A MINOR PROJECT REPORT

ON

VISON BASED ACCESS FOR FINANACIAL TRANSACTIONS

Submitted in partial fulfillment of the requirement

for the award of the degree of

BACHELOR OF TECHNOLOGY

IN

COMPUTER SCIENCE AND ENGINEERING

BY

BANOTH ASHOK	**21P61A0521**
DEVULAPALLI LIKITH	**21P61A0559**
DHANAVATH VIJAY	**21P61A0560**

Under the esteemed guidance of

MR.P.HANUMANTH RAO

Assistant Professor

Dept. of CSE

Counselling Code : VBIT

VIGNANA BHARATHI Institute of Technology

(A UGC Autonomous Institution, Approved by AICTE, Accredited by NBA & NAAC-A Grade, Affiliated to JNTUH)

VIGNANA BHARATHI INSTITUTE OF TECHNOLOGY

(A UGC Autonomous Institution, Approved by AICTE, Affiliated to JNTUH, Accredited by NBA & NAAC)

Aushapur (V), Ghatkesar (M), Medchal(dist)

2024 – 2025

Counselling Code : VBIT

VIGNANA BHARATHI Institute of Technology ®

(A UGC Autonomous Institution, Approved by AICTE, Accredited by NBA & NAAC-A Grade, Affiliated to JNTUH)

CERTIFICATE

This is to certify that the minor project titled “**VISON BASED ACCESS FOR FINANCIAL TRANSACTION**” submitted to the **Vignana Bharathi Institute of Technology**, affiliated to **JNTUH** by **Banoth Ashok (21P61A0521), Devulapalli Likith (21P61A0559), Dhanavath Vijay (21P61A0560)** in B. Tech IV-I semester **Computer Science and 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**
Mr.P.Hanumanth Rao	Dr.Raju Dara
Assistant Professor	Professor
Dept.of CSE	Dept.of CSE

EXTERNAL EXAMINER

Counselling Code : VBIT

VIGNANA BHARATHI Institute of Technology ®

(A UGC Autonomous Institution, Approved by AICTE, Accredited by NBA & NAAC-A Grade, Affiliated to JNTUH)

DECLARATION

We, **B.Ashok, D.Likith, D.Vijay** bearing hall ticket numbers **21P61A0521, 21P61A0559, 21P61A0560** hearby declare that the minor project report entitled **“VISON BASED ACCESSED FOR FINANCIAL TRANSACTIONS”** under the guidance of **MR.P.HANUMANTH RAO,** 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.

By:

BANOTH ASHOK (21P61A0521)

DEVULAPALLI LIKITH (21P61A0559)

DHANAVATH VIJAY (21P61A0560)

ACKNOWLEDGEMENT

The satisfaction that accompanies the successful completion of any task would be incomplete without the mention of the people who made it possible and whose encouragement and guidance has been a source of inspiration throughout the course of the project.

It is great pleasure to convey our profound sense of gratitude to our principal **Dr. P.V. S Srinivas**, **Dr. Raju Dara,** Head of the CSE Department, Vignana Bharathi Institute of Technology for having been kind enough for arranging the necessary facilities for executing the project in the college.

We would like to express our sincere gratitude to our Guide, **MR.P.HANUMANTH RAO,** Assistant Professor, **CSE Dept**, **Vignana Bharathi Institute of Technology,** whose guidance and valuable suggestions have been indispensable to bring about the completion of our project.

We wish to acknowledge special thanks to the Project Coordinators **Dr.N.Swapna,** Associate Professor of **CSE Dept and Mr.G.Arun**, Associate Professor of **CSE Dept**, **Vignana Bharathi Institute of Technology** for assessing seminars, inspiration, moral support and giving us valuable suggestions in our project.

We would also like to express our gratitude to all the staff members and lab faculty, department of **Computer Science and Engineering**, **Vignana Bharathi Institute of Technology** for the constant help and support.

We wish a deep sense of gratitude and heartfelt thanks to management for providing excellent lab facilities and tools. Finally, we thank all those whose guidance helped us in this regard.

ABSTRACT

In the era of digital banking and increasing financial transactions, ensuring secure, efficient, and user-friendly access mechanisms is paramount. Vision-based access systems leverage advanced technologies such as computer vision, biometric recognition, and machine learning to authenticate users through facial recognition, iris scanning, or gesture analysis. These systems enhance security by minimizing reliance on traditional methods like passwords or PINs, which are prone to theft and misuse.

Keywords:

Web-based ATM simulator, Facial recognition technology, User authentication, Banking tasks, Checking account balances, Transferring funds, Withdrawing case, Secure interface.

DEPARTMENT
OF
COMPUTER SCIENCE AND ENGINEERING

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 1: 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)

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.

LIST OF INPUT / OUTPUT SCREENS

TABLE OF CONTENTS

CHAPTER 1

Introduction

1.1 Overview of project:

The Vision-Based Access for Financial Transactions project aims to transform how people interact with financial systems by using facial recognition technology for secure and convenient access. Traditional methods like physical cards, PINs, or passwords are often prone to theft, loss, or misuse. This system replaces these outdated methods with facial authentication, ensuring only authorized users can access their accounts, reducing risks such as unauthorized access or identity theft. By eliminating the need for physical devices, the system allows users to log in and perform transactions with a simple face scan, making it both secure and user-friendly.

The system supports various banking services, such as checking account balances, transferring funds, viewing transaction history, and withdrawing or depositing funds virtually. It provides enhanced security through facial recognition, a biometric technology that is unique to each individual and cannot be easily guessed or stolen. Built with modern web development frameworks and advanced facial recognition APIs, the platform is designed for fast and efficient performance, ensuring a seamless user experience.

This innovative approach offers numerous benefits, including improved security, as biometric authentication minimizes fraud risks; convenience, as users no longer need to carry cards or remember PINs; and a future-ready design that leverages cutting-edge technology to meet modern financial needs. The system's intuitive web interface ensures accessibility for users of all experience levels, making it suitable for widespread adoption. Overall, this project delivers a secure, efficient, and user-centric financial service platform, aligning with the evolving demands of modern banking.

1.2 Problem statement:

The Vision-Based Access for Financial Transactions project addresses the growing challenges of security, convenience, and efficiency in the modern banking system. Traditional methods of accessing financial services, such as physical ATM cards, PINs, and passwords, have significant drawbacks. Cards can be lost or stolen, and PINs or passwords can be forgotten or guessed, leading to unauthorized access, fraud, and identity theft. These limitations create a need for a more reliable and user-friendly authentication method.

