**FACE RECOGNITION ATM SYSTEM**

**Project report in partial fulfillment of the requirement for the award of the degree of**

**Bachelor of Technology**

**In**

**Computer Science & Engineering**

**Submitted By**

Aratrik Banerjee Enrollment No. 12021002001230

Samriddhi Guha Enrollment No. 12021002001220

Shameek De Enrollment No. 12021002001064

Swapnaneel Bose Enrollment No. 12021002001122

Sayak Bhattacharjee Enrollment No. 12021002001139

Subhojit Chakraborty Enrollment No. 12021002001195

Argha Ghosh Enrollment No. 12021002001210

Debangshu Bhowmick Enrollment No. 12021002001194

Akash Chowdhury Enrollment No. 12021002001218

Pratiyush Singh Enrollment No. 12021002001262

**Under the guidance of**

Prof. Sumit Anand.

Department of Computer Science & Engineering



UNIVERSITY OF ENGINEERING & MANAGEMENT, KOLKATA

University Area, Plot No. III – B/5, New Town, Action Area – III, Kolkata – 700160.

**CERTIFICATE**

This is to certify that the project titled **Face Recognition ATM System** submitted **Aratrik Banerjee** (University Roll No. 12021002001230), **Swapnaneel Bose** (University Roll No. 12021002001122), **Subhojit Chakraborty** (University Roll No. 12021002001195), **Argha Ghosh**(University Roll No. 12021002001210), **Sayak Bhattacharjee**(University Roll No. 12021002001139), **Pratiyush Singh** (University Roll No. 12021002001262), **Debangshu Bhowmick**(University Roll No. 12021002001194), **Akash Chowdhury**(University Roll No. 12021002001218), **Shameek De**(University Roll No. 12021002001064) and **Samriddhi Guha**(University Roll No. 12021002001) students of **UNIVERSITY OF ENGINEERING & MANAGEMENT, KOLKATA**, in partial fulfillment of requirement for the degree of Bachelor of Computer Science and Engineering, is a bonafide work carried out by them under the supervision and guidance of **Prof. Sumit Anand** during **6th Semester** of academic session of 2023-2024. The content of this report has not been submitted to any other university or institute. I am glad to inform that the work is entirely original and its performance is found to be quite satisfactory.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Signature of Guide

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Signature of Head of the Department

**ACKNOWLEDGEMENT**

We would like to take this opportunity to thank everyone whose cooperation and encouragement throughout the ongoing course of this project remains invaluable to us.

We are sincerely grateful to our guide Prof. Sumit Anand of the Department of Computer Science & Engineering, UEM, Kolkata, for his wisdom, guidance and inspiration that helped us to go through with this project and take it to where it stands now.

Last but not the least, we would like to extend our warm regards to our families and peers who have kept supporting us and always had faith in our work.

Aratrik Banerjee

Samriddhi Guha

Shameek De

Swapnaneel Bose

Sayak Bhattacharjee

Subhojit Chakraborty

Argha Ghosh

Debangshu Bhowmick

Akash Chowdhury

Pratiyush Singh

**TABLE OF CONTENTS**

**ABSTRACT.................................................................................. 5**

**INTRODUCTION................................................................................... 6**

**PROBLEM STATEMENT .................................................................... 7**

**PROPOSED SOLUTION ....................................................................... 8**

**EXPERIMENTAL SETUP AND RESULT ANALYSIS**

* **Experimental Setup................................................................. 9**
* **Program Snapshot .................................................................. 10**

**DATA FLOW DIAGRAM.......................................................................... 13**

**CONCLUSION & FUTURE SCOPE........................................................ 14**

**BIBLIOGRAPHY ....................................................................................... 15**

**ABSTRACT**

In today's world, where security risks are ever-present, the reliability of traditional methods like PINs and cards can seem outdated and vulnerable. Enter face authentication: a cutting-edge solution that utilizes the distinct features of your face to securely and conveniently verify your identity. Our project focuses on two-factor authentication, combining face ID with account numbers to ascertain the rightful owner of each account.

Built using Python libraries such as tkinter and pillow for image insertion, along with MySQL connector modules for database connectivity, our project simplifies the authentication process while ensuring robust security measures. Through machine learning implemented in Python, facial recognition technology is seamlessly integrated into our system.

