Payment Transaction Using Biometric Authentication

Prof. Arati S. Nayak
Department of Information Science and Engineering SDM College of Engineering and Technology Dharwad, India

Isha Shet
Department of Information Science and Engineering SDM College of Engineering and Technology Dharwad, India

Gayatri G. Shetti
Department of Information Science and Engineering SDM College of Engineering and Technology Dharwad, India

Jayganesh Nayak
Department of Information Science and Engineering SDM College of Engineering and Technology Dharwad, India

ABSTRACT

This paper of introduction of biometric authentication has radically transformed payment transactions, enabling application of advanced security, convenience and inclusivity. This article demonstrates the integration of biometrics into the platforms of payment, bringing to light their roles in fighting fraud and simplifying the process of authentication. Employing biometrics such as skin patterns, facial features or iris patterns as a means of authentication provides a reliable identity verification, so as to enhance security against unauthorized access and fraudulent activities. Also, biometric authentication with its smooth and seamless process that minimizes the friction between customers and sellers boosts transactions as well as efficiency at the point-of-sale terminals and online platforms. Furthermore, biometric authentication is uniquely positioned to resolve accessibility issues, thus expanding the digital economy to cover individuals with any type of abilities. This paper emphasizes the transformative power of biometric authentication in transaction payment, which is in turn opening a door for secure, faster, and more inclusive financial services.

Keywords: Biometric POS systems, Biometric payment, Contactless payments, Biometric payment technology.

INTRODUCTION

The environment of the payment system has been changed lately which is brought about by the benefits of technology. Biometric technology is the kind of innovation that has got so much recognition of late. Biometrics, namely, the measurement and analysis of distinct features of physiological and behavioral traits, are gradually becoming a popular option for identification verification since they are secure and convenient to use. In Biometric authentication, fingerprint recognition, facial and iris scans offer a powerful remedy for the problem of fraud and for the purpose of improving the user experience in payment transactions. Originally, customers preferred usual forms of payment which were physical passwords, PINs, and magnetic stripe cards. Nevertheless, these methods are not able to withstand the security breach, and identity theft, financial fraud become common incidents. Trying to overcome the inefficiencies of the traditional authentication process, companies and financial agencies have come up with biometric technology to strengthen their security and tame the transaction process. Biometric authentication uses pattern recognition technique which is based on the use of unique biological details to verify a person's identity. Contrary to passwords or PINs that can be forgotten, stolen, or simply cloned, biometric identifiers are indispensable and secure. With the use of biometric data such as fingerprints, face or iris features, transactions are authenticated and secured, reducing the impact of unauthorized access or fake activities. What's more, biometric authentication gives you an experience of

unmatched convenience and speed in payments. Whereas smart phones with bio section sensors simplify payment authorization by using either touch or glazing print, without needing passwords or PINs, speeding u p the

process. This smooth and easy authentication process does not only contribute to better user experience but also generates faster transaction times as at a POS terminal and online platforms thus fosters efficiency. In summary, the use of biometric authentication in payments is a really important step towards security, convenience, and mutual inclusion.

1. LITERATURE REVIEW

[1] Payment Integration using Biometric and Virtual 3D Password: This survey gives us a wide knowledge about how the working of the fingerprint recognition works. Even though there are many papers on fingerprint detection, in this we can learn about the 3D password and integrate it into our project work. In this, the user fingerprint is scanned using the fingerprint scanner and matched with the existing fingerprint images to authenticate the user. This data is also used as the training data.

[2] A Broad Survey on Fingerprint Recognition Systems: This paper discusses about fingerprint mechanisms based on Minutiae based approach, Pattern Recognition Approach, Wavelet based Approach. The mechanism first scans the user's unprocessed image and then pre-processes it. The features of the image of the fingerprint are defined in terms of vector and are protected in the database. In this paper, wavelets and wave atoms are also introduced as for recognition of the fingerprint of the user.

[3] Fingerprint Based Online Payment System: The Fingerprint recognition and fabricating it in the database to authorize users. In this paper, to obtain accuracy of the user fingerprint it tries to get more perfect images of the finger so that while training its confidence is high.