This project aims to solve these problems by introducing facial recognition as a means of authentication for financial transactions. Facial recognition is a biometric technology that leverages a person’s unique facial features, which cannot be easily replicated or stolen, to verify their identity. By eliminating the dependency on physical cards and PINs, this system provides a secure and intuitive solution that allows users to perform essential banking tasks like checking account balances, transferring funds, and withdrawing money. This approach not only enhances security but also streamlines the user experience by reducing the complexity of accessing financial services. Furthermore, the system’s integration with advanced facial recognition APIs and modern web development frameworks ensures it is fast, efficient, and capable of meeting the demands of today’s tech-savvy users.

1.3 AIM and OBJECTIVES:

Aim:

The aim of the **Vision-Based Access for Financial Transactions** project is to create a secure, efficient, and user-friendly system that uses facial recognition technology to authenticate users and enable them to perform financial transactions without relying on traditional methods like physical cards or PINs.

Objectives:

Enhance Security:

Use facial recognition technology to ensure only authorized users can access their accounts, reducing fraud and unauthorized transactions.

Eliminate Physical Dependence:

Remove the need for ATM cards, PINs, or passwords, providing a more convenient and reliable way to access financial services.

Simplify Banking Tasks:

Enable users to perform essential banking operations such as checking account balances, transferring money, and withdrawing funds through a seamless and intuitive interface.

Leverage Modern Technology:

Integrate advanced facial recognition APIs and web development frameworks to create a fast, accurate, and efficient authentication system.

Improve User Experience:

Provide a simple and accessible platform that caters to users of all technical skill levels, ensuring wide usability.

Promote Innovation:

Introduce a future-ready solution that aligns with modern digital banking trends and sets a benchmark for secure and convenient financial transactions.

1.4 Literature Survey:

1.Eigenfaces for Recognition: Description

Eigenfaces is a facial recognition technique that uses principal component analysis (PCA) to represent and analyze facial images in a reduced-dimensional space, emphasizing the essential features that distinguish one face from another. Developed in the early 1990s, Eigenfaces introduced a computationally efficient approach to facial recognition, leveraging linear algebra to identify patterns in high-dimensional image data**.**

2.Fisherfaces vs. Eigenfaces: Literature Survey

Eigenfaces and Fisherfaces are two prominent approaches in facial recognition that employ dimensionality reduction techniques, but they differ in their methodologies, focus, and performance under varying conditions. Below is a comparative description highlighting their features, strengths, and limitations.

3.Labeled Faces in the Wild: A Database for Studying Face Recognition in Unconstrained Environments

The Labeled Faces in the Wild (LFW) database is a landmark dataset in the field of facial recognition, designed to benchmark and evaluate algorithms performance in real-world, unconstrained settings. Released in 2007, it has become a standard resource for assessing facial recognition systems under challenging conditions.

4.DeepFace: Closing the Gap to Human-Level Performance

DeepFace is a seminal deep learning-based facial recognition system introduced by Facebook in 2014. It represents a significant leap toward achieving human-level performance in recognizing faces by leveraging deep convolutional neural networks (CNNs) and addressing the limitations of earlier feature-engineering approaches. This model marked a turning point in facial recognition research by demonstrating the effectiveness of deep learning in achieving robust and scalable solutions for face verification and recognition tasks.

5.FaceNet: A Unified Embedding for Face Recognition and Clustering

FaceNet, introduced by Google in 2015, is a groundbreaking facial recognition system that revolutionized the field by introducing a unified embedding approach. Unlike traditional models focused on classification or verification, FaceNet directly maps facial images into a compact Euclidean space, where distances between embeddings represent the similarity of faces. This innovation enables efficient face recognition, verification, and clustering, all within a single framework.

6.Deep Learning for Face Recognition

Deep learning has revolutionized face recognition by enabling automatic feature learning from raw image data, bypassing the need for handcrafted features. The ability of deep neural networks, particularly convolutional neural networks (CNNs), to extract hierarchical and discriminative features has made them the dominant approach in modern face recognition systems. This section explores the evolution, methodologies, and impact of deep learning in face recognition, as well as its performance on benchmark datasets.

7.Face Recognition: A Literature Survey

Face recognition has been a pivotal area of research in computer vision and pattern recognition for decades. Its applications range from security and surveillance to social media and human-computer interaction. Over time, face recognition methods have evolved from traditional approaches relying on handcrafted features to modern deep learning-based techniques that achieve near-human performance. This survey summarizes key milestones, methodologies, and advancements in face recognition research.

8.Adversarial Attacks and Defenses in Face Recognition

Adversarial attacks pose significant challenges to the reliability and security of face recognition systems. These attacks exploit vulnerabilities in deep learning models by introducing subtle, often imperceptible perturbations to input images, causing misclassifications or failures in recognition. As face recognition systems are widely deployed in critical applications like security, banking, and surveillance, the need for robust defenses has become paramount. This section explores the nature of adversarial attacks, their implications for face recognition, and countermeasures designed to mitigate these risks.

9.Defenses Against Adversarial Attacks in Face Recognition Systems

This survey focuses on the defense mechanisms developed to mitigate adversarial attacks in face recognition systems. The study categorizes defenses based on their approaches, such as preprocessing, adversarial training, and feature manipulation.

10.Security and Privacy Implications of Adversarial Attacks in Face Recognition

Adversarial attacks have raised serious concerns about the security and privacy of face recognition systems, especially as they are deployed in sensitive areas such as surveillance, border control, and law enforcement.

11.Transferable Attacks in Face Recognition Systems

This survey delves into the phenomenon of transferability in adversarial attacks, where an attack generated for one model can be effective on another model. Transferable attacks are a significant challenge because they can bypass defenses based on model-specific architectures.

12.Evaluation of Face Recognition Systems Under Adversarial Conditions

This survey evaluates the overall performance and reliability of face recognition systems when exposed to adversarial conditions. It compares different models' vulnerabilities and the effectiveness of various defense strategies, providing an empirical analysis of both attacks and countermeasures.

13.Advanced Adversarial Attacks in Face Recognition Systems

This survey explores advanced adversarial attack techniques specifically designed to target face recognition systems. It covers both well-known methods and cutting-edge innovations in adversarial machine learning that pose challenges to the field.

