bounding box.

2. Face Alignment. Normalize the face to be consistent with the database, such as geometry and

photometrics.

3. Feature Extraction. Extract features from the face that can be used for the recognition task.

4. Face Recognition. Perform matching of the face against one or more known faces in a prepared

database.

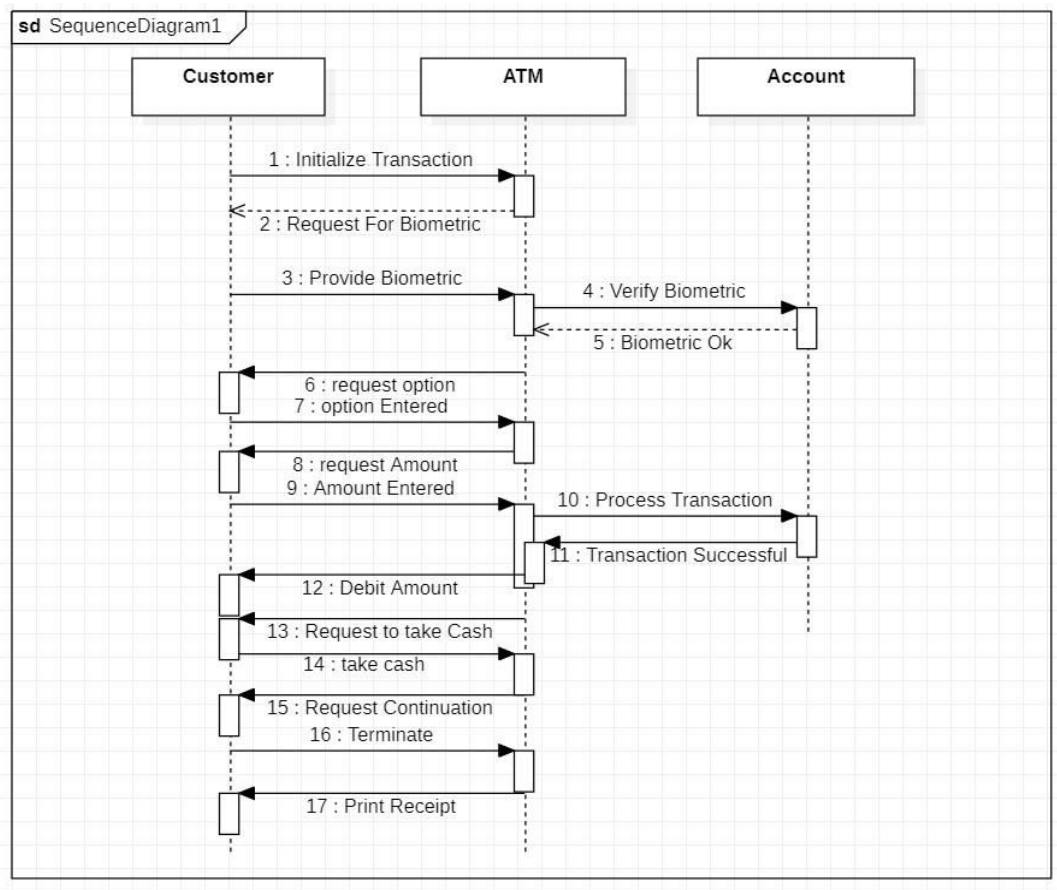
- Fingerprint is detected. -Verify And Authenticate
- Face is Verified and Authenticated.
- Fingerprint is verified authenticated,
- Transaction is Processed

B. System Architecture



. Figure 1 System Architecture

C. Sequence For System:



. Figure 2 Sequence Diagram

IV. RESULTS & DISCUSSIONS

Register Face

ID Face 3

Personal Information

First Name

Last Name

Phone Number

Address

Bank Details

Account No.

Branch

IFSC

Initial Balance

Finish

After registration, capture 25 photos.

