## **A MINI PROJECT REPORT**

## **ON**

**SECURING DIGITAL PAYMENTS WITH IRIS SCANNING USING BLOCKCHAIN TECHNOLOGY**

*Submitted in partial fulfillment of the requirement*

*for the award of the degree of*

## **BACHELOR OF TECHNOLOGY**

## **IN**

**COMPUTER SCIENCE AND ENGINEERING**

By

BOMMA TANYA (21P61A0535)

DIVYANSHI ROY (21P61A0562)

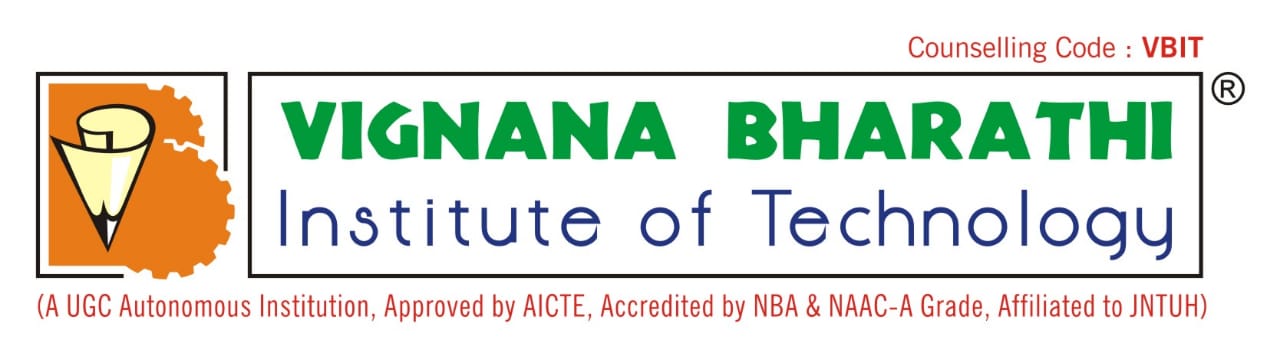
SNIGDHA BOMMIDALA (21P61A0536)

*Under the esteemed guidance of*

**Dr.G.Sreeram**

***Professor***

***Dept. of CSE***



Accredited by NBA & NAAC) Aushapur (V), Ghatkesar (M), Medchal(dist.)

**December – 2024**

**DECLARATION**

We, **Bomma Tanya ,Divyanshi Roy, Snigdha Bommidala** bearing hall ticket numbers (**21P61A0535 ,21P61A0562 , 21P61A0536)** hereby declare that the mini project report entitled “**Securing Digital Payments With Iris Scanning Using Blockchain Technology**” under the guidance of **Dr.G. Sreeram,** Professor, Department of Computer Science and Engineering**, Vignana Bharathi Institute of Technology, Hyderabad**, have submitted to Jawaharlal Nehru Technological University Hyderabad, Kukatpally, in partial fulfillment of the requirements for the award of the degree of Bachelor of Technology in Computer Science and Engineering.

This is a record of Bonafide work carried out by us and the results embodied in this project have not been reproduced or copied from any source. The results embodied in this project report have not been submitted to any other university or institute for the award of any other degree or diploma.

BOMMA TANYA (21P61A0535)

DIVYANSHI ROY (21P61A0562)

SNIGDHA BOMMIDALA (21P61A0536)

ii

#### D:\VBIT-LOGO.jpg

Aushapur (V), Ghatkesar (M), Hyderabad, Medchal – Dist, Telangana – 501 301.

### **DEPARTMENT**

### **OF**

**COMPUTER SCIENCE & ENGINEERING**

***CERTIFICATE***

This is to certify that the mini project titled **“****SECURING DIGITAL PAYMENTS WITH IRIS SCANNING USING BLOCKCHAIN TECHNOLOGY”** Submitted by **Bomma Tanya(21p61A0535), Divyanshi Roy(21p61A0562), Snigdha Bommidala (21p61A0536)** in B. Tech IV-I semester Computer Science & Engineering is a record of the bonafide work carried out by them.

The results embodied in this report have not been submitted to any other University for the award of any degree*.*

**INTERNAL GUIDE HEAD OF THE DEPARTMENT**

### **Dr. G. Sreeram Dr. Raju Dara**

**Professor Professor**

### **EXTERNAL EXAMINER**

iii

**ACKNOWLEDGEMENTS**

We are extremely thankful to our beloved Chairman, **Dr. N. Goutham Rao** andSecretar**y, Dr. G. Manohar Reddy** who took keen interest to provide us the infrastructural facilities for carrying out the project work.

We whole-heartedly thank **Dr. P. V. S. Srinivas, Professor & Principal**, and **Dr. Dara Raju**, Professor & Head of the Department, Computer Science and Engineering for their encouragement and support and guidance in carrying out the mini project phase I.

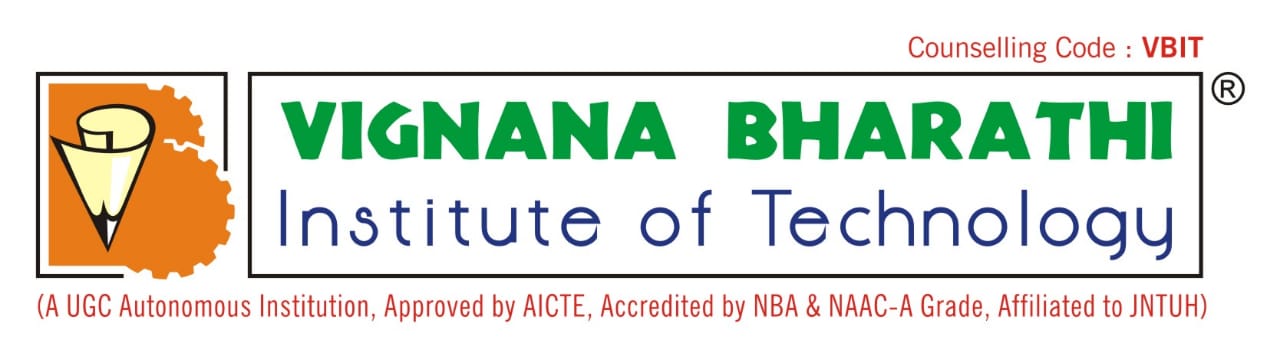
We would like to express our in debtedness to the Overall Project Coordinator, Dr. N. Swapna Associate Professor, and Section coordinators, **Mr. G.Arun**, Associate Professor, Department of CSE for their valuable guidance during the course of project work.

We thank our Project Guide, **Dr. G. Sreeram,** Professor, for providing us with an excellent project and guiding us in completing our mini project phase I successfully.

We would like to express our sincere thanks to all the staff of Computer Science and Engineering, VBIT, for their kind cooperation and timely help during the course of our project.

Finally, we would like to thank our parents and friends who have always stood by us whenever we were in need of them.

iv



**VISION**

To become, a Center for Excellence in Computer Science and Engineering with a focused Research, Innovation through Skill Development and Social Responsibility.

**MISSION**

**DM-1:** Provide a rigorous theoretical and practical framework across ***State-of-the-art*** infrastructure with an emphasis on ***software development***.

**DM-2:** Impact the skills necessary to amplify the pedagogy to grow technically and to meet ***interdisciplinary needs*** with collaborations.

**DM-3:** Inculcate the habit of attaining the professional knowledge, firm ethical values, ***innovative research*** abilities and societal needs.

**PROGRAM EDUCATIONAL OBJECTIVES (PEOs)**

**PEO-01: Domain Knowledge:** Synthesize mathematics, science, engineering fundamentals, pragmatic programming concepts to formulate and solve engineering problems using prevalent and prominent software.

**PEO-02: Professional Employment:** Succeed at entry- level engineering positions in the software industries and government agencies.

**PEO-03: Higher Degree:** Succeed in the pursuit of higher degree in engineering or other by applying mathematics, science, and engineering fundamentals.

**PEO-04: Engineering Citizenship:** Communicate and work effectively on team-based engineering projects and practice the ethics of the profession, consistent with a sense of social responsibility.

**PEO-05: Lifelong Learning:** Recognize the significance of independent learning to become experts in chosen fields and broaden professional knowledge.

**PROGRAM SPECIFIC OUTCOMES (PSOs)**

**PSO-01:** Ability to explore emerging technologies in the field of computer science and engineering.

**PSO-02:** Ability to apply different algorithms indifferent domains to create innovative products.

**PSO-03:** Ability to gain knowledge to work on various platforms to develop useful and secured

applications to the society.

**PSO-04:** Ability to apply the intelligence of system architecture and organization in designing the new era of computing environment.

**PROGRAM OUTCOMES (POs)**

**Engineering graduates will be able to:**

**PO-01: Engineering knowledge:** Apply the knowledge of mathematics, science, engineering fundamentals, and an engineering specialization to the solution of complex engineering problems.