14.Ensemble Approaches for Robust Face Recognition Against Adversarial Attacks

This survey investigates the use of ensemble learning techniques as a defense against adversarial attacks in face recognition systems. Ensemble methods combine multiple models or classifiers to enhance robustness and accuracy, particularly in the face of adversarial perturbations.

1.5 Advantages of the project:

1. Better Security

Face recognition is harder to hack than passwords or PINs. It's tough to fake someone's face, so it's more secure than passwords that can be stolen or guessed.

2. Easy to Use

Users just need to look at the camera, no need to remember passwords.

3. Quick and Real-Time Access

Instant login and faster transaction approval with no delays. This speeds up transactions, so you don't waste time on authentication.

4. Reduced Fraud

Face recognition is difficult to fake, making fraud less likely.

5. Works on Multiple Devices

Can be used on phones, websites, or other devices with ease. It can work across different platforms, so users can access their accounts from different devices.

6. Affordable and Lightweight

Flask is cost-effective and the system runs on basic hardware.

7. Easily Integrates with Other Technologies

Supports AI tools and connects easily with banking systems.

8. Better Customer Experience

Simple and fast authentication builds trust with users. Customers feel more confident knowing their transactions are secured with advanced technology.

9. Privacy and Security

Data is encrypted and protected, ensuring privacy.

1.6 Applications

1. Banking Apps

Log into banking apps and authorize transactions securely using face recognition.

2. ATMs

Access ATMs and authorize withdrawals with face scans instead of cards or PINs.

3. Mobile Payments

Confirm mobile payments and access digital wallets using facial authentication.

4. E-Commerce

Speed up checkout and protect user accounts with face recognition for payment approval.

5. Insurance

Authenticate insurance claims and prevent fraud with face-based verification.

6. Government Services

Securely access tax filings, benefits, and other financial government services using face recognition.

7. Corporate Systems

Employees can access payroll and approve expenses through face-based authentication.

8. Investment Platforms

Secure login and transaction approval for stock trading platforms via facial recognition.

9. Cryptocurrency

Protect crypto wallets and authorize transactions using face recognition.

10. Healthcare Payments

Make medical bill payments and access health accounts with facial authentication.

CHAPTER 2

INNOVATIVE AUTHENTICATION

2.1 Introduction

As digital transactions become more common, securing financial accounts has become a major concern. Traditional methods like passwords and PINs are vulnerable to hacking and theft. To address this, **Vision-Based Access for Financial Transactions** uses **face recognition** to provide a more secure and convenient way for users to access their financial accounts and authorize transactions.

Built with the lightweight **Python Flask** framework, this system allows users to log in, approve payments, and perform financial actions with just a facial scan. It enhances security by reducing the risk of fraud while improving user experience by eliminating the need for passwords.

This system offers a future-proof solution to digital authentication, making it easier, faster, and more secure to conduct financial transactions, while also setting the stage for more advanced biometric technologies.

2.2 Overview of Innovative Authentication:

We use **face recognition** as an innovative way to authenticate users. Unlike traditional methods like passwords or PINs, face recognition offers a more secure and user-friendly approach. Since each person's face is unique, it provides a much stronger form of identification that's harder to hack or steal. Users simply need to look at the camera to log in or approve transactions, making the process faster and more convenient. This system improves security by making it difficult for unauthorized users to access accounts, and it works in real-time, ensuring quick and seamless authentication. Overall, face recognition offers an easy-to-use, secure, and efficient way to protect sensitive financial information while enhancing the user experience.

CHAPTER 3

ENHANCED SECURITY

3.1 Introduction:

As more people use digital banking and online financial services, securing accounts and transactions has become a major concern. Traditional security methods like passwords and PINs can be easily hacked or stolen, leading to identity theft and fraud. To solve this problem, our **Vision-Based Access for Financial Transactions** project uses **face recognition** technology to securely authenticate users. With this system, users can log in and approve transactions just by looking at the camera, offering a safer and easier way to access financial services.

3.2 Overview of Enhanced Security:

The **enhanced security** in our project comes from using **face recognition** instead of traditional passwords or PINs. Since each person's face is unique, it provides a much stronger form of protection. This makes it nearly impossible for hackers to access accounts or steal personal information. The system also includes features like **liveness detection**, which prevents fraudsters from using photos or videos to trick the system. All data, including face scans, is securely encrypted to protect users' privacy. Overall, face recognition offers a safer, more reliable way to secure financial transactions while also being more convenient for users.

The system also includes advanced **anti-spoofing** features, such as **liveness detection**, which prevents hackers from using photos or videos to trick the system. Additionally, all data, including biometric information, is transmitted securely using encryption, ensuring that users' personal data remains protected.

With face recognition, security is not only enhanced, but it's also more convenient. Users no longer need to remember complex passwords or worry about password theft. This system provides a **stronger, safer, and more convenient** way to protect sensitive financial transactions, making it a highly effective solution for today's digital security challenges.

CHATPER 4

FASTER TRANSACTIONS

4.1 Introduction

In today’s fast-paced world, efficiency is key, especially when it comes to financial transactions. Traditional authentication methods like entering passwords or PINs can be time-consuming and create delays in completing transactions. Our **Vision-Based Access for Financial Transactions** project addresses this issue by using **face recognition** for quick and seamless authentication. Users can log in and approve payments in seconds, speeding up the entire transaction process. This technology not only makes financial services more efficient but also enhances the overall user experience by reducing waiting times and simplifying the process.

4.2 Overview of Faster Transactions

Our **project** enhances the speed and efficiency of financial transactions by utilizing **face recognition** technology for **instant authentication**. Traditional authentication methods like typing passwords, entering PINs, or waiting for one-time passcodes (OTPs) can slow down the process and create unnecessary delays, especially when users are in a hurry. With face recognition, users no longer need to remember passwords or go through multiple security steps. Instead, authentication happens almost **instantly**—a simple **face scan** is all it takes to verify the user and authorize a transaction.

The **real-time authentication** process ensures that users can quickly access their accounts and authorize payments without any interruptions or time-consuming actions. Whether it's transferring money, paying bills, or confirming online purchases, the system dramatically speeds up every transaction step. By reducing the time spent on logging in and verifying actions, users can complete financial tasks in a fraction of the time compared to traditional methods.