With face authentication, the hassle of remembering complex PINs or worrying about losing your card becomes a thing of the past. A simple glance at the ATM camera grants access to your account, promising a revolution in how we interact with ATMs.

Beyond convenience, our project emphasizes inclusivity. For individuals with disabilities or those struggling with traditional authentication methods, face authentication provides a much-needed solution, ensuring accessibility to banking services for all.

Addressing privacy and data security concerns, we have implemented stringent measures to safeguard customer data and ensure ethical use of facial recognition technology.

**INTRODUCTION**

In today's fast-paced world, technology is constantly evolving, and so are the security needs of the banking industry. That's why we're excited to introduce a groundbreaking solution: face authentication in ATMs. This innovative approach marks a significant shift in how we ensure security and streamline the banking experience for our customers.

Traditionally, accessing ATM services has relied on remembering PINs and carrying physical cards. But let's face it, these methods aren't foolproof. PINs can be forgotten or stolen, and cards can be easily misplaced or skimmed. That's where face authentication steps in, offering a more secure and convenient alternative.

Picture this: instead of fumbling for your card or trying to remember a complex PIN, you simply look at the ATM camera. Behind the scenes, advanced facial recognition algorithms analyze your unique facial features to confirm your identity. It's quick, it's seamless, and most importantly, it's secure.

By integrating face authentication into ATMs, we're not just improving security; we're also enhancing the overall user experience. No more worrying about forgetting your PIN or losing your card. Transactions become smoother and more efficient, allowing you to get in and out of the ATM in record time.

But perhaps most importantly, face authentication has the potential to make banking services more accessible to everyone. For individuals with disabilities or those who struggle with traditional authentication methods, this technology provides a much-needed solution. It's about creating an inclusive banking experience that caters to the needs of all our customers.

Of course, we understand that with any new technology comes concerns about privacy and data security. That's why we've implemented stringent measures to protect customer data and ensure that facial recognition technology is used responsibly.

**PROBLEM STATEMENT**

In contemporary security systems, traditional methods relying on cards and PINs for authentication are encountering significant limitations, necessitating a more robust and convenient solution. The following issues highlight the inadequacies of the conventional card and PIN-based systems:

1. Security Vulnerabilities:

* Traditional card-based systems are susceptible to theft, loss, or unauthorized duplication of cards. PINs, though ostensibly secure, can be compromised through various means such as shoulder surfing or brute-force attacks.
* PINs can be easily forgotten or shared, compromising the integrity of the authentication process and leading to unauthorized access.

1. Ease of Unauthorized Access:

* Theft or loss of a physical card can result in unauthorized access to sensitive areas or systems. Even if a PIN is required along with the card, it can be easily guessed or obtained through social engineering tactics.

1. Limited Scalability:

* Traditional card and PIN-based systems face challenges in scaling up to accommodate growing user bases or expanding access requirements.
* Issuing and managing physical cards for a large number of users can become cumbersome and costly, requiring additional administrative efforts and resources.

1. Inconvenience and User Experience:

* Users often find it cumbersome to carry physical cards and remember associated PINs, leading to inconvenience and potential delays in accessing secured areas or systems.
* Forgetting or misplacing cards or PINs can lead to frustration and hinder productivity in various environments, such as workplaces or commercial premises.

1. Lack of Multifactor Authentication:

* Traditional card and PIN-based systems typically lack robust multifactor authentication mechanisms, relying solely on something the user possesses (the card) and something they know (the PIN). This leaves them vulnerable to sophisticated attacks and compromises.**PROPOSED SOLUTION**

**Facial Recognition Integrated with PIN**

In response to the limitations posed by traditional card and PIN-based systems, a proposed solution involves integrating facial recognition technology with PIN authentication, eliminating the need for physical cards while enhancing security and user convenience. The proposed system operates as follows:

**Facial Recognition Enrollment:**

* During the registration process, users provide their account number and undergo facial recognition enrollment. High-resolution facial images are captured and stored securely in the system's database alongside the corresponding account information.

**PIN Registration:**

* Users set up a unique Personal Identification Number (PIN) associated with their account during the registration process. The PIN serves as an additional layer of security and verification.