**PO-02: Problem analysis:** Identify, formulate, review research literature, and analyze complex engineering problems reaching substantiated conclusions using first principles of mathematics, natural sciences, and engineering sciences.

**PO-03: Design/development of solutions:** Design solutions for complex engineering problems and design system components or processes that meet the specified needs with appropriate consideration for the public health and safety, and cultural, societal, and environmental considerations.

**PO-04: Conduct investigations of complex problems:** Use research-based knowledge and research methods including design of experiments, analysis and interpretation of data, and synthesis of the information to provide valid conclusions.

**PO-05: Modern tool usage:** Create, select, and apply appropriate techniques, resources, and modern engineering and IT tools including prediction and modelling to complex engineering activities with an understanding of the limitations.

**PO-06: The engineer and society:** Apply reasoning informed by the contextual knowledge to assess societal, health, safety, legal and cultural issues and the consequent responsibilities relevant to the professional engineering practice.

**PO-07: Environment and sustainability:** Understand the impact of the professional engineering solutions in societal and environmental contexts, and demonstrate the knowledge of, and need for sustainable development.

**PO-08: Ethics:** Apply ethical principles and commit to professional ethics and responsibilities and norms of the engineering practice.

**PO-09: Individual and team work:** Function effectively as an individual, and as a member or leader in diverse teams, and in multidisciplinary settings.

**PO-10: Communication:** Communicate effectively on complex engineering activities with the engineering community and with society at large, such as, being able to comprehend and write effective

reports and design documentation, make effective presentations, and give and receive clear instructions.

**PO-11: Project management and finance:** Demonstrate knowledge and understanding of the engineering and management principles and apply these to one's own work, as a member and leader in a team, to manage projects and in multidisciplinary environments.

**PO-12: Life-long learning:** Recognize the need for, and have the preparation and ability to engage in

independent and life-long learning in the broadest context of technological change.

**ABSTRACT**

The rapid advancement of digital payment systems necessitates robust security measures to ensure safe and seamless transactions. This study proposes an innovative framework that integrates iris-scanning technology with blockchain to enhance payment security. Iris recognition, known for its accuracy and uniqueness, serves as the primary authentication method, ensuring precise user identity verification by leveraging the distinct patterns of each user’s iris. Blockchain strengthens security by recording and safeguarding transaction data in a way that makes unauthorized alterations extremely difficult, significantly reducing the risk of tampering and fraud. Additionally, the use of iris scanning eliminates the need for traditional passwords or PINs, offering a more convenient and secure user experience. This framework not only enhances security but also improves transaction speed and efficiency, addressing key challenges in modern payment systems. By combining the precision of biometric authentication with the reliability of advanced data protection, it sets a new standard for digital payment security, fostering trust and paving the way for a more secure and user-friendly financial future.

**TABLE OF CONTENTS**

|  |  |  |
| --- | --- | --- |
| **CONTENTS** |  | **PAGE NO** |
| Declaration |  | II |
| Certificate |  | III |
| Acknowledgements |  | IV |
| Vision & Mission |  | V |
| Abstract |  | VI |
| Table of Contents |  | VII |
| List of Figures |  | VIII |
| Output Screens |  | IX |
| Nomenclature |  | X |

1. Introduction
   1. [Introduction to the system 1](#_bookmark0)
   2. Problem Definition 1
   3. Objectives 1
   4. [Aim of the project 1](#_bookmark1)
2. [Literature Survey 2](#_bookmark2)-3
   1. [Proposed System](#_bookmark4) 3
   2. [Scope of the project 3](#_bookmark5)
3. Requirement [Analysis](#_bookmark6) 4-7
   1. Operating Environment 4
   2. [Functional](#_bookmark4) Requirements 4
   3. Non Functional Requirements 5
   4. [System](#_bookmark10) Analysis 7
4. System Design 8-9
   1. Architectural Design 8
   2. UML Diagrams 9
5. Implementation 10-20
   1. Explanation of Key Function 10
   2. [Method](#_bookmark12)ology and Modular Implementation 10
6. [Testing And Validation 2](#_bookmark2)0-25
   1. [Testing](#_bookmark3) Process 20
   2. [Test](#_bookmark4) Scenarios and Cases 21
   3. [Validation](#_bookmark5) of Security Performance 25
7. [Output Screens 2](#_bookmark2)6-28
   1. User Registration and Login Screens 26
   2. [Transaction](#_bookmark4) Screens with Iris Authentication 27
   3. [Blockchain](#_bookmark5) Transaction Records 28
8. [Conclusion and Future Enhancement 2](#_bookmark2)9
   1. [Conclusion](#_bookmark3) 29
   2. [Future](#_bookmark4) Scope and Enhancement 29

**List Of Figures**

|  |  |  |
| --- | --- | --- |
| **Sno** | **TITLE** | **PAGE NO** |
| 1. | General view of proposed system | 8 |
| 2. | Use Case for the application | 9 |
| 3. | Sequence Diagram | 9 |

viii

**List Of Output Screens**

|  |  |  |
| --- | --- | --- |
| **Sno** | **TITLE** | **PAGE NO** |
| 1. | Logo Page | 26 |
| 2. | User Registration | 26 |
| 3. | Iris Authentication | 27 |
| 4. | Transaction Screen | 27 |
| 5. | Transaction Status | 28 |
| 6. | Blockchain Transaction Records | 28 |

ix

**Nomenclature**

* Iris Scanning: A biometric authentication method that uses the unique patterns of the human iris for secure and accurate user verification.
* Blockchain: A decentralized and immutable ledger that records all transactions securely and transparently across multiple nodes.
* Digital Payment Platform: A system that facilitates the transfer of money electronically between users, merchants, and banks without requiring physical cash.
* Biometric Authentication: A process that verifies a user's identity based on unique biological traits, replacing traditional PINs or passwords.
* Secure Transactions: Financial activities safeguarded against unauthorized access, fraud, or data breaches using advanced security protocols like biometrics and blockchain.
* Transaction ID: A unique identifier assigned to each transaction for tracking and auditing purposes.
* User Identity Verification: The process of confirming user authenticity through iris scans instead of conventional methods like PINs or passwords.
* Transaction History: A detailed log of all user transactions, stored securely on the blockchain for transparency and traceability.
* Payment Gateway: A service integrated into the application to securely process digital payment transactions.
* Contactless Payments: Payments made using technologies like QR codes or NFC, eliminating the need for physical touchpoints.

x

* Integration API: A set of tools enabling the app to connect with banks, merchants, and third-party services for enhanced functionality.
* Customer Support Module: A built-in feature providing users with support for transaction disputes, authentication issues, and general inquiries.

**CHAPTER 1**

**INTRODUCTION**

## **INTRODUCTION**

### **Introduction To The System**

The rise of digital payment platforms has greatly enhanced transaction efficiency but exposed vulnerabilities in traditional authentication methods like PINs and passwords, which are prone to cyber threats. This system proposes a solution by integrating iris scanning, a secure biometric authentication method, with blockchain technology, a decentralized, tamper-proof ledger. Iris scanning offers precise and non-transferable user identification, while blockchain ensures secure, transparent, and fraud-resistant transactions. Together, they provide a highly secure, reliable, and transparent payment solution that mitigates fraud and enhances user trust, setting a new standard for digital payment security.

### **Problem Statement**

Traditional authentication methods like PINs, passwords, and OTPs are vulnerable to cyber threats such as hacking, phishing, and credential theft, posing security risks to digital payment systems. These weaknesses lead to fraud, unauthorized access, and data breaches, undermining user trust. This project aims to address these issues by integrating iris scanning for secure biometric authentication and blockchain technology for tamper-proof, transparent transaction recording, creating a more reliable and secure digital payment system.

### **1.3 Objective**

The objective of this system is to develop a secure and efficient digital payment platform that utilizes iris scanning for biometric authentication and blockchain technology for transparent, tamper-proof transaction recording. The goal is to enhance security, prevent fraud, and improve user trust by offering a seamless and robust authentication method, while ensuring that all transactions are securely processed and recorded in a decentralized, immutable ledger

### **1.4 Aim of The Project**

## The aim of this project is to develop a digital payment system that integrates iris scanning for biometric authentication and blockchain for secure, decentralized transaction management, enhancing reliability and user confidence.