[4] Face Recognition Login Authentication for Digital Payment Solution at COVID-19: To overcome some of the risk factors such as Theft of Emoney, Duplication of the original card, creating a fake message to trick users to make payments illegally. This paper tries to eliminate these risk factors by using fingerprint, Iris, face, etc. Using these as payment authorization we can risk those factors even in the money transactions.

[5] Face Recognition Based Payment Processing System: Face recognition can be done using webcams and in-built

cameras inlaptops. In this, Haar-cascade Algorithm is used to get facial features such as size and shape of Eyes and cheekbones, etc. Haar-cascade creates a set of classifiers of positive and negative images. These images will authorize who the users are when payment or verification is done. Facial features of each person are unique and this is used to represent a unique identity so that each person can have authorization and no fake authorization takes place. This paper surveys this algorithm trying to create a system that accurately recognizes the user.

[6] Designing of Face Recognition System: Face recognition is the most used authentication system especially in the smartphones to authenticate their users. The Authentication system face recognition is indeed very safe and cannot be overcome or fake easily. This paper studies the real-time face recognition and there are other criteria face recognition based on such eyes, nose and mouth. The system is run on python with OpenCV for face detection which makes it easier to create and store images on the Operating system. The paper is based on the study of Local binary pattern (LBP) which is used for extracting facial features and processing it.

The document describes a system that uses facial recognition to identify people. The technology became popular because it allows machines to "see" and understand faces; This can improve the way they interact with people. The process outlined in the article can impact the way we live by putting the face of security, payment, and even crime.

The entire system was developed using the popular programming language Python. OpenCV is a specialized function library designed for computer vision processing, providing important functions such as face detection and feature extraction. Additionally, Kivy, another Python library, is used to create user-friendly interfaces to interact with the system and even create programs that can run on different devices.

The entire system was developed using the popular programming language Python. OpenCV is a specialized function library designed for computer vision processing, providing important functions such as face detection and feature extraction. Additionally, Kivy, another Python library, is used to create user-friendly interfaces to interact with the system and even create programs that can run on different devices.

2. SYSTEM ARCHITECTURE

Fig. 3.1 shows the installation of some of the necessary python packages for the Payment system to run successfully. Information about the modules is given below:

```
Main.py ×
 1  import cv2
 2  import numpy as np
 3  import os
 4  import time
 5  import subprocess
 6  import json
 7  import urllib.request
 8  import urllib3
 9  import requests
10  from mfrc522 import SimpleMFRC522
11  import serial
12  import adafruit_fingerprint
```

Fig. 3.1 Modules Imported to Implemented Transactions Systems.

A. Imported Modules

[1]   Cv2

Cv2 module is feature extraction from images. It is a python binding in OpenCv which provides face detection for the payment system as the user's face is stored with an ID. It detects and identifies users in real-time.

[2]   numpy

NumPy is a scientific computation library implemented in Python. It offers a selection of mathematical functions in addition to tools for manipulating arrays and matrices. It is extensively utilised in machine learning and data science, and is regarded as an indispensable instrument for manipulating numerical data.

[3]   os

OS module helps the code to interact with the system allowing the access system files or accessing variables in the environment. OS provides function for directory operations.

[4]   time

The time module gives functions for generating delays or getting time intervals and also timestamps while the code is running.

[5]   subprocess

This module enables us to interact with the shell commands or system features, etc. Subprocess module allows the python script to run external commands.

[6]   json

To change or encode the python objects into JSON informationor decode the JSON information to python object, this module provides functions allowing to interchange the data when received.

[7]   Urllib.request, Urllib3, requests

To access data from web services like downloading the data or interacting with the web services, etc. This module is used for managing requests from web services like HTTP requests for data.

[8]   mfrc522

We are using RFID tags for identifying products and this module helps to read and write the RFID tags. This module interacts with the RFID reader chip and gives the information about what the product that tag refers to.

[9]   serial

Serial module allows the communication of the Raspberry Pi connected with the computer's serial port. This allows our Raspberry Pi to communicate with different features or parts of the system.

[10]   Adafruit_fingerprint

This module allows the python script to extract the fingerprint image of a user allowing the fingerprint sensor features to be used in our Transaction system. This Adafruit_fingerprint module is specially only for Adafruit fingerprint scanner hardware.