Moreover, this **seamless process** removes friction from the user experience, making digital banking, e-commerce, and other financial activities much more efficient. **Face recognition** not only provides security but also enhances convenience by streamlining the entire process—leading to faster decision-making and smoother transactions overall. This makes the system particularly beneficial for people on the go, businesses needing quick payment processing, and anyone looking for a more efficient way to handle their financial activities.

CHAPTER 5

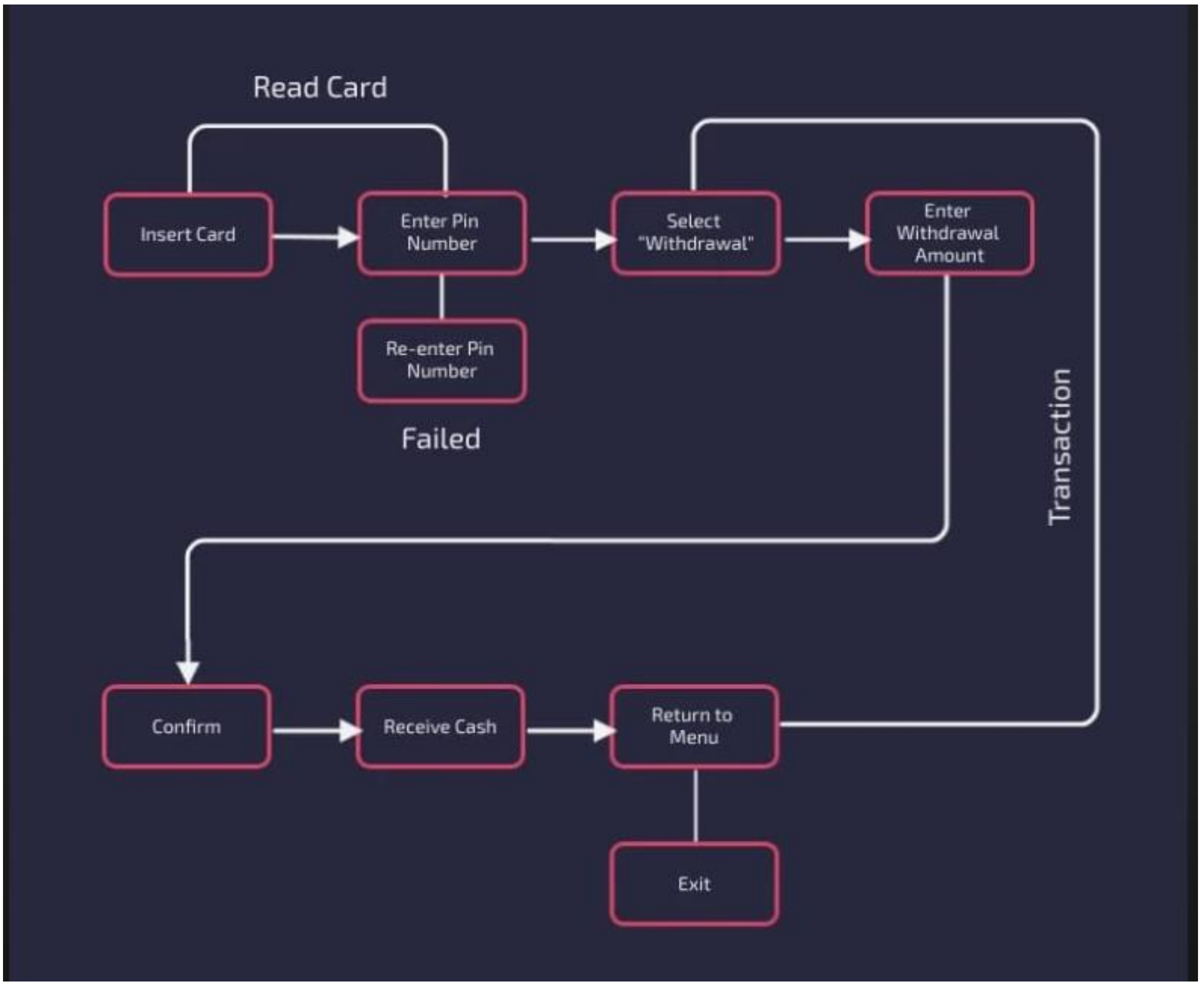
EXISTING METHOD

5.1 Introduction:

Previous ATM simulator projects have largely been console-based, offering a basic, text-driven interface that lacks visual appeal and interactive features. These early models primarily focus on simulating fundamental banking operations through command-line interfaces, with no provision for graphical user interfaces (GUIs) or advanced security features. As a result, they often miss out on providing a realistic and engaging user experience.

Additionally, these traditional simulators do not incorporate modern security technologies such as facial recognition. User authentication in earlier models is typically handled through basic text input for PINs or account numbers, which does not address contemporary security concerns or provide a seamless user experience.

5.2 Existing Method Block Diagram



The diagram illustrates the typical workflow of an ATM transaction. It begins with the insertion of an ATM card, followed by the input of a PIN for account verification. Upon successful verification, the user is presented with a menu of options, including cash withdrawal, deposit, transfer, and balance inquiry. Selecting an option prompts the ATM to guide the user through the specific steps for that action. Once the transaction is complete, the ATM ejects the card and dispenses the requested cash, if applicable.

5.3 Limitations of this Method:

1.Dependence on Card and PIN:
If the card is damaged or lost, the user cannot access the service. A forgotten PIN prevents the transaction.

2.Security Risks:
PIN theft (e.g., via shoulder surfing or skimming devices) could lead to unauthorized transactions. Stolen or cloned cards pose a security threat.

3.Insufficient Balance:
The transaction fails if the account lacks sufficient funds, which may inconvenience the user.

4.Technical Issues:
Machine malfunctions (e.g., card reader errors, cash dispenser issues) can disrupt the process. Network or server downtime may prevent transactions.

5.Limited User Authentication:
The system relies solely on a PIN for authentication, which is less secure compared to advanced methods like biometrics.

6.Transaction Limits:
Daily withdrawal limits may restrict the amount a user can withdraw, even if they have sufficient funds.

7.Fraud and Errors:
The machine may dispense the wrong amount due to mechanical or software errors.

CHAPTER 6

PROPOSED METHOD

6.1 To overcome the limitations in Existing Method:

The project involves creating a web-based ATM simulator with facial recognition for secure user authentication. The development includes designing an intuitive graphical interface using HTML, CSS, and JavaScript, and integrating facial recognition.