1

**CHAPTER 2**

**LITERATURE SURVEY**

## **LITERATURE SURVEY**

With the rise of digital payment platforms, ensuring security and user authentication has become a critical concern. Traditional authentication methods such as PINs, passwords, and OTPs are increasingly vulnerable to cyber threats like hacking and phishing. Biometric technologies, especially iris scanning, offer a more secure alternative due to their unique and difficult-to-replicate characteristics. Studies show that iris recognition provides a higher level of accuracy and security than other biometric methods, making it an ideal candidate for digital payment systems​

In parallel, blockchain technology has emerged as a powerful tool to enhance the security and transparency of digital transactions. Blockchain’s decentralized and immutable nature ensures that transaction data cannot be tampered with, providing an extra layer of security. Integrating blockchain with iris scanning for authentication in payment systems has been proposed as an ideal solution to mitigate fraud and enhance security. This combination ensures that both the user and the transaction are securely verified without relying on central authorities, reducing vulnerability to cyberattacks​

While the integration of these technologies is still in its nascent stage, pilot projects and research highlight the potential of this combined approach. By leveraging blockchain’s decentralized nature and the high accuracy of iris scanning, digital payment systems can achieve a level of security and transparency that traditional systems cannot offer.

2

### **Proposed System**

The proposed system relies on specific inputs to ensure secure and efficient operation. During user registration, high-resolution iris data is captured and processed for future authentication, alongside basic user details. For transaction processing, the system accepts inputs such as recipient details, transaction amount, and optional remarks. Real-time iris scans are performed during login and payment authorization to validate user identity, ensuring that only authorized individuals can access and use the system for secure financial transactions.

### **Scope of the Project**

The project focuses on integrating iris scanning for biometric authentication with blockchain technology for secure digital payments. It aims to replace traditional methods like PINs and passwords with iris recognition to enhance security and reduce fraud.

3

**CHAPTER 3**

**REQUIREMENT ANALYSIS**

**REQUIREMENT ANALYSIS**

**3.1 Operating Environment**

**3.1.1 Hardware Requirements:**

* Processor: Intel i3 or higher, or equivalent
* RAM: Minimum 8 GB
* Storage: Minimum 256 GB SSD
* Camera: High-resolution camera (at least 1080p)

**3.1.2 Software Requirements:**

* Operating System:
* Microsoft Windows 10/11Development Environment:
* IDE: Visual Studio Code
* Programming Languages : Python (v3.x),Solidity, JavaScript, HTML/CSS
* Libraries and Frameworks: OpenCV ,Web3.py ,Flask
* Blockchain Framework: Ganache ,Truffle , Ethereum.
* Package Managers and Other Tools: NPM (Node Package Manager) ,Chocolatey ,JSON files

**3.2 Functional Requirements**

The functional requirements for Securing Digital Payments with Iris Scanning Using Blockchain Technology outline the key capabilities and operations that the system must support to ensure efficient and secure user interaction with the payment platform.

User Registration and Authentication:

* The system must allow users to register by capturing their iris data using a high-resolution camera. During login, the system should authenticate users through iris scanning for secure access, replacing traditional PINs and passwords.

Transaction Verification:

* Every financial transaction must be verified through iris recognition to ensure that the user is authorized to perform the action. The system should capture the iris image, match it with the registered data, and proceed only if a match is found, preventing unauthorized access.

4

Blockchain Integration:

* The system must use blockchain technology to record all transactions in a decentralized, immutable ledger, ensuring that data cannot be tampered with. Each transaction will include a hash generated from the iris scan and transaction data, which is then recorded on the blockchain.

Real-Time Processing:

* The platform must process transactions in real-time. Once the iris scan is authenticated and the transaction verified, the blockchain should record it immediately, ensuring timely payment confirmations.

Data Privacy and Security:

* The system should ensure that all biometric data (iris images) is encrypted and stored securely. User data and transaction records on the blockchain should be protected with advanced cryptography to maintain privacy and prevent unauthorized access.

User Interface:

* The system should provide a user-friendly interface for registering, logging in, and performing transactions. The interface should allow users to see their transaction history and the status of their payment confirmations.

Transaction Monitoring and Alerts:

* The platform should offer real-time alerts to users about transaction status, including successful payments, pending verifications, or potential issues. This feature ensures transparency and allows users to track their financial activities.

Scalability and Performance:

* The system must support high volumes of concurrent users and transactions. The infrastructure should be scalable to accommodate future growth.

**3.3** **Non- Functional Requirements**

* The non-functional requirements define the overall qualities and performance standards of the Securing Digital Payments with Iris Scanning Using Blockchain Technology system, ensuring that it operates efficiently, reliably, and securely.

5

Performance:

* The system must provide low latency for iris scanning and transaction verification. It should authenticate users and process payments in real-time, with minimal delays between scanning, verification, and transaction completion. Transaction processing time should be under a predefined threshold to ensure a smooth user experience.

Scalability:

* The system must be able to handle increasing volumes of users and transactions as it grows. It should support a large number of concurrent users without degradation in performance, ensuring that both iris scanning and blockchain processing are efficient even with a high transaction load. This can be achieved by using cloud infrastructure or distributed systems.

Security:

* The system must adhere to industry-standard encryption protocols for storing and transmitting biometric data and transaction records. It should ensure that both iris data and blockchain records are protected from unauthorized access or tampering. Additionally, the system must comply with privacy regulations like GDPR to safeguard user data.

Usability:

* The platform should be easy to use with a simple, intuitive interface for both users and administrators. The biometric authentication process should be seamless and quick, with minimal user input. Users should be able to perform transactions effortlessly, with clear instructions and feedback throughout the process.

Reliability:

* The system should ensure high availability with minimal downtime. It must be resilient to system failures, offering failover mechanisms and quick recovery in case of unexpected disruptions. Regular backups of blockchain data should be performed to prevent data loss.

Maintainability:

* The system architecture should be modular, allowing for easy updates, bug fixes, and system upgrades without affecting overall performance. Code should be clean and well-documented to facilitate ongoing maintenance and future development.

Compatibility:

* The system must be compatible with various devices and platforms, including smartphones, tablets, and web browsers. It should support a wide range of operating systems, including Android and iOS, ensuring that users can access the payment platform regardless of their device choice.

6

Interoperability:

* The system must be able to integrate with existing payment gateways, banks, and blockchain networks. It should support a range of currencies and payment methods, ensuring a global reach for users.

**3.4 System Analysis:**

* The system analysis for Securing Digital Payments with Iris Scanning Using Blockchain Technology examines both functional and non-functional aspects to ensure seamless integration and efficient operation. The system relies on iris scanning for user authentication. Real-time scanning and matching with the registered iris template will be essential to prevent delays during authentication. Blockchain technology will be employed to create a decentralized ledger that records transactions immutably and transparently, ensuring transaction data cannot be altered and adding an extra layer of security. The system will integrate a distributed network of nodes for transaction processing and validation, ensuring the integrity and accountability of the payment process. Smart contracts, using platforms like Ethereum or Hyperledger, will automate transaction verification and execution, reducing reliance on third-party intermediaries.
* Given the sensitive nature of biometric data, the system will implement stringent security measures, such as encryption for storing iris data securely, while blockchain will protect transaction information through cryptographic hashes. The user workflow will involve registering with an iris scan, storing the scan in the blockchain for secure reference, and scanning the iris again during transaction initiation for real-time authentication. Once authenticated, the transaction will be securely recorded in the blockchain, ensuring validation and visibility without exposing sensitive data.
* To enhance user experience, the system will feature a user-friendly interface, making the iris scanning process quick and reliable. Blockchain integration will be seamless and transparent, focusing on streamlining transactions while maintaining high security. Features like user notifications and transaction history will enhance usability and transparency, ensuring users can track their financial activities with ease. Overall, the system analysis ensures that the platform will deliver a secure, scalable, and efficient digital payment solution that improves both security and user experience.

7

**CHAPTER 4**

**SYSTEM DESIGN**

**SYSTEM DESIGN**

**4.1 Architectural Design**

The system's architecture integrates three key components: the User Interface, Iris Recognition Module, and Blockchain Network. The User Interface facilitates registration, authentication, and transaction management. The Iris Recognition Module uses advanced algorithms to capture, encrypt, and verify biometric data. Once authenticated, the Blockchain Network records transactions securely in a decentralized ledger. The design ensures seamless interaction between components, prioritizing real-time performance, scalability, and data security while maintaining a user-friendly experience.