**Login Procedure:**

* To access secured areas or systems, users input their account number and associated PIN through a secure interface, such as a keypad or touchscreen.
* Upon submission of the account number and PIN, the system prompts the user to position themselves in front of a designated camera for facial recognition.

**Facial Recognition and Verification**:

* The system employs advanced facial recognition algorithms to analyze the facial features of the user in real-time. The captured facial image is compared against the enrolled facial templates stored in the database.

**PIN Verification**:

* Concurrently, the system verifies the entered PIN against the stored PIN associated with the provided account number in the database.

**EXPERIMENTAL SETUP AND RESULT ANALYSIS**

**Experimental Setup:**

1. **Data Collection:**

* During registration, facial photos of each user are captured and saved directly into the "Face Data" folder. The data is organized into subfolders named after the respective account numbers.
* Within each account folder, the facial images are stored as "face.jpg".

1. **Face Detection and Recognition Model:**

* A pre-trained deep learning model for face detection is employed to accurately locate faces within the images.
* For face recognition, a model is trained using the collected dataset to extract facial features and recognize individuals.

1. **Database Integration:**

* A database is established to store account information, including account numbers, associated PINs.

1. **Login Procedure**:

* Upon login attempt, users are prompted to enter their account number and PIN.
* The facial image associated with the entered account number is retrieved from the " Face Data" folder. During login, the user's facial image is captured and saved temporarily as "test.jpg" in the respective account folder.

1. **Verification Process**:

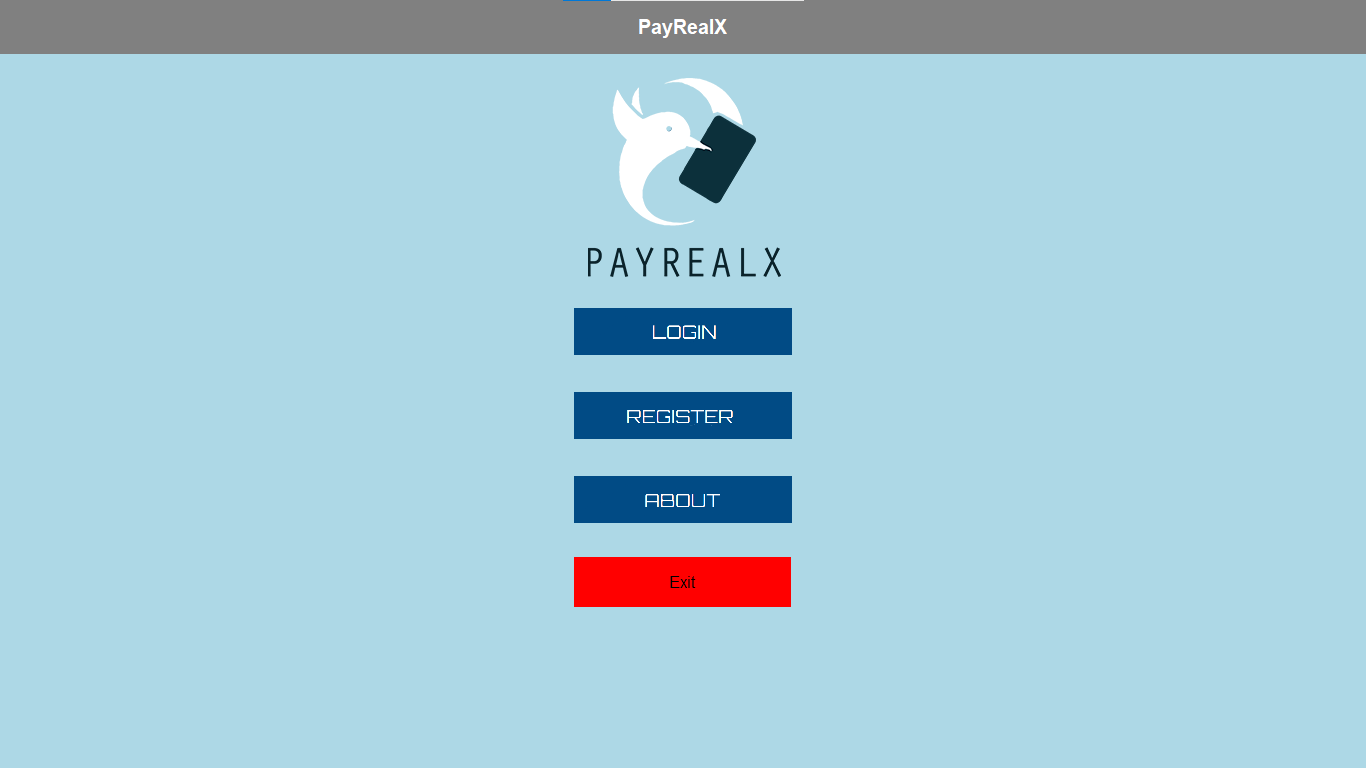
* Facial features extracted from "test.jpg" are compared with the facial features of "face.jpg" using the face recognition model.
* Verification is successful only if the entered PIN matches the PIN stored in the database for the corresponding account number.

