SECURING ATM TRANSACTION WITH FACIAL RECOGNITION BASED VERIFICATION SYSTEM

TEAM MEMBERS

BARATH S (922221104007)

DHANASEKARAN N (922221104012)

KUMARASAN T (922221104701)

GUIDE : MR.AYYAPPARAJA K ,AP/CSE

ABSTRACT

ATM or Automated Teller Machines are widely used by people nowadays. Performing cash withdrawal transaction with ATM is increasing day by day. The existing conventional ATM is vulnerable to crimes because of the rapid technology development. A secure and efficient ATM is needed to increase the overall experience, usability, and convenience of the transaction at the ATM. Specifically, the goal of this project is to give a computer vision method to solve the security risk associated with accessing ATM machines. This project proposes an automatic teller machine security model that uses electronic facial recognition using Deep Convolutional Neural Network. Face Verification Clickbait Link will be generated and sent to bank account holder to verify the identity of unauthorized user through some dedicated artificial intelligent agents, for remote certification.

INTRODUCTION

ATM transactions are an essential part of modern banking, but traditional authentication methods like PIN codes and ATM cards are highly vulnerable to theft, skimming, and fraud. Criminals stolen cards and leaked PINs to gain unauthorized access, leading to financial losses. Face recognition is a method of identifying or verifying the identity of an individual using their face. Due to its non-intrusive and natural characteristics, face recognition has been the prominent biometric technique for identity authentication. The blend of deep learning models with facial recognition technology has enhanced the service in terms of speed and accuracy. It holds the power to improve the accuracy of facial recognition systems by using trained Convolutional Neural Networks (CNNs).

OBJECTIVES

1. To enhance ATM security using advanced facial recognition technology.
2. Eliminate unauthorized access through biometric verification.
3. Provide a contactless and convenient authentication method.
4. To reduce ATM fraud and card skimming incidents.
5. Integrate AI-based facial detection for real-time identity validation.
6. To ensure user privacy and data protection during transactions.

LITERATURE SURVEYS

1.Secure Biometric Verification in the Presence of Malicious Adversaries.

Author : Kamela Al-Mannai, **Year** : 2024

-Encryption and formal security proofs ensure privacy and trust in biometric authentication system.

2.DeepLearning-Enabled Face Recognition for Smart Banking Applications

Author : Journal of AI & Data Science**,** **Year** : 2023

-Discusses the integration of CNN models for real-time face recognition in banking systems.

3.Hybrid Biometric Authentication Using Face and Voice Recognition for ATM Security

Author : International Journal of Biometrics and Cybersecurity, **Year :** 2024

-Explores multi-modal biometric verification combining facial and voice features to enhance ATM safety.

4.AI-Powered Real-Time Fraud Detection in ATM Networks

Author : IEEE Transactions on AI in Financial Technology, **Year :** 2023

-Highlights the