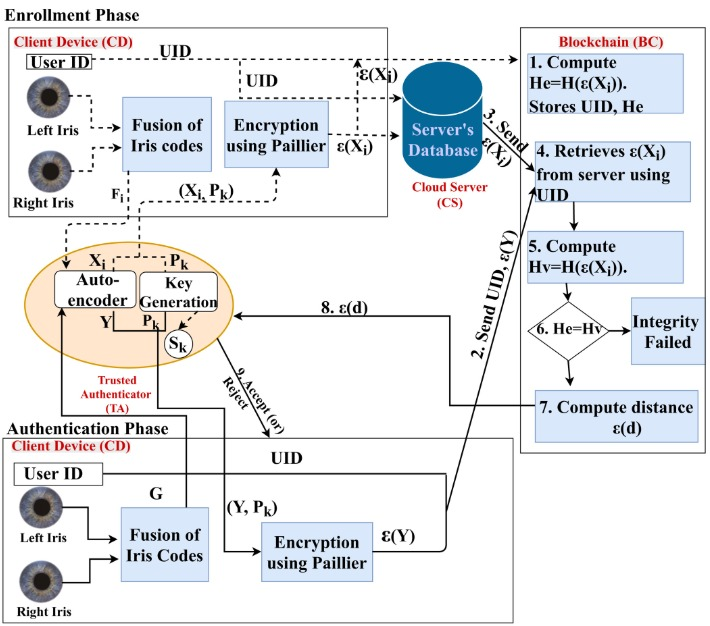


Fig:4.1 General view of Proposed system

**4.2 UML Diagrams**

The use case diagram for this application highlights the interactions between the user and the system's core functionalities. It includes key actions such as registering the user with iris data, authenticating via iris scanning, initiating financial transactions, and viewing transaction history. The diagram also showcases how the system communicates with the blockchain network to verify and record transactions

8

securely, ensuring data integrity and privacy. By depicting these interactions, the diagram provides a clear outline of the application's functionality and its relationship with external systems.

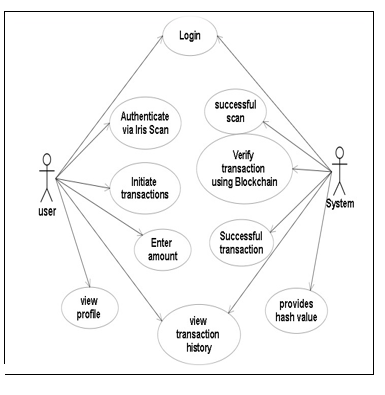


Fig:4.2 Use Case for the application

The sequence diagram details the step-by-step interaction flow within the application. It captures the process of user authentication, where the iris data is scanned and validated against stored records. Following authentication, the sequence of initiating a transaction, verifying it through the blockchain, and providing real-time confirmation to the user is illustrated. The diagram also includes the flow of encrypting biometric data and generating notifications for transaction updates, emphasizing the system’s operational sequence and the coordination between its component.

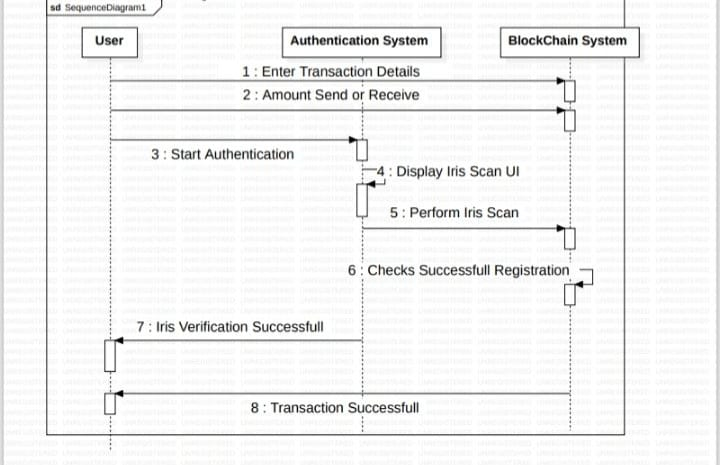
****

Fig:4.3 Sequence diagram

9

**CHAPTER 5**

**IMPLEMENTATION**

**IMPLEMENTATION**

**5.1 Explanation of Key Functions:**

The Securing Digital Payments Using Iris Scanning and Blockchain Technology system integrates cutting-edge biometric authentication with blockchain-based transaction processing for enhanced security in financial transactions. The core functionality begins with iris scanning, where a user’s unique iris patterns are captured and processed using Open CV for accurate feature extraction. This biometric data is then compared to stored reference information to verify the user’s identity. Upon successful authentication, the system leverages Ethereum blockchain for processing payments, where smart contracts automatically validate the conditions for the transaction.

In the blockchain layer, Web3.js connects the front-end application to the blockchain, enabling the execution of smart contracts that control the payment process. These contracts ensure that payments are only executed when the biometric authentication and predefined transaction conditions are met. The use of Ganache and Truffle facilitates development, testing, and deployment of these contracts. All transactions are securely logged onto the blockchain, creating a transparent, immutable record of every payment. This ensures both security and accountability. The system is compatible with various platforms and uses Flask for the backend API, allowing seamless interaction between the web interface, biometric authentication, and blockchain for real-time transaction validation.

**5.2 Methodology and Modular Implementation:**

The system is implemented using a modular architecture, integrating biometric authentication with blockchain technology to ensure secure and efficient digital payments. The Iris Recognition Module handles the capture and processing of biometric data for user registration and authentication. The Transaction Processing Module enables users to initiate transactions, while the Blockchain Module securely verifies and records these transactions on a decentralized ledger. These modules work in harmony to provide a seamless, reliable, and secure payment experience.

**Source code:**

**Homepage.html**

<!DOCTYPE html>

<html lang="en">

<head>

    <meta charset="UTF-8">

10

    <meta name="viewport" content="width=device-width, initial-scale=1.0">

    <title>Iris Pay - Home</title>

    <link rel="stylesheet" href="https://cdnjs.cloudflare.com/ajax/libs/font-awesome/6.0.0-beta3/css/all.min.css">

    <style>

        /\* Body and base styles \*/

        body {

            font-family: Arial, sans-serif;

            margin: 0;

            padding: 0;

        }

        /\* Header Section \*/

        .header {

            background-color: #4CAF50;

            color: white;

            text-align: center;

            padding: 1rem 0;

        }

        /\* Profile Section \*/

        .profile-section {

            display: flex;

            align-items: center;

            padding: 1rem;

            background-color: #f4f4f4;

            border-bottom: 1px solid #ddd;

            cursor: pointer;

        }

        .profile-section i {

            font-size: 3rem;

            margin-right: 1rem;

        }

        .profile-section h2, .profile-section p {

            margin: 0;

        }

        /\* QR Code Section \*/

        .qr-section {

            text-align: center;

            margin: 2rem 0;

        }

11

        .qr-section i {

            font-size: 4rem;

            margin-top: 1rem;

            color: #4CAF50;

        }

        /\* Main Content \*/

        .main-content {

            padding: 1rem;

        }

        /\* Actions Section \*/

        .actions {

            display: flex;

            justify-content: space-around;

            margin-bottom: 2rem;

        }

        .action-card {

            text-align: center;

            text-decoration: none;

            color: inherit;

        }

        .action-card i {

            font-size: 2rem;

            display: block;

            margin-bottom: 0.5rem;

            color: #4CAF50;

        }

        .action-card p {

            margin: 0;

        }

        /\* Transaction Form \*/

        .transaction-form {

            max-width: 400px;

            margin: 0 auto;

            padding: 1rem;

            border: 1px solid #ddd;

            border-radius: 5px;

            background-color: #f9f9f9;

        }

12

        .transaction-form input {

            width: 100%;

            padding: 0.5rem;

            margin-bottom: 1rem;

            border: 1px solid #ddd;

            border-radius: 5px;

        }

        .transaction-form button {

            width: 100%;

            padding: 0.7rem;

            background-color: #4CAF50;

            color: white;

            border: none;

            border-radius: 5px;

            cursor: pointer;

        }

        .transaction-form button:hover {

            background-color: #45a049;

        }

        /\* Icon Header Section \*/

        .icon-header {

            display: flex;

            justify-content: space-around;

            padding: 0.5rem 0;

            background-color: #4CAF50;

            position: fixed;

            bottom: 0;

            width: 100%;

        }

        .icon-header a {

            text-align: center;

            text-decoration: none;

            color: white;

        }

        .icon-header i {

            font-size: 1.5rem;

        }

</style>

</head>

13

<body>

    <!-- Header Section -->

    <div class="header">

        <h1>Welcome to Iris Pay</h1>

    </div>

    <!-- Profile Section -->

    <a href="/userdetails" style="text-decoration: none; color: inherit;">

        <div class="profile-section">

            <i class="fas fa-user-circle"></i>

            <div>

                <h2>John Doe</h2>

                <p>+91 123 456 7890</p>

                <p>johndoe@example.com</p>

            </div>

        </div>

    </a>

    <!-- QR Code Section -->

    <div class="qr-section">

        <h2>Scan to Pay</h2>

        <i class="fas fa-qrcode"></i>

    </div>

    <!-- Actions Section -->

    <div class="main-content">

        <div class="actions">

            <a href="/sendmoney" class="action-card">

                <i class="fas fa-paper-plane"></i>

                <p>Send Money</p>

            </a>

            <a href="/receivemoney" class="action-card">

                <i class="fas fa-plus-circle"></i>

                <p>Receive Money</p>

            </a>

            <a href="/paybills" class="action-card">

                <i class="fas fa-file-invoice-dollar"></i>

                <p>Pay Bills</p>

            </a>

        </div>

        <!-- Transaction Form -->

        <div class="transaction-form">

            <h2>Send Money</h2>

            <form id="sendForm">

14

                <input type="text" id="recipientAddress" placeholder="Recipient Address" value="0x7f5Ee9249b31d3bFD6Eb89ac9383D365D4951964" required>