1. **Access Control**:

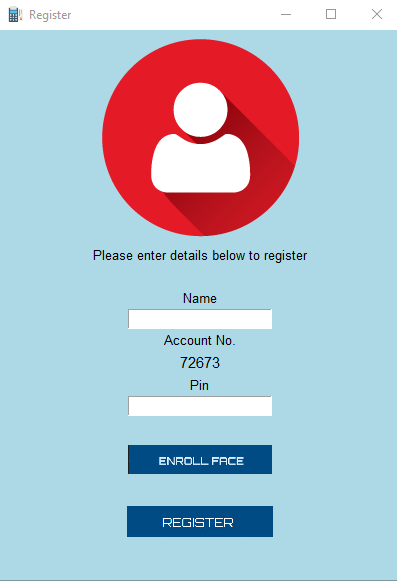
* Access is granted only if the facial features match within a certain threshold and the entered PIN is correct.
* If either the facial recognition or PIN verification fails, access is denied.

**Program Snapshots:**

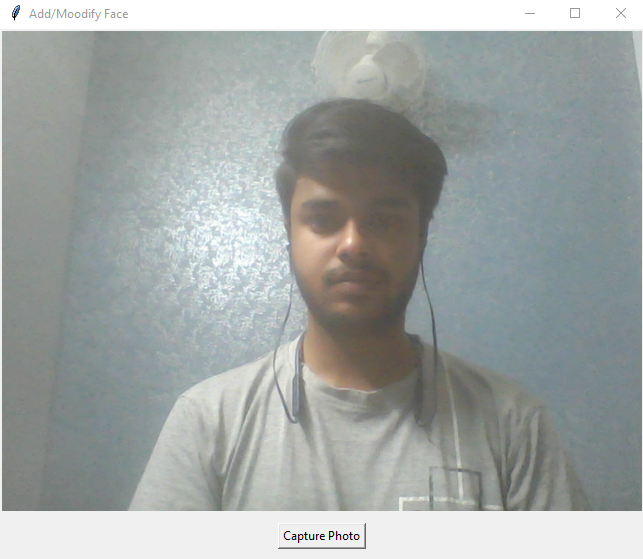
* Home Window



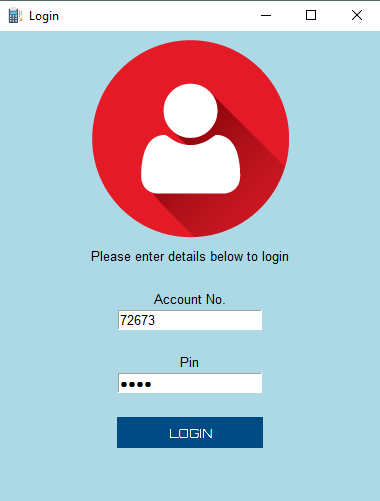
* Register Window



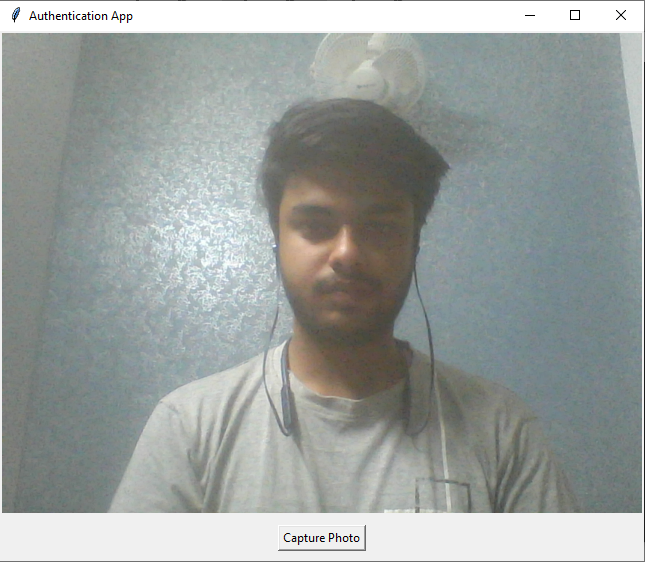
* Enroll Face Window



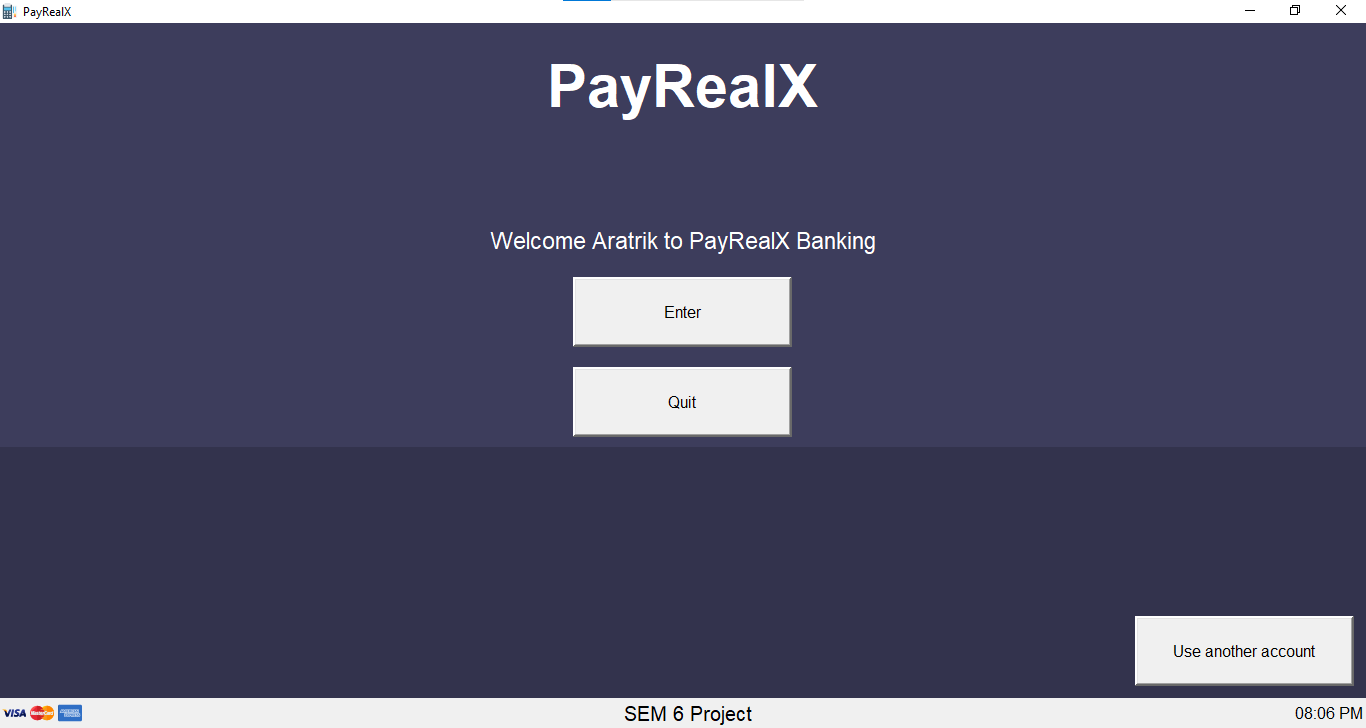
* Login Window

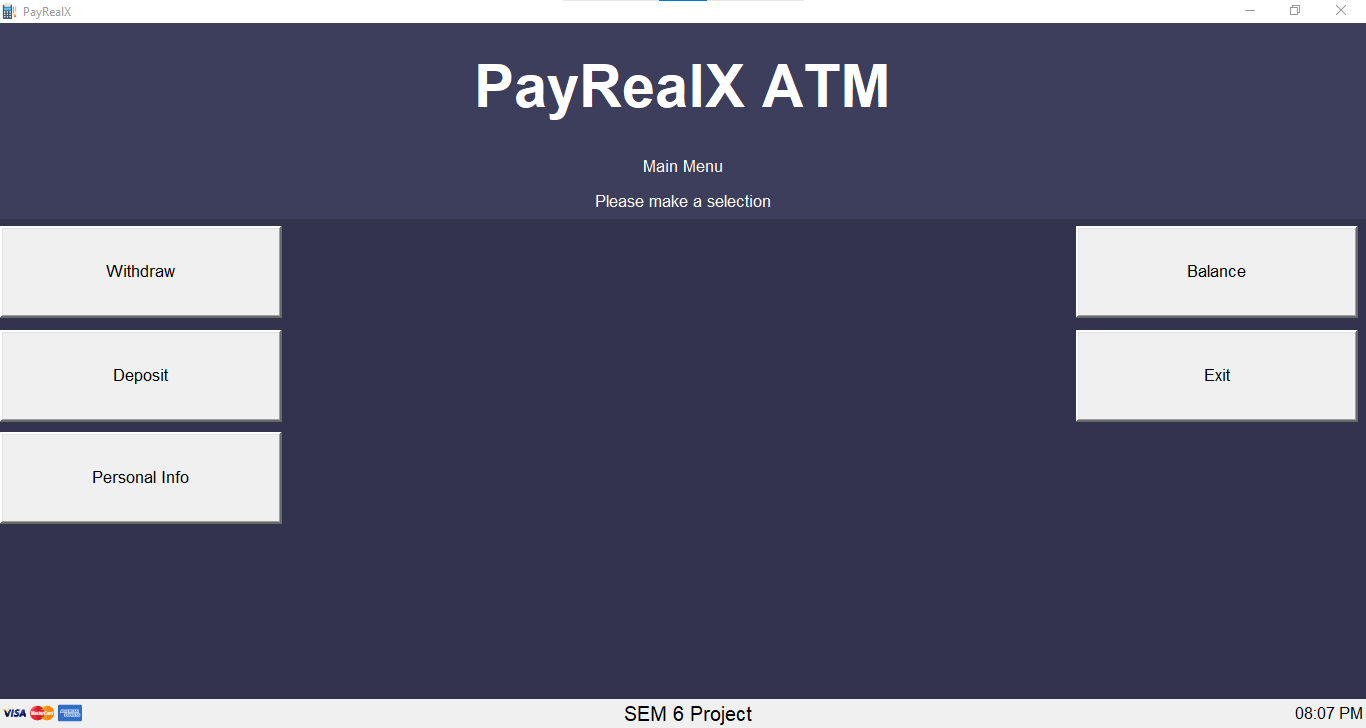


* Authentication Window



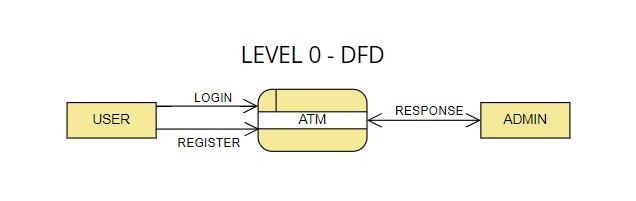
* ATM Main Screen

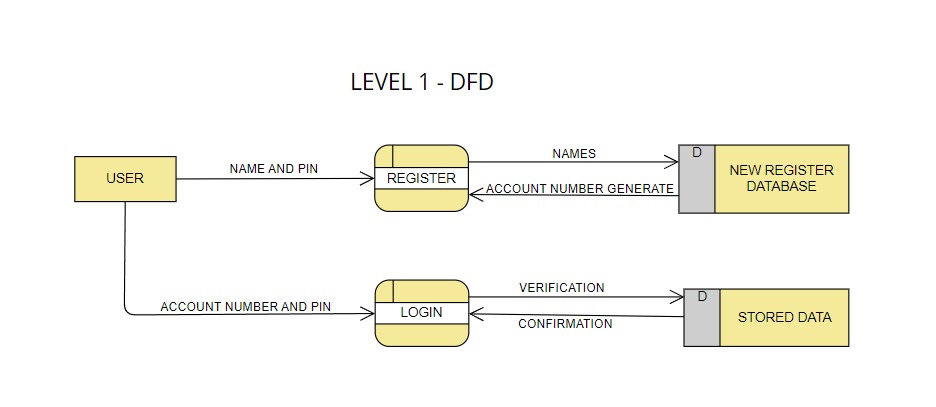


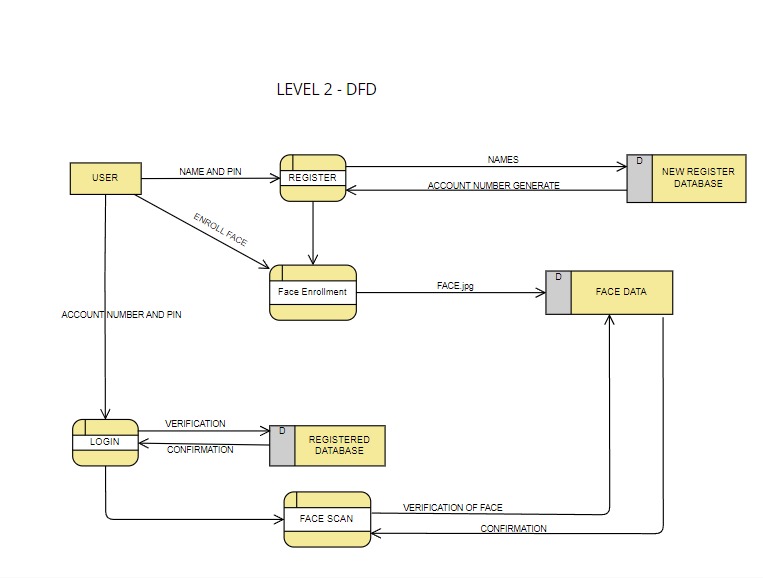