On the backend structured database stores user profiles and transaction history with strong encryption for data protection. After integration and thorough testing, the application is deployed, monitored, and maintained for performance and security.

6.2 Tools Required

Minimum Hardware Requirements

Ethernet/Wi-Fi module for online operations.

720p HD webcam for basic facial recognition testing.

Minimum Software Requirements

VS code ide

Frontend Technologies: HTML, CSS, Javascript

Backend Technologies: Python, PHP

Libraries: face recognation and dlib

Database Management System (DBMS): MySQL

6.3 Steps in the Algorithm

Start:
Initialize the system and prepare for input.
Capture Input:
Use a camera to capture the user's biometric data (e.g., face image or video).

Preprocessing:
Enhance the captured image by adjusting for lighting, size, and clarity.
Remove background noise to focus on the relevant features.

Feature Extraction:
Extract unique biometric features, such as facial landmarks (eyes, nose, mouth).
Use machine learning or computer vision techniques for feature identification.

Authenticate User :
Compare the extracted features with the biometric templates stored in a secure database.

If a match is found:
Proceed to the next step.

If no match is found:
Deny access and terminate the process.

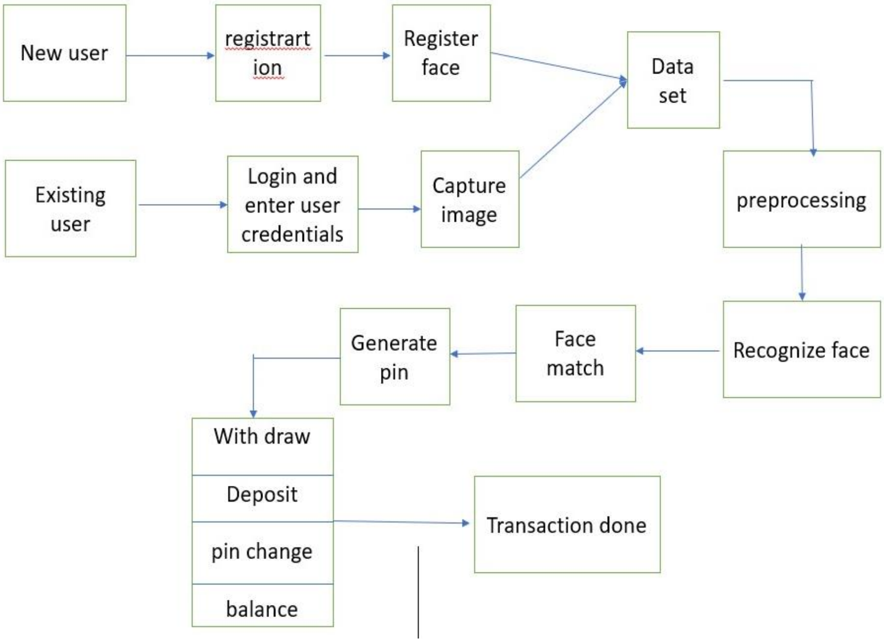
User Verification:
Verify the user’s intent and confirm their identity for the transaction.

Transaction Details:
Allow the user to input financial transaction details (e.g., amount, recipient).
Verify the provided details for correctness.

Approve Transaction:
Perform final checks, such as account balance verification and fraud detection.
If all checks pass, authorize the transaction.

Complete Transaction:
Display the transaction success message to the user.
Record the transaction details in the database for future reference.

6.4 Block Diagram:

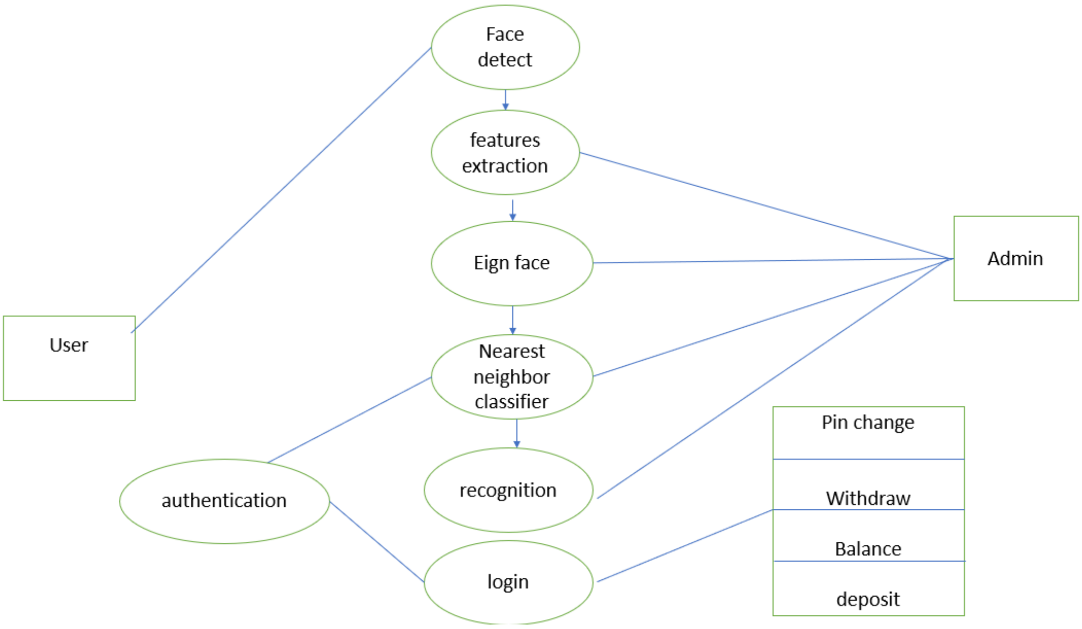


The diagram illustrates a system likely used for secure financial transactions. It starts with user authentication. New users register by providing their information and capturing their face for recognition. Existing users log in with their credentials.

Once authenticated, the system captures the user's face image and compares it with a stored dataset. If the match is successful, the user can proceed with transactions like withdrawal, deposit, or PIN change. After each transaction, the system records it as "Transaction Done.

This system ensures that only authorized individuals can access and perform financial operations, adding an extra layer of security with facial recognition.

6.5 use case diagram



The given diagram outlines a facial recognition and authentication system. The process begins with capturing a user's face, followed by detecting and extracting key facial features. These extracted features are then compared to a database of known faces using techniques like Principal Component Analysis (PCA). The system employs a nearest neighbour classifier to identify the closest match and authenticate the user. Once authenticated, the user can perform various actions such as changing their PIN, withdrawing funds, checking their balance, or making deposits. Additionally, an administrator can manage user accounts and system settings. This system finds applications in diverse fields, including security systems, biometric authentication, and facial recognition software.