                <input type="number" id="amountEth" value="0.1" step="0.01" placeholder="Amount (ETH)" required>

                <input type="text" id="note" placeholder="Note (optional)">

                <button type="button" id="sendMoneyBtn">Send Money</button>

            </form>

            <div id="result"></div>

        </div>

    </div>

    <!-- Navigation -->

    <div class="icon-header">

        <a href="/">

            <i class="fas fa-home"></i>

            <p>Home</p>

        </a>

        <a href="/history">

            <i class="fas fa-history"></i>

            <p>History</p>

        </a>

    </div>

    <!-- JS Logic -->

    <script>

        document.getElementById('sendMoneyBtn').addEventListener('click', async () => {

            const recipientAddress = document.getElementById('recipientAddress').value;

            const amountEth = document.getElementById('amountEth').value;

            const note = document.getElementById('note').value;

            try {

                const response = await fetch('/send\_money', {

                    method: 'POST',

                    headers: { 'Content-Type': 'application/json' },

                    body: JSON.stringify({ recipient\_address: recipientAddress, amount\_eth: amountEth, note })

                });

               const result = await response.json();

                const resultDiv = document.getElementById('result');

                if (response.ok) {

                    resultDiv.innerHTML = `<p style="color: green;">Transaction Successful! Tx Hash: ${result.tx\_hash}</p>`;

                } else {

15

                    resultDiv.innerHTML = `<p style="color: red;">Error: ${result.error}</p>`;

                }

            } catch (error) {

                console.error(error);

                alert('An error occurred while processing the transaction.');

            }

        });

    </script>

</body>

</html>

**Sendmoney.html**

<!DOCTYPE html>

<html lang="en">

<head>

    <meta charset="UTF-8">

    <meta name="viewport" content="width=device-width, initial-scale=1.0">

    <title>Send Money - Iris Pay</title>

    <link rel="stylesheet" href="https://cdnjs.cloudflare.com/ajax/libs/font-awesome/6.0.0-beta3/css/all.min.css">

    <style>

        /\* Include your CSS styles here \*/

        .camera-container {

            display: none;

        }

    </style>

</head>

<body>

    <div class="header">

        <h1>Send Money</h1>

    </div>

    <form id="sendForm">

        <input type="text" id="recipientAddress" placeholder="Recipient Address" value="0x7f5Ee9249b31d3bFD6Eb89ac9383D365D4951964" required>

        <input type="number" id="amountEth" value="0.1" step="0.01" placeholder="Amount (ETH)" required>

        <input type="text" id="note" placeholder="Note (optional)">

        <button type="button" id="sendMoneyBtn">Send Money</button>

    </form>

    <!-- Camera container -->

    <div id="cameraContainer" class="camera-container">

        <h2>Scanning Iris...</h2>

16

        <video id="video" width="640" height="480" autoplay></video>

        <button id="scanCompleteBtn">Complete Scan</button>

    </div>

    <div id="result"></div>

    <script>

        document.getElementById('sendMoneyBtn').addEventListener('click', async () => {

            // Get user inputs

            const recipientAddress = document.getElementById('recipientAddress').value;

            const amountEth = document.getElementById('amountEth').value;

            const note = document.getElementById('note').value;

            // Trigger iris scan before proceeding with transaction

            const irisScanResponse = await startIrisScan();

            if (irisScanResponse.status === 'success') {

                // If iris scan is successful, proceed with sending money

                const response = await fetch('/send\_money', {

                    method: 'POST',

                    headers: { 'Content-Type': 'application/json' },

                    body: JSON.stringify({ recipient\_address: recipientAddress, amount\_eth: amountEth, note })

                });

                const result = await response.json();

                const resultDiv = document.getElementById('result');

                if (response.ok) {

                    resultDiv.innerHTML = `<p style="color: green;">Transaction Successful! Tx Hash: ${result.tx\_hash}</p>`;

                } else {

                    resultDiv.innerHTML = `<p style="color: red;">Error: ${result.error}</p>`;

                }

            } else {

                // If iris scan fails, show an error message

                document.getElementById('result').innerHTML = `<p style="color: red;">Iris scan failed. Please try again.</p>`;

            }

        });

        async function startIrisScan() {

            // Show camera container

            document.getElementById('cameraContainer').style.display = 'block';

17

            // Access camera

            const video = document.getElementById('video');

            const stream = await navigator.mediaDevices.getUserMedia({ video: true });

            video.srcObject = stream;

            // Wait for the user to click the "Complete Scan" button

            return new Promise((resolve, reject) => {

                document.getElementById('scanCompleteBtn').addEventListener('click', () => {

                    // Stop the video stream when scan is complete

                    stream.getTracks().forEach(track => track.stop());

                    document.getElementById('cameraContainer').style.display = 'none';  // Hide camera

                    resolve({ status: 'success', message: 'Iris scan completed successfully!' });

                });

            });

        }

    </script>

</body>

</html>

**Iris\_scan.py**

import cv2

def iris\_scan():

    print("Opening camera for iris scan...")

    cap = cv2.VideoCapture(0)

    if not cap.isOpened():

        print("Error: Camera could not be opened!")

        return False

    print("Press 'q' to simulate iris scan completion.")

    while True:

        ret, frame = cap.read()

        if not ret:

            print("Error: Could not read frame.")

            break

        cv2.imshow("Iris Scan in Progress", frame)

        if cv2.waitKey(1) & 0xFF == ord('q'):  # Simulate successful scan

            print("Iris scan completed successfully!")

            cap.release()

            cv2.destroyAllWindows()

            return True

18

    cap.release()

    cv2.destroyAllWindows()

    return False

if \_\_name\_\_ == '\_\_main\_\_':

    if iris\_scan():

        print("Iris scan completed successfully!")

    else:

        print("Iris scan failed.")

**app.py**

from flask import Flask, jsonify, request, send\_from\_directory

from flask\_cors import CORS

import os

import subprocess

app = Flask(\_\_name\_\_)

# Enable CORS for all routes

CORS(app)

# Path to the frontend folder

frontend\_folder = os.path.join(app.root\_path, 'frontend')

# Routes for serving frontend pages

@app.route('/')

def homepage():

    return send\_from\_directory(frontend\_folder, 'homepage.html')

@app.route('/sendmoney')

def sendmoney():

    return send\_from\_directory(frontend\_folder, 'sendmoney.html')

@app.route('/receivemoney')

def receivemoney():

    return send\_from\_directory(frontend\_folder, 'receivemoney.html')

@app.route('/paybills')

def paybills():

    return send\_from\_directory(frontend\_folder, 'paybills.html')

@app.route('/requestmoney')

def requestmoney():

    return send\_from\_directory(frontend\_folder, 'requestmoney.html')

19

@app.route('/mobilerecharge')

def mobilerecharge():

    return send\_from\_directory(frontend\_folder, 'mobilerecharge.html')

@app.route('/investments')

def investments():

    return send\_from\_directory(frontend\_folder, 'investments.html')

@app.route('/wealth')

def wealth():

    return send\_from\_directory(frontend\_folder, 'wealth.html')

@app.route('/insurance')

def insurance():

    return send\_from\_directory(frontend\_folder, 'insurance.html')

# Endpoint for Send Money functionality

@app.route('/send\_money', methods=['POST'])

def send\_money():

    data = request.get\_json()

    recipient\_address = data.get('recipient\_address')

    amount\_eth = data.get('amount\_eth')

    note = data.get('note')

    # Simulate transaction logic

    response = {

        "tx\_hash": "0x1234567890abcdef",

        "status": "Success"

    }

    return jsonify(response)

# Endpoint for Iris Scan Simulation

@app.route('/start\_iris\_scan', methods=['POST'])

def start\_iris\_scan():

    try:

        # Call the iris\_scan.py script to simulate the iris scan

        result = subprocess.run(['python', 'iris\_scan.py'], capture\_output=True, text=True)

        if "Iris scan completed successfully!" in result.stdout:

            return jsonify({"status": "success", "message": "Iris scan completed successfully!"})

        else:

            return jsonify({"status": "failure", "message": "Iris scan failed!"})

    except Exception as e:

        return jsonify({"status": "failure", "message": str(e)})

20

if \_\_name\_\_ == '\_\_main\_\_':

    # Start the Flask app on host 0.0.0.0 to make it accessible on the network

    app.run(debug=True, host='0.0.0.0', port=8080)

21

**CHAPTER 6**

**TESTING AND VALIDATION**

**TESTING AND VALIDATION**

**6.1 Testing Process:**

The testing process for Securing Digital Payments with Iris Scanning Using Blockchain Technology aims to ensure that the system meets the functional, security, and performance requirements. It involves a comprehensive approach, testing each component individually and evaluating how they work together in the overall system. The process is divided into several stages, each focusing on a different aspect of the system to verify its reliability, accuracy, and robustness.