00/25

ID Face

Username

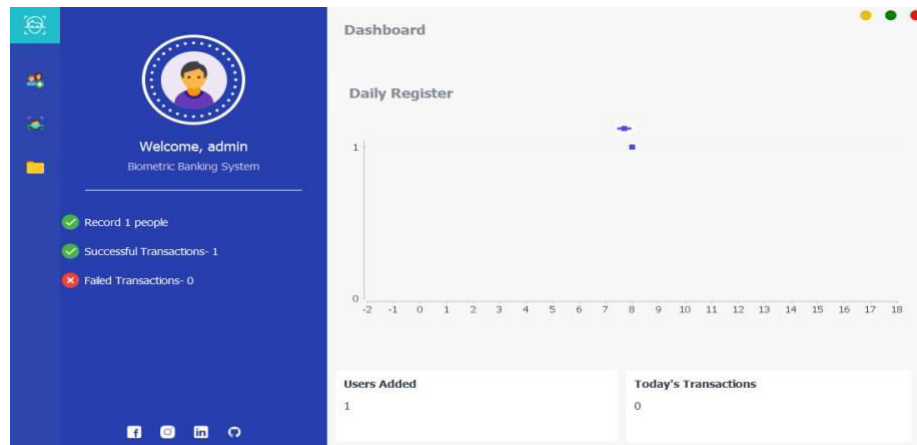
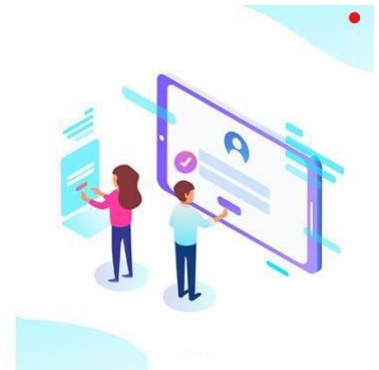
Password

Remember Me

Forgot Password?

Login

Sign Up



Records

ID Face 3

Search here...

	Name	Phone	Address	Account No	Branch
	Dinesh Ubale	(+91)73504...	Pune	123456	Wagholi
	Shubham Pa...	(+91)95039...	Pune	654123	Wagholi

Info

First Name

Last Name

Dinesh

Ubale

Address

Phone

Pune

(+91)7350456969

Account No

Branch

123456

Wagholi


IFSC

Balance

MAHB0001425

1000

Save

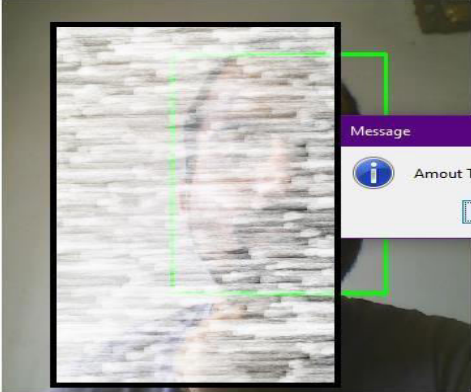

Add Beneficiary

Beneficiary Bank Details

Account No. Branch

IFSC Beneficiary Name:

Recognize Face



Amount: 10...

Personal Information

Fullname: Phone:


Message

Amount Transfer successfully..

Records

ID Face 3

Search here...