By combining these modules, we are building a Python program that captures data with cv2, processes it using NumPy, interacts with the operating system and external programs using os, time, and subprocess, sends or receives data over the network with the various request libraries, interacts with RFID readers and serial devices, and potentially implements fingerprint-based and also Face-recognition based authorization.

Payment systems have users choose their desired choice and make payment transactions. It will be faster and more secure as the modules are highly built making it a very possible implementation that can be used for bank-to-bank or shopping transactions

Flow Chart

The given flowchart describes the steps in which the flow of the payment system happens.
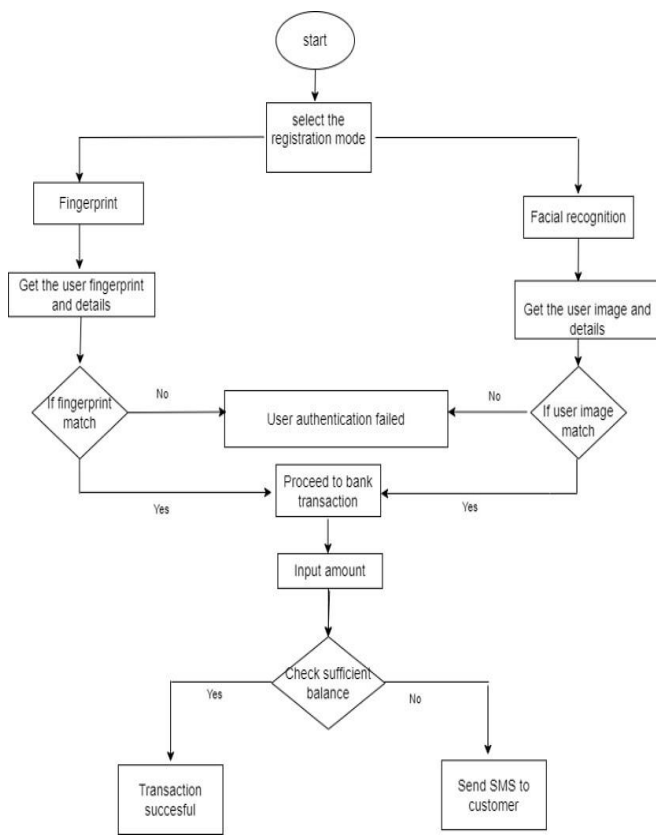
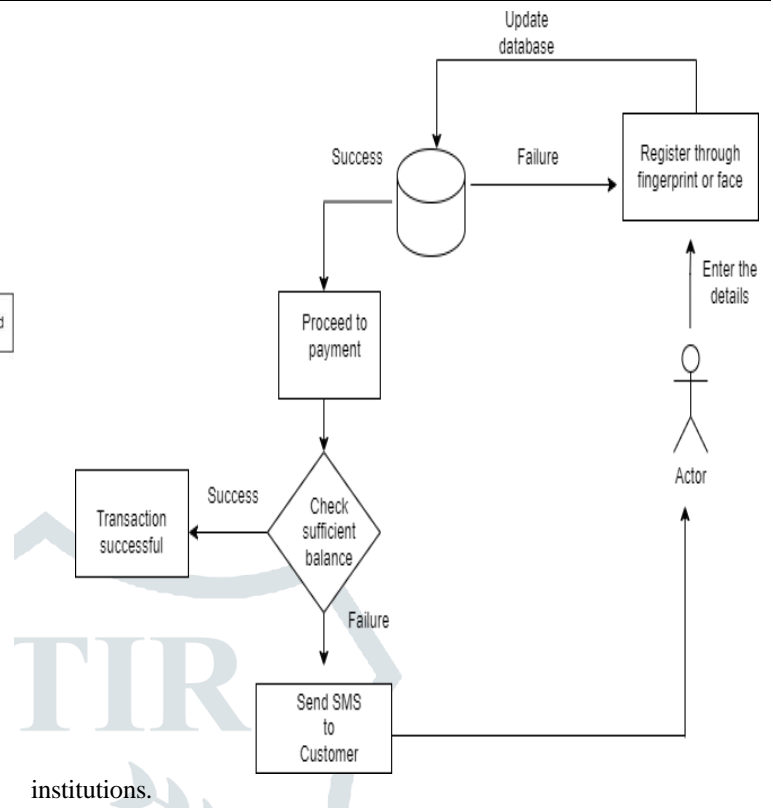Fig. 3.2 Flow Chart for a payment system using biometric authentication