The first stage of testing involves unit testing, where individual components like the iris scanning module, blockchain integration, encryption mechanisms, and user interface are tested in isolation. This ensures that each module performs as expected in terms of functionality and security. The iris scanning module will be tested for accuracy in recognizing users, using a variety of iris images to validate the recognition algorithms. Blockchain integration will be tested to ensure that transactions are being recorded correctly, smart contracts are executing as intended, and the decentralized ledger is functioning as expected.

Next, integration testing will be performed to assess how well the modules interact with each other. This step is crucial to ensure that the iris scanning and blockchain components integrate seamlessly during the authentication and transaction processes. The system’s ability to record transactions on the blockchain, along with the authentication of users through iris scanning, will be evaluated in a controlled environment. The user authentication and transaction flow will be tested under different conditions to simulate real-world scenarios.

Following integration testing, performance testing will be conducted to ensure that the system can handle high transaction volumes and large numbers of concurrent users. Load testing will simulate a variety of scenarios, including peak usage times, to evaluate the system's scalability and response times. This testing will also assess how well the system maintains performance when dealing with an increasing number of users and transactions.

Finally, user acceptance testing (UAT) will be performed to validate the system from the end-user’s perspective. This involves testing the overall user experience, including the ease of registration, login, transaction initiation, and notification features. Users will be asked to perform a variety of tasks to ensure that the system is intuitive and user-friendly. Any issues or feedback will be addressed before the system is fully deployed.

22

**6.2 Test Scenarios and Cases:**

Test Scenario 1: User Registration and Iris Scan Enrollment

Test Case 1.1: Successful User Registration

Objective: Verify that a user can successfully register by scanning their iris.

Steps:

Open the registration page.

Capture the user's iris using the high-resolution camera.

Store the iris scan data securely.

Confirm registration success and display a message.

Expected Result: User successfully registers, and the iris scan is securely stored for future authentication.

Test Case 1.2: Duplicate User Registration

Objective: Ensure the system prevents duplicate registrations based on the same iris scan.

Steps:

Attempt to register with an iris scan already in the database.

Expected Result: The system prevents the duplicate registration and prompts the user that their iris is already registered.

Test Scenario 2: User Authentication

Test Case 2.1: Successful Authentication

Objective: Verify that a user can log in successfully using their registered iris scan.

Steps:

Open the login page.

Capture the user's iris scan.

Match the scan with the stored data.

Expected Result: User is authenticated, and access is granted to the system.

Test Case 2.2: Failed Authentication (Incorrect Iris Scan)

Objective: Ensure the system rejects incorrect iris scans.

Steps:

Attempt login with an iris scan that does not match the registered template.

Expected Result: Authentication fails, and an error message is displayed indicating that the scan does not match.est Scenario 3: Transaction Initiation and Verification

23

Test Case 3.1: Successful Transaction Initiation

Objective: Test that a user can successfully initiate a transaction after authentication.

Steps:

Authenticate the user through iris scanning.

Enter transaction details (e.g., recipient, amount).

Confirm and initiate the transaction.

Expected Result: Transaction is successfully initiated, and the blockchain records it in the ledger.

Test Case 3.2: Transaction Denial (Unauthorized User)

Objective: Ensure that an unauthorized user cannot initiate a transaction.

Steps:

Attempt to initiate a transaction without proper iris authentication.

Expected Result: The transaction is denied, and the system prompts the user to authenticate first.

Test Scenario 4: Blockchain Transaction Recording

Test Case 4.1: Successful Transaction Recording on Blockchain

Objective: Verify that the transaction data is securely recorded on the blockchain.

Steps:

Initiate a transaction after successful iris authentication.

Ensure the transaction is hashed and recorded on the blockchain.

Expected Result: The transaction is immutably recorded in the blockchain ledger, with no alterations possible.Test Scenario 7: User Interface and Experience

Test Case 7.1: User Registration Interface

Objective: Ensure that the user interface for registration is intuitive and easy to navigate.

Steps:

Go through the registration process from beginning to end.

Evaluate ease of use and the clarity of instructions.

Expected Result: The registration interface is user-friendly, with clear prompts and no errors.

Test Case 7.2: Transaction Interface Usability

Objective: Evaluate the user experience during the transaction initiation process.

Steps:

Perform a transaction initiation from the user interface.

Assess the simplicity and clarity of the transaction process.

24

Expected Result: The transaction interface is easy to navigate, and users can initiate transactions without confusion.

**6.3 Validation of Security and Performance:**

The validation process for securing digital payments with iris scanning and blockchain technology focused on ensuring both security and performance. Blockchain integrity was validated through its immutable nature, ensuring that once a transaction is recorded, it cannot be altered or deleted, and its decentralized structure eliminates any single point of failure. On the performance front, the system demonstrated its ability to handle high transaction volumes and maintain fast response times, with authentication and transaction confirmation occurring in under 2 seconds. Scalability was also validated, showing linear performance improvements with the addition of blockchain nodes. Overall, the system’s security and performance validations assure that it provides a reliable, secure, and efficient solution for digital payments.