	Name	Phone	Address	Account No	B
	Shubham Pa...	(+91)95039...	Pune	654123	W

Info

First Name Last Name

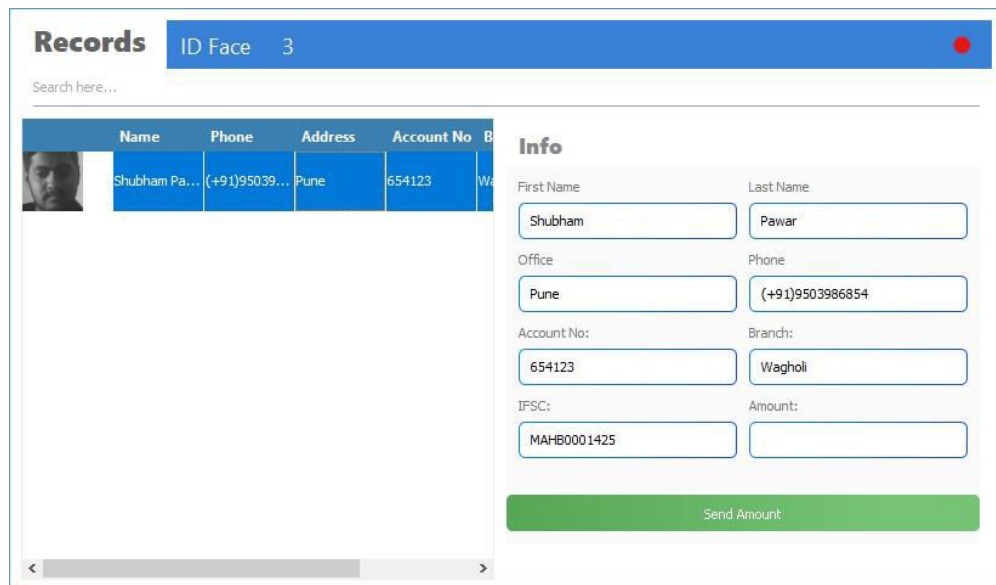
Phone

Branch:

IFSC: Amount:


Message

Biometric Authentication success..



Records ID Face 3

Search here...

Name	Phone	Address	Account No	B
 Shubham Pa...	(+91)95039...	Pune	654123	W

Info

First Name: Last Name:

Office: Phone:

Account No: Branch:

IFSC: Amount:

V. CONCLUSION

The present system for internet banking requires the user to always remember the username and password for all the account that he holds across various branches. If biometric login is used instead, the user does not have to remember the credentials as all the accounts are now being Aadhaar linked. If an unknown person knows the credentials of a user then the wrong use of the account can be done and money can be transferred from the user's account without his/her knowledge. In this system it is never possible as the user needs to give the thumb impression and face recognition while logging. In the system an additional hardware is present i.e. the finger print scanner and camera, which is to be attached to the computer while logging into the system. Moreover the cost of the fingerprint scanner is an additional burden to the user, but if produced in large scale for the users' the cost of the fingerprint scanners' will reduce.

REFERENCES

1. Sharma, Risabh. "ATM Management System." Turkish Journal of Computer and Mathematics Education (TURCOMAT) 12, no. 6 (2021): 5151-5160.
2. Kadam, Pankaj Anil, PradnyaPranodPatil, and SupriyaYogeshNaik. "Enhanced ATM Security based on Machine Vision." 2021
3. Aldakheel, Eman Abdullah, and Mohammed Zakariah. "MOBILE DEVICES AND CYBERSECURITY ISSUES AUTHENTICATION TECHNIQUES WITH MACHINE LEARNING." Journal of Management Information and Decision Sciences 24 (2021): 1-15.
4. IYAW, OG, EI IHAMA, and PCI IGBINIGIE. "THE NEED FOR A BIOMETRIC SYSTEM FOR CLASSROOM ATTENDANCE." (2021)
5. Tait, Bobby L. "Aspects of Biometric Security in Internet of Things Devices." In Digital Forensic Investigation of Internet of Things (IoT) Devices, pp. 169-186. Springer, Cham, 2021.
6. X. Xu, L. Zhang and F. Li, "MSSVT: Multi-scale feature extraction for single face recognition," 2018 24th International Conference on Pattern Recognition (ICPR), Beijing, 2018, pp. 1996-2001, doi: 10.1109/ICPR.2018.8545343



INNO SPACE
SJIF Scientific Journal Impact Factor
Impact Factor: 8.118



ISSN INTERNATIONAL
STANDARD
SERIAL
NUMBER
INDIA



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

 **9940 572 462**  **6381 907 438**  **ijirset@gmail.com**



www.ijirset.com

Scan to save the contact details