Fig. 3.3 Activity Diagram

Activity Diagram

The activity diagram depicts all the steps which come into play when a biometric-based payment is executed. The first step of the process is to initiate the payment transaction. Afterwards, the user goes through authentication of their identity, an imperative step in the process to verify their authenticity and protection from any malicious acts. This process of authentication contains the step of capturing the user's biometric data such as fingerprints and face features, followed by the step of verifying which is matching the stored templates and to confirm the same. Then, if user authentication is successful the next option is selecting the desired payment method (biometric /facial recognition) Next the customer gives out the transaction specifics such as the payment amount and the details of the recipient so as to make the entries both accurate and complete. Then it schedules the payment to be processed, involving the appropriate gateway or financial institutions.

A successful processing of the transaction ends up with a confirmation of the transfer of funds, with the user receiving an indication of the transaction being completed. The end comes finally, and the process is done, thus marking the end of the payment transaction, which gives the user the liberty to proceed with the next step or exit the payment interface. Generally, the activity diagram outlines the activities involved sequentially, and it is a visual representation of the entire processing of the transaction that is integrated into biometric authentication. Besides that, the diagram helps to achieve a very high level of security and procedural integrity throughout the transaction process. This diagram will help us build a seamless transaction system that comes with a high level of security, as shown in the activity diagram, making it a highly integrated system for payment systems that can be used in different scenarios other than the shopping system. The SMS system shown in the diagram is to notify the user so that the user keeps track of the transactions.

Block-Diagram

Fig. 3.4 describes the block diagram for Payment transaction using biometric authentication and the explanation about the same is give below.
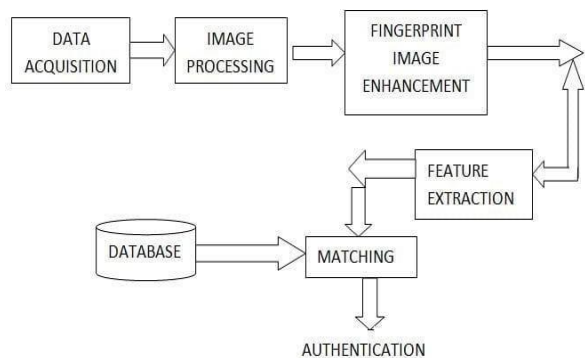

Fig. 3.4 Program Block Diagram for Payment Transaction System

The block diagram displays a complex system with the main purpose of authenticating the payment transactions implied by the use of biometric technologies. This would be a key factor that makes up the biometric scanner. The Biometric Scanner, which is this module's most sophisticated component, captures and analyzes the user's biological features, like fingerprints, face, or eye prints. Juxtaposing this module is the Payment Info Entry Interface, which is the most flexible platform that enables users to fill in the details of transactions. The interface provides functions such as defining the transaction amount and recipient information for users in order to let them have the advantage of tailoring their payment instructions into the particular form that they need. The Authentication Module verifies the transaction and payment data provided by the user once the information has been input. This fundamental feature utilizes advanced algorithms to conduct the verification by matching up the biometric information acquired with existing templates that are located within the system. The thorough screening through biometric authentication is the ultimate measure that assures that only authorized persons will be allowed to operate in the system by initiating the transaction request, thus ensuring the security posture. After that authentication, a hit on the Payment Processing System divulges the actual facts of the payment transaction. Being involved in financial communications, the system liaises with numerous payment gateways, banking institutions, and databases to create necessary and convenient transaction settings.The operation process in which authorization checks have common processes until the end, where funds are transferred, is covered by the Payment Processing System with unity and accuracy. The last result of your transaction is the secure and smooth payment experience that a user feels.

In fact, the block diagram is a summary of the complex scenario, where different components are closely interwoven and the system for biometric authentication serves as the monitor. Thanks to the combination of recent high-tech biometric technologies, natural intuitive user interfaces, and effective processing of payments, this system rests at the apex of quality in relation to the security and convenience of the present digital age.