6.6 Advantages of this Project

1. Enhanced Security

Biometric authentication, like facial recognition, ensures that only authorized users can access financial accounts.

Prevents unauthorized access, even if login credentials (e.g., passwords or PINs) are stolen.

2. Contactless and Hygienic

Vision-based systems are contactless, eliminating the need to touch surfaces like PIN pads or fingerprint scanners.

Promotes hygiene, especially in public settings or during pandemics.

3. Faster Transactions

Biometric verification is quick, reducing the time required for authentication compared to traditional methods like entering a PIN or password.

4. Convenience

Users do not need to remember passwords, PINs, or carry physical cards for authentication.

Accessible to users of all ages and abilities (with proper design).

5. Fraud Prevention

Reduces risks of card cloning, password phishing, or PIN theft since the system relies on unique biometric data.

Difficult for fraudsters to replicate facial features or other vision-based biometrics.

6. Increased User Confidence

Provides users with a sense of security, knowing their transactions are protected by advanced technology.

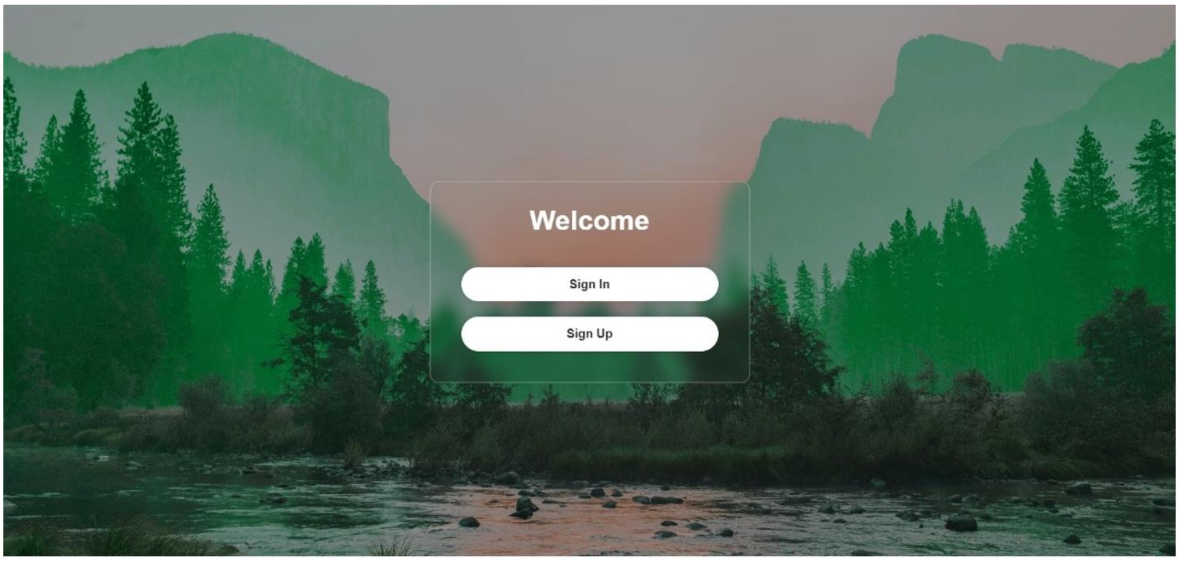
7. Integration with Advanced Technologies

Can be combined with Artificial Intelligence (AI) for fraud detection, ensuring even higher levels of security. Supports multi-factor authentication when paired with other systems like OTPs (One-Time Passwords).

CHAPTER 7

SIMULATIONS

7.1 Home page:

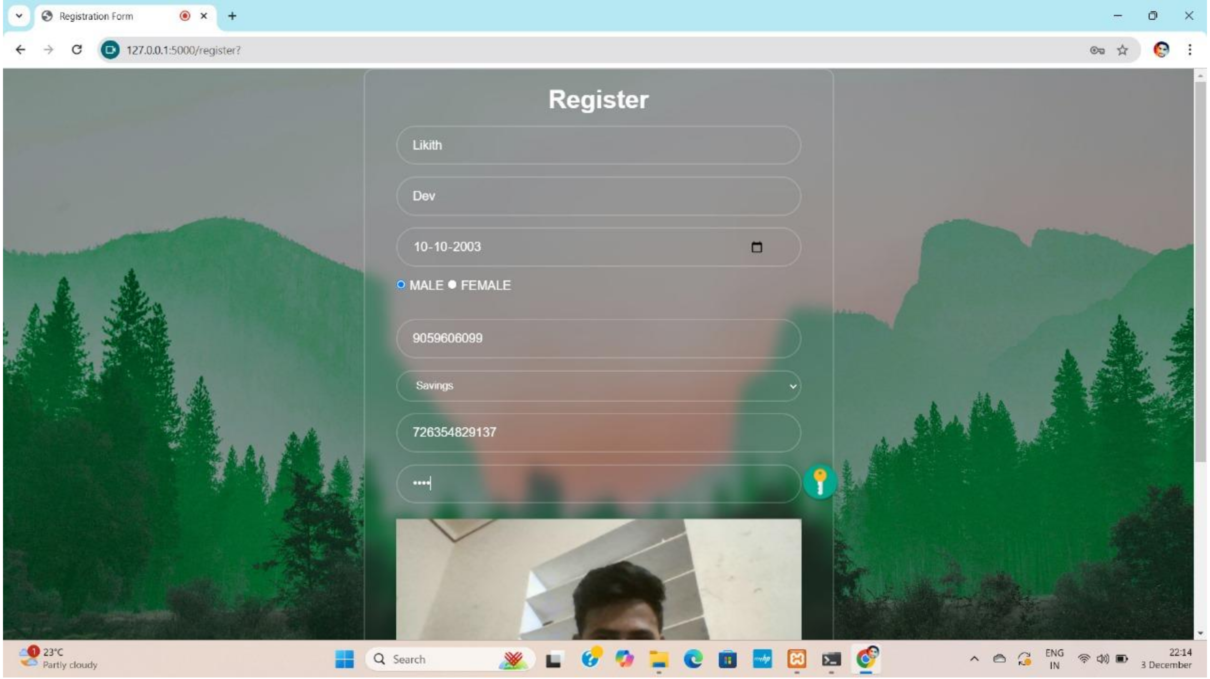


The above picture shows a webpage with two buttons, "Sign In" and "Sign Up." These buttons would typically be part of a user authentication system:

"Sign In" Button: This button is for users who have already registered. Clicking it would prompt the user to enter their credentials (usually username/email and password) to log into their account.