Follow on screen Instructions for normal ATM usage.

**DATA FLOW DIAGRAM**

****

****

****

**CONCLUSION & FUTURE SCOPE**

Implementing face recognition on ATM machines can greatly enhance security by providing a more secure and convenient authentication method. By using facial recognition technology, ATM machines can verify the identity of the user without the need for physical cards or PIN numbers, reducing the risk of theft or fraud. Additionally, it can help in preventing unauthorized access to ATM services, safeguarding customers' financial information.

While face recognition technology offers numerous benefits, there are also potential challenges and concerns to consider. These include privacy issues related to the collection and storage of biometric data, the possibility of false positives or negatives in the recognition process, and the need for robust cybersecurity measures to prevent hacking or misuse of the technology.

Overall, implementing face recognition on ATM machines requires a thoughtful approach that balances the benefits of enhanced security with the need to address privacy and security concerns. Proper implementation and adherence to strict data protection regulations can help ensure the successful integration of this technology into ATM services to provide a safer and more efficient banking experience for customers.

In future:

* Fingerprint Authentication can be added to completely eliminate the use of PINs.
* More reliable and accurate machine learning algorithms can be used to increase the efficiency and accuracy of the face recognition system.
* Add more Admin options to the project for better administration of accounts from the GUI.

**BIBLIOGRAPHY**

* [face-recognition · PyPI](https://pypi.org/project/face-recognition/)
* [GeeksforGeeks | A computer science portal for geeks](https://www.geeksforgeeks.org/)
* [tkinter — Python interface to Tcl/Tk — Python 3.12.2 documentation](https://docs.python.org/3/library/tkinter.html)
* [Python Pillow Tutorial - GeeksforGeeks](https://www.geeksforgeeks.org/python-pillow-tutorial/)
* [pillow · PyPI](https://pypi.org/project/pillow/)
* [PySimpleGUI: The Simple Way to Create a GUI With Python – Real Python](https://realpython.com/pysimplegui-python/)