3. METHODOLOGY

For biometric authentication. Upon initiating the authentication process, the device captures the user's biometric information again and performs a comparison with the stored template. Advanced algorithms are utilized to analyze and match the captured biometric data with the stored reference, ensuring a high level of accuracy and reliability. Throughout this process, robust encryption techniques are implemented to safeguard the biometric data during transmission and storage, preserving user privacy and preventing unauthorized access. By leveraging biometric authentication, payment transactions become not only more convenient but also significantly enhance security by providing a unique identifier tied directly to the user's physical characteristics. This information is then extracted, and the dialogue management component crafts a response-tailored enrollment process where they register their unique payment transaction, the user interacts with a compatible device, or the technology payment transaction using biometric authentication encompasses several key steps to ensure seamless and secure authentication. Initially, users undergo an enrollment process where they register their unique payment transaction. The user then interacts with a compatible device or platform, which prompts a promising avenue for secure and frictionless payment experiences in an increasingly digitized world.

4. RESULT AND DISCUSSION

Seamless transactions: Shopping will be done with seamless transactions with a glance at the camera or just with your fingerprint to authorize the payment. This will significantly reduce the waiting line or slow pace of use of the cards, PIN entry, etc.

User Comfortability: The system we proposed here gives users a choice on which type of payment authorization they want. Users can either select face or fingerprint for the payment transaction, so whichever they choose can be used to authorize the final payment.

Secure and Safe: Enhanced security can be achieved as the user's biometric data cannot be replicated or faked that easily, and the system will detect easily if there are any changes in the authorization and decline the payment.

The biometric payment system will be more secure and faster with the use of the Raspberry Pi, and both face and fingerprint detection will be integrated into it. As shown in Figures 5.1, 5.2, 5.3, and 5.4 below, these are the dashboard and completion of payment transactions using the biometric system via web host.

User Details: In this, we can see the user details who are registered with their details such as name, mobile number, email, city, and address.

Add User: We can add users here using their mobile, and then after the user adds their mobile number next, they'll give their other details like email, address, etc.

Product Details: The products can be seen here after the user takes them for checkout, and the product details are shown, such as the name, quantity, amount, or price of the product. Here, after the product is finalized, the user will be able to pay via face or biometric (face), and the transaction processes and authorizes the user.

Payment Successful: Once the user's transaction is completed, the dashboard will be redirected, showing that the payment successful and allowing them to proceed with the checkout.
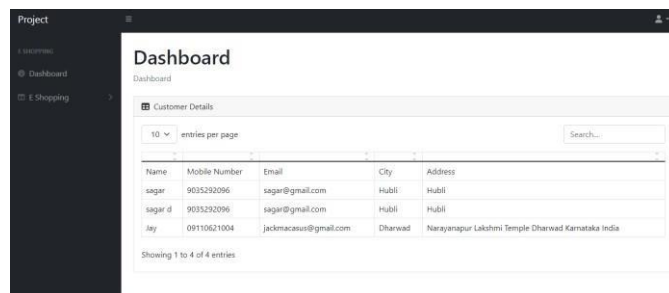

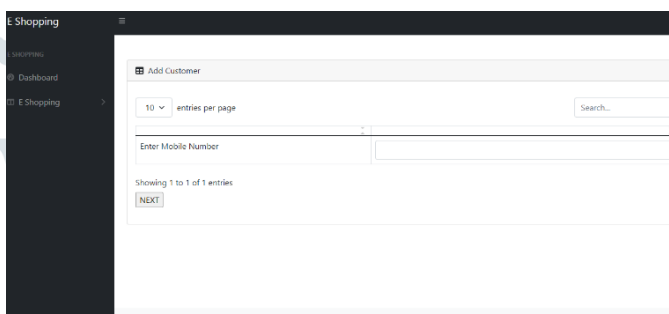Fig. 5.1 Dashboard Output of User Details
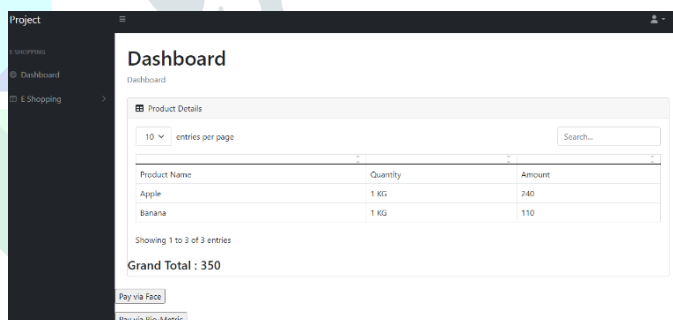