"Sign Up" Button: This button is for new users who have not registered yet. When clicked, it would open a registration form where users can enter their details (such as name, email, password, etc.) to create a new account.

7.2 Registration page



Register

Likith

Dev

10-10-2003

◉ MALE ○ FEMALE

9059606099

Savings

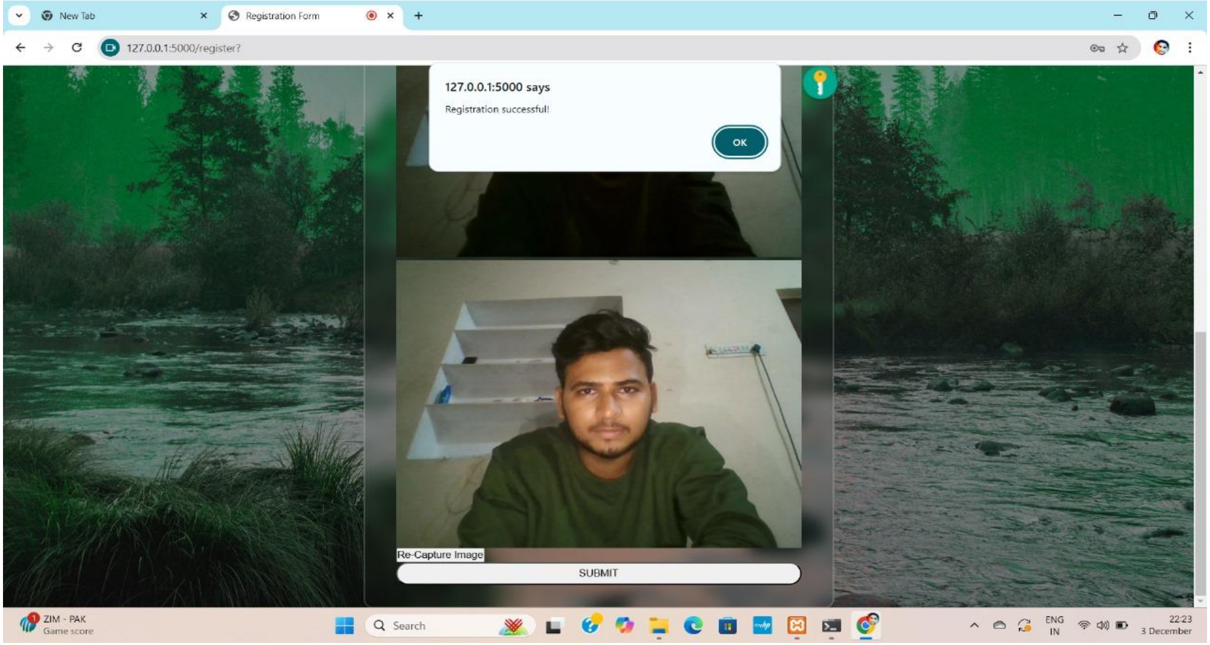
726354829137

••••

The above picture show the webpage after tapping on the button “Sign Up” registration process that involves both entering personal details and capturing a facial image for verification.

A button labeled **"Capture"** allows the user to take a photo of their face using the device’s camera

Once we capture image of user we can directly use the captured image as the facial authentication for the user or we can also have option to **recapture** the image of user in case captured image is having any problem or not of good quality



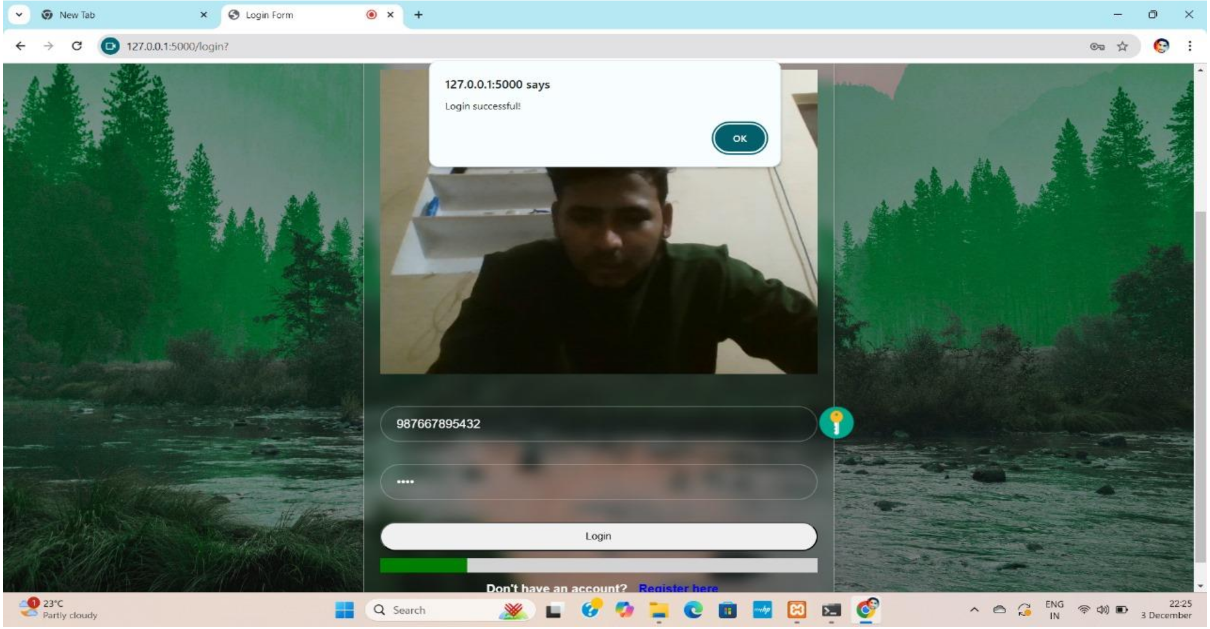
127.0.0.1:5000/register?

127.0.0.1:5000 says

Registration successful!