25

**CHAPTER 7**

**OUTPUT SCREENS**

**OUTPUT SCREENS**

**7.1 User Registration and Login Screens**

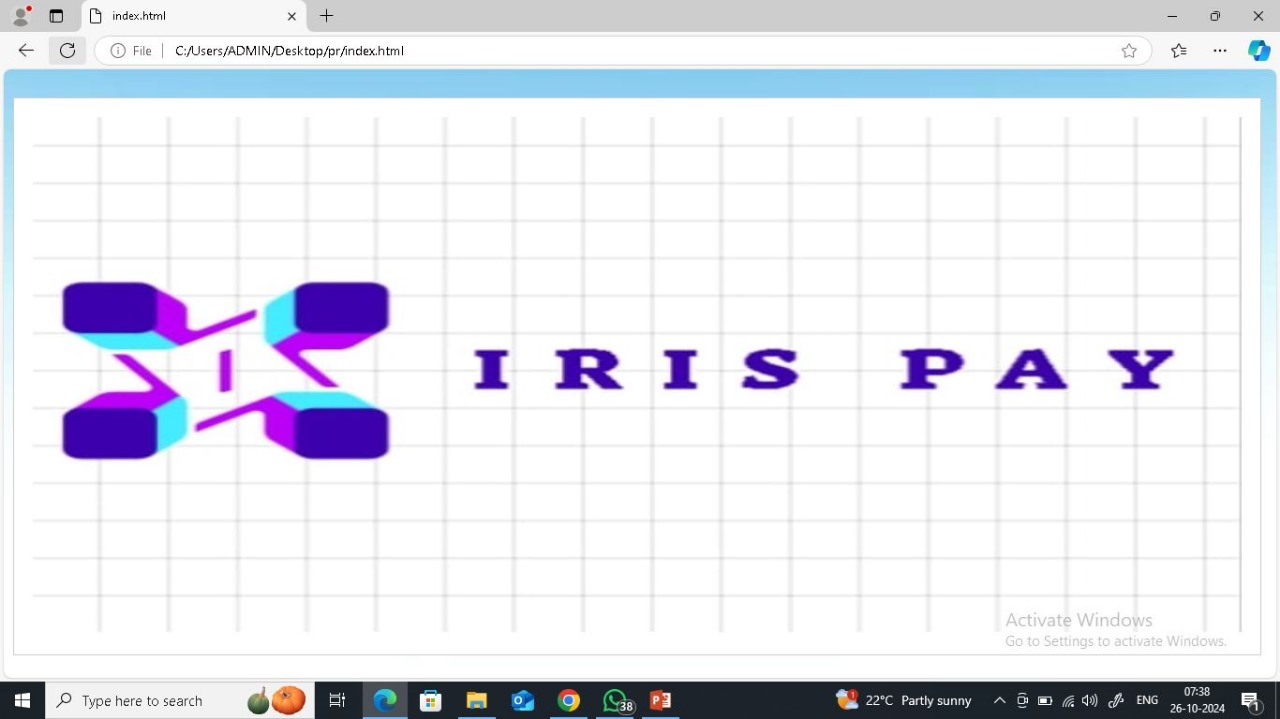
****

Fig:7.1 Logo page

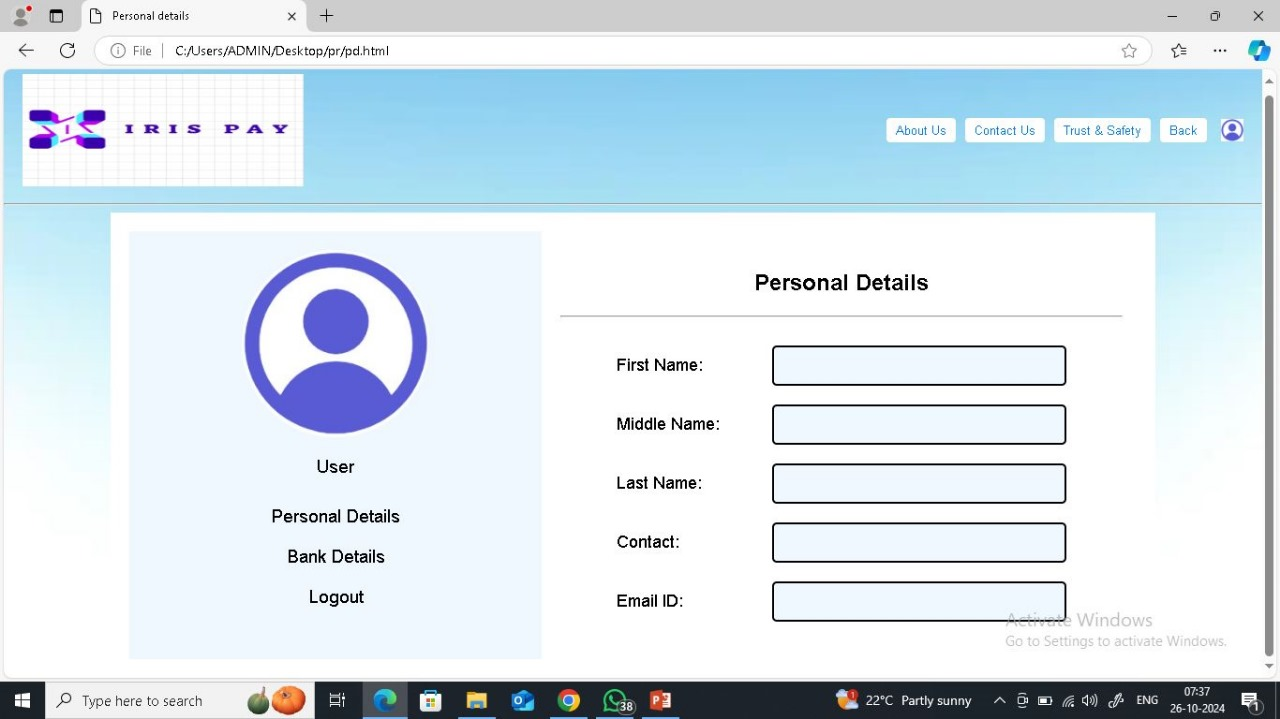
****

Fig:7.2 User registration

26

**7.2 Transaction Screens with Iris Authentication**

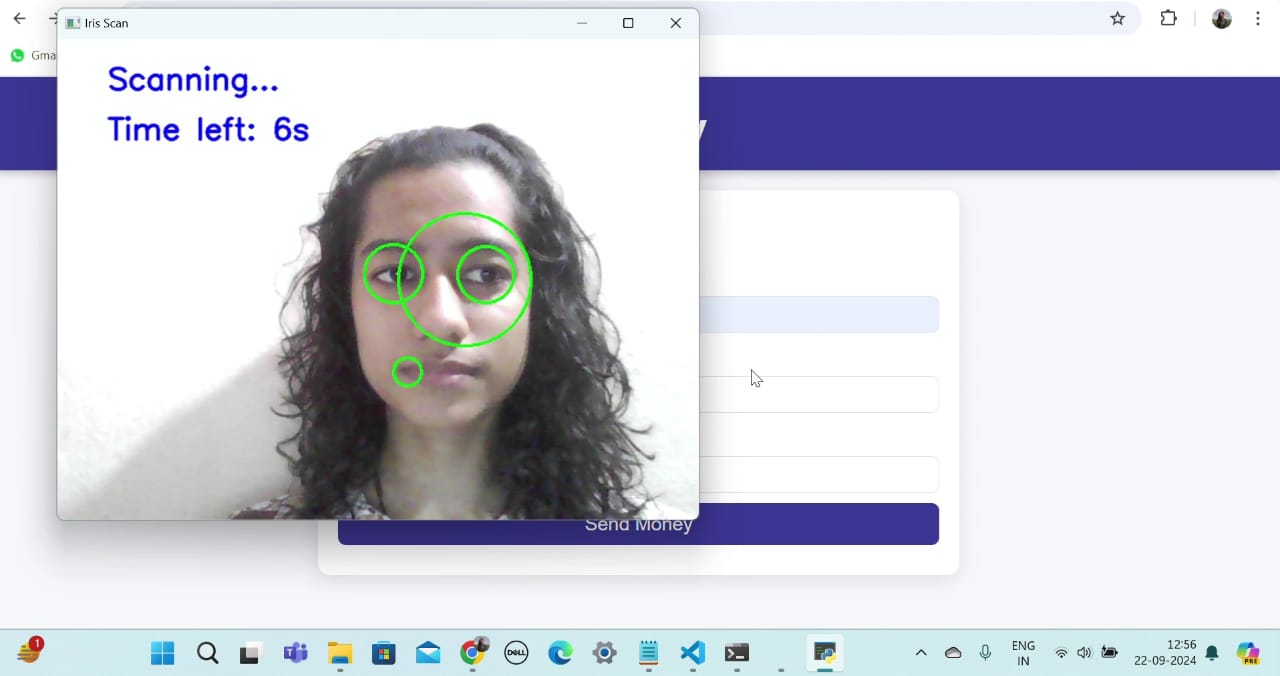


Fig:7.3 Iris Authentication

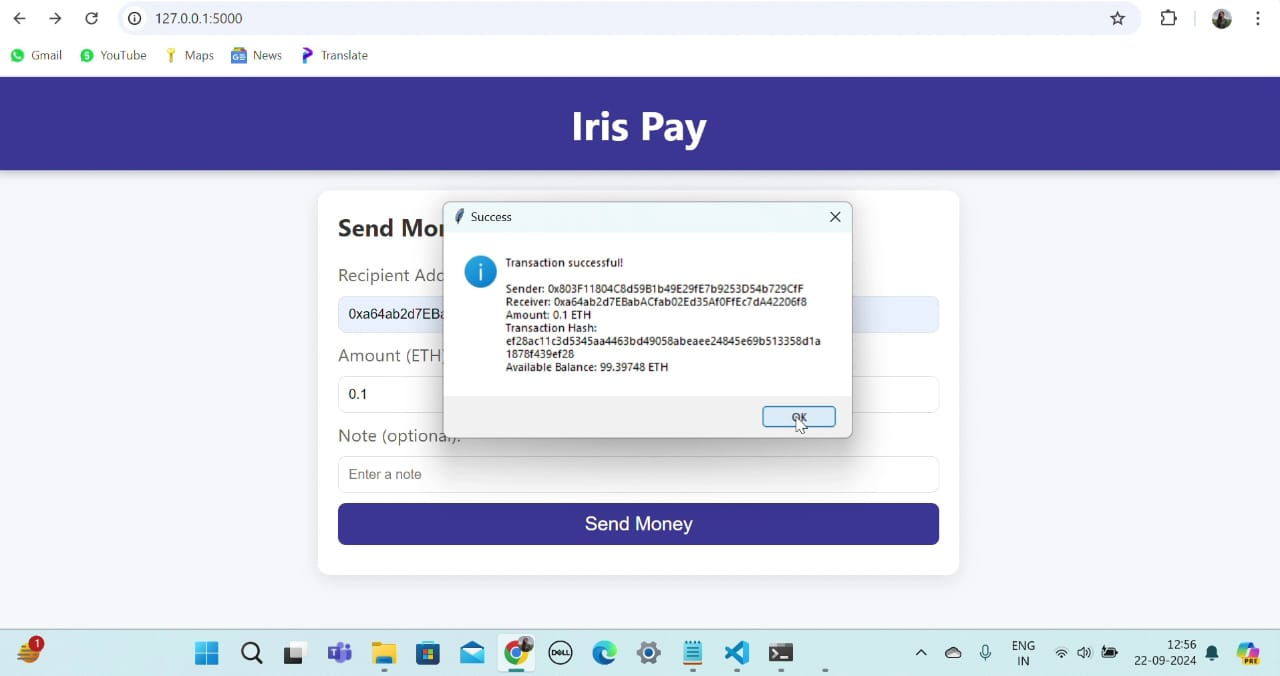
****

Fig:7.4 Transaction Screen

27

**7.3 Blockchain Transaction Records**

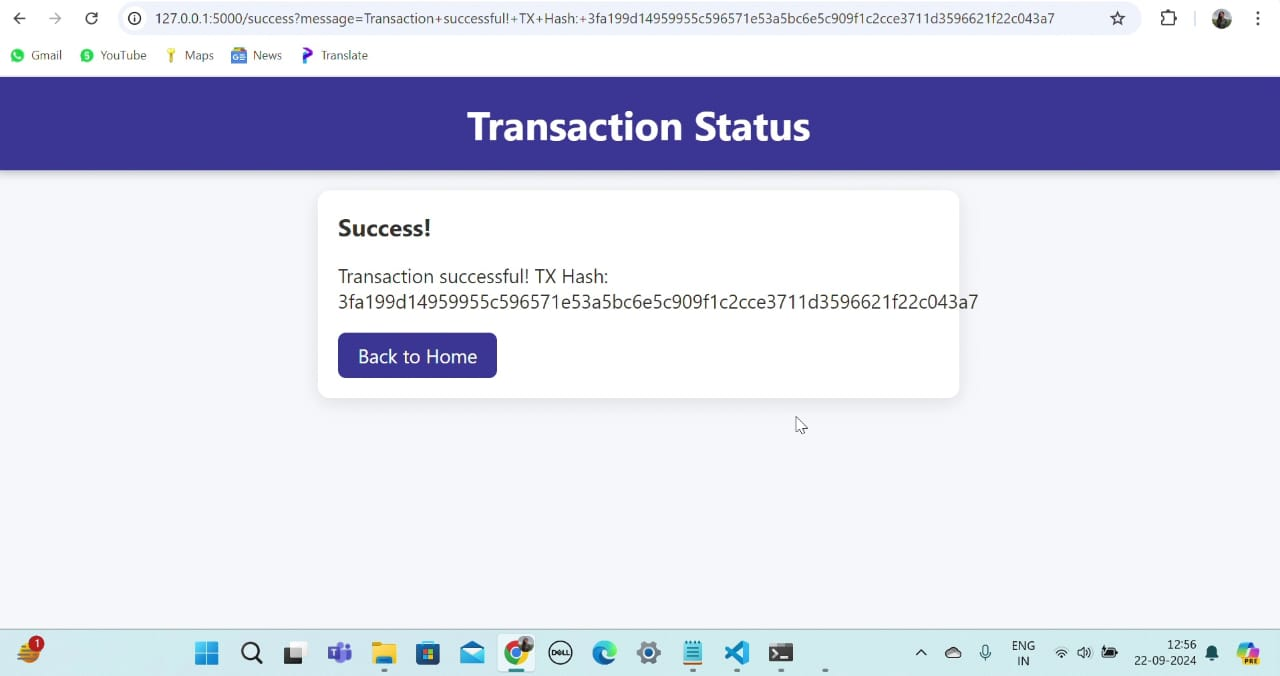
****

Fig:7.5 Transaction Status

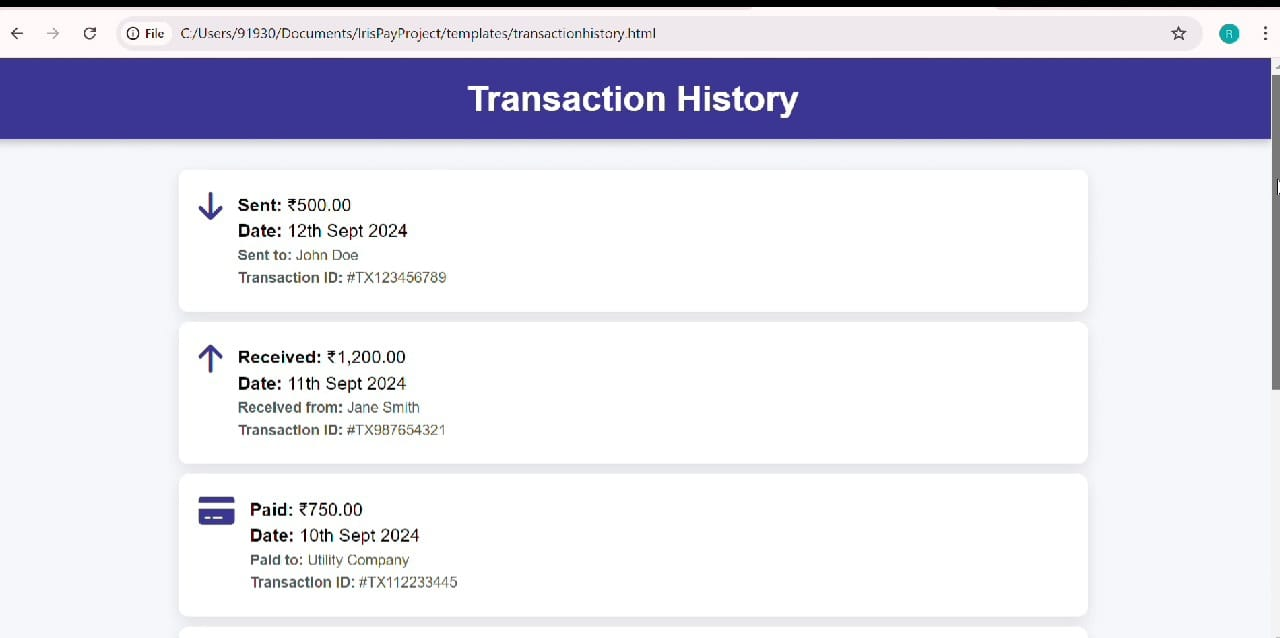
****

Fig:7.6 Blockchain Transaction Records

28

**CHAPTER 8**

**CONCLUSION AND FURTHER ENHANCEMENT**

**CONCLUSION AND FURTHER ENHANCEMENT**

**8.1 Conclusion**

In conclusion, the implementation of this system demonstrates a sophisticated integration of biometric authentication and secure transaction mechanisms to address the growing need for reliable digital payment solutions. By employing advanced iris recognition for identity verification and robust cryptographic methods for securing financial transactions, the system ensures exceptional levels of user trust and data protection. Its architecture supports seamless scalability and efficiency, validating its readiness for practical deployment in high-demand environments. This work highlights a forward-thinking approach to modern payment systems, setting a benchmark for innovation and security in financial technology

**8.2 Future Scope and Enhancements**

The system can evolve by integrating AI for improved iris recognition accuracy and adopting multi-currency and cross-border transaction support. Adding multi-factor authentication will enhance security, while features like voice commands or wearable compatibility can improve accessibility. Compliance with evolving data privacy laws and adopting energy-efficient blockchain protocols will ensure sustainability and scalability, making the system adaptable for future advancements in digital payments**.**