Fig. 5.2 Dashboard Output of Adding User

Fig. 5.3 Dashboard Output of Product Details and Payment Selection
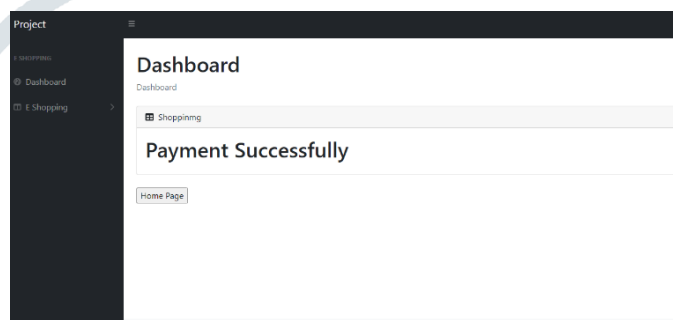

Fig. 5.4 Dashboard Output of Payment Transaction Successful

5. CONCLUSION

The process of buying and selling goods has undergone a dramatic paradigm shift driven by innovation and technology in the last decade. Biometrics, the science that encompasses the measurement and processing of irreplaceable anatomical (or behavioral) characteristics, is an effective and easy replacement for the traditional identification verification methods. Biometric recognition now comes in various forms, such as fingerprint recognition and facial and iris scans. What it does is increase the level of security and deliver a better experience for consumers when it comes to payment transactions. Traditional payment transactions required the processing of passwords, PINs, and magnetic stripe cards. Nevertheless, these methods are vulnerable to security flaws, with cases of identity theft and monetary fraud occurring more and more nowadays. Due to the shortcomings of conventional authentication methods, businesses and financial institutions have embraced biometrics as an additional feature of their security systems, which at the same time has simplified payment. Biometric authentication is based on the premise of using the unique biological characteristics of a person for the purpose of verifying the user's identity. Unlike passwords or PINs that can be misplaced, stolen, or easily replicated, biometric identifiers are uniquely and intrinsically associated with an individual personality and are highly impossible to forge or imitate. Through the application of biometric data, including fingerprints, facial features, and iris patterns, transaction verification can be done, and access to unauthorized and fraudulent activities can be reduced.

Furthermore, biometric authentication has become a standard for speed and convenience in payment transactions. Today, thanks to the growing number of smartphones with biometric sensors, payments' authorization has become as easy as a touch or a glance without the arising necessity of PINs and passwords. This smooth and trouble-free user authentication not only delights the user experience but also leads to transaction acceleration, hence favoring increased efficiency at points of sale terminals and online shopping platforms.

REFERENCES

[1] Prof. N.M. Mule, Vivek Mote, Abhishek Bhosle, Pratiksha Jadhav, Ankita Kulkarni "Payment Integration using Biometric and Virtual 3D Password" International Journal of Engineering Research & Technology (IJERT), Vol. 12 Issue 06, June-2023

[2] Subba Reddy Borra, G. Jagadeeswar Reddy, E. Sreenivasa Reddy "A Broad Survey on Fingerprint Recognition Systems" JUL 2022, IEEE WiSPNET, Volume 6 Issue 1

[3] R. Logeswari, M. Saikotesw ara, M. V. Sudheerkumar "Fingerprint Based Online Payment System", e-ISSN: 2395-0056, International Research Journal of Engineering and Technology (IRJET) Volume: 05 Issue: 10, Oct 2018

[4] Muhammad Irwan Nasution, Nurbaiti Nurbaiti, Nurlaila Nurlaila, Tri Inda Fadhila Rahma, Kamilah Kamilah "Face Recognition Login Authentication for Digital Payment Solution at COVID-19" (2020) International Conference on Computer and Informatics Engineering (IC2IE) Volume 21, Issue 5

[5] Romano Araujo, Adarsh Potekar, Mayuresh Raikar "Face Recognition Based Payment Processing System" International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056 Volume: 09 Issue: 07 | July 2022

[6] Vijay Kumar Sharma "Designing of Face Recognition System" International Conference on Intelligent Computing and Control Systems (ICICCS 2019), Volume:03 | July-2019