Once the form is successfully submitted, a pop-up message will appear, saying 'Registration Successful.' This confirms that the registration process has been completed.

7.3 Login page:



127.0.0.1:5000/login?

127.0.0.1:5000 says

Login successful!

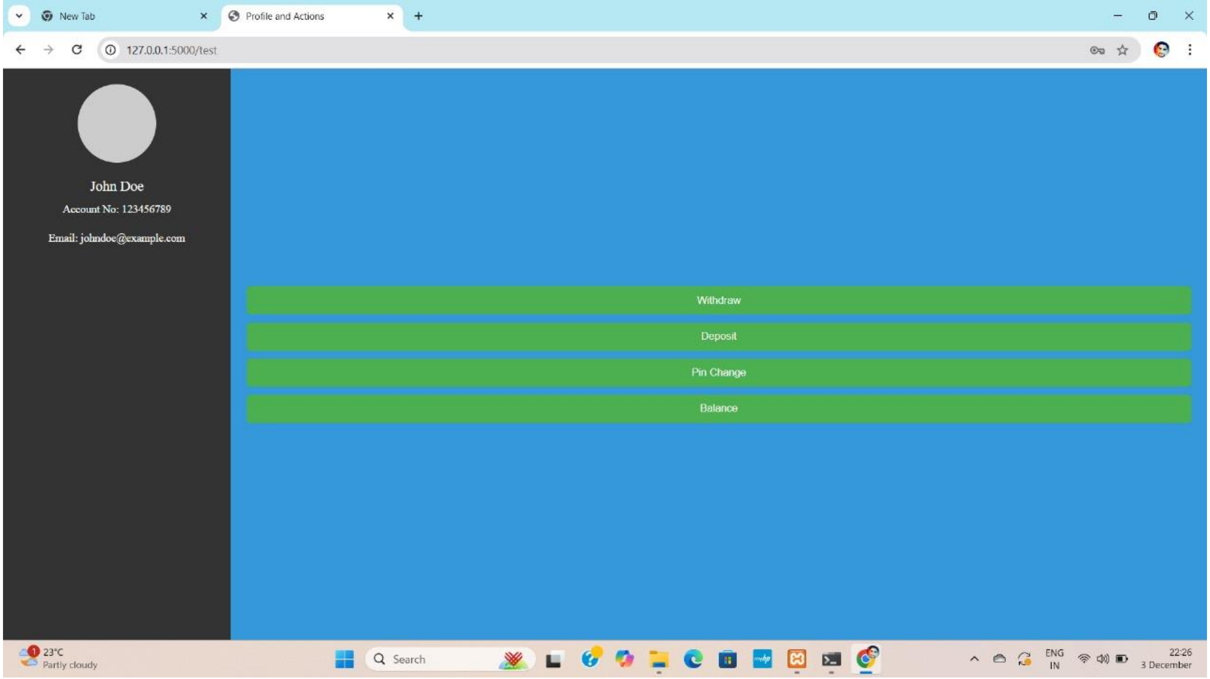
987667895432

••••

Don't have an account? Register here

The above picture shows the login page, which appears after clicking on the 'Sign In' button on the first webpage. You can log in by entering your account number and PIN, along with face verification using the webcam. After successfully logging in, a 'Login Successful message will appear, and you will be redirected to the required home page.

7.4 Final output



New Tab

Profile and Actions

127.0.0.1:5000/test

John Doe

Account No: 123456789

Email: johndoe@example.com

This is the final page after completing the sign-in verification. Once the login is successful, the user is redirected to this page, where they can access the features and services of the application or website.

This page provide the us the basic functionalities of banking transactions like pin generation, deposit, withdraw, balance checking etc.

CHAPTER 8

FUTURE SCOPE

1. Integration with Blockchain Technology

Blockchain ensures a tamper-proof record of transactions, enhancing data integrity and security.
It enables transparent financial processes, fostering trust among users and stakeholders.

2. Fraud Detection with AI

AI algorithms can identify suspicious patterns and anomalies in transactions, flagging potential fraud instantly.
Machine learning improves detection accuracy over time, reducing false positives and protecting users.

3. Multi-Modal Biometric Authentication

Combining facial recognition with fingerprints or voice adds an additional layer of authentication, making it harder to breach.
Multi-modal systems enhance reliability by verifying identity through multiple biometric markers.

4. Support for Mobile Devices, Wearables, and IoT Platforms

The system's adaptability across smartphones, smartwatches, and IoT devices increases convenience for users.
It ensures seamless integration into daily life, providing secure access anywhere, anytime.

CHAPTER 9

CONCLUSION

Vision-Based Access for Financial Transactions provides a secure, efficient, and user-friendly solution for modern banking needs. By leveraging advanced biometric technologies like facial recognition, this system ensures robust authentication, reducing the risks of fraud and unauthorized access. Its contactless nature promotes hygiene and convenience, making it highly suitable for public and remote financial operations.

Additionally, the integration of AI and machine learning further enhances its accuracy and scalability, making it a viable replacement for traditional methods such as PINs and passwords. Overall, this innovative approach is a step forward in ensuring secure and seamless financial transactions in the digital age.

CHAPTER 10

REFERENCES

1. Facial-Recognition Payment: An Example of Chinese Consumers, Wen Kun Zhang ; Min Jung Kang, IEEE Access, Year: 2019
2. Secure multifactor authentication payment system using NFC, Anirudhan Adukkathayar ; Gokul S Krishnan ; Rajashree Chinchole, 2015 10th International Conference on Computer Science & Education (ICCSE)
3. Biometric Face Recognition Payment System, Surekha. R. Gondkar Saurab. Dr. C. S. Mala International Journal of Engineering Research & Technology NCESC - 2018 Conference Proceedings
4. Facial Recognition in Banking – Current Applications, Niccolo Mejia,2019 Conference Proceedings
5. "Face Detection and Recognition for Bank Transaction ", International Journal of Emerging Technologies and Innovative Research, Sudarshan Dumbre,Shamita Kulkarni ,Devashree Deshpande ,P.V.Mulmule Journal of Emerging Technologies and Innovative Research 2018
6. Continuous User Identity Verification Using Biometric Traits for Secure Internet Services,Dr. SHAIK ADBUL MUZZER, 2GOSALA SUBHASIN
7. Face Detection and Recognition for Bank Transaction, Sudarshan Dumbre1, Shamita Kulkarni2, Devashree Deshpande3,Prof P.V.Mulmule4