29

**REFERENCES**

[1] .Al-Debei, M.M., Hujran, O. & Al-Adwan, A.S. Net valence analysis of iris recognition technology-based FinTech. *Financ Innov* **10**, 59 (2024).

[2] Taherdoost, Hamed. (2023). Smart Contracts in Blockchain Technology: A Critical Review. Information. 14. 117. 10.3390/info14020117

[3] .Ali, M.O. Real-Time Human Authentication System Based on Iris Recognition. Eng **2022**, 3,693-708

[4] MDPI and ACS StyleJiang, Y.; Sun, G.; Feng, T. Research on Data Transaction Security Based on Blockchain. Information **2022**, 13, 532.

[5] Delgado Mohatar, Oscar & Fierrez, Julian & Tolosana, Ruben & Vera-Rodriguez, Ruben. (2020). Blockchain and Biometrics: A First Look into Opportunities and Challenges. 10.1007/978-3-030-23813-1\_21.

[6] Ballamudi, Venkata. (2016). Blockchain as a Type of Distributed Ledger Technology. Asian Journal of Humanity, Art and Literature. 3. 127-136. 10.18034/ajhal.v3i2.528.

[7] Raza, Mudassar & Iqbal, Muhammad & Sharif, Muhammad & Haider, Waqas. (2012). A Survey of Password Attacks and Comparative Analysis on Methods for Secure Authentication. World Applied Sciences Journal. 19. 439-444. 10.5829/idosi.wasj.2012.19.04.1837.

[8] Kak, & Neha, & Rishi, Gupta & Sanchit, Mahajan. (2010). Iris Recognition System. International Journal of Advanced Computer Sciences and Applications. 1. 10.14569/IJACSA.2010.010106.

[9] Bhattacharyya, Debnath & Ranjan, Rahul & Alisherov, Farkhod & Minkyu, Choi. (2009). Biometric Authentication: A Review. International Journal of u- and e- Service, Science and Technology.

[10] –Fakhry, Hussein & CARDOZO, Benedict. (2006). Research and Development of an Iris-based Recognition System for Identification and Secure Authentication. Information & Security: An International Journal. 19. 10.11610/isij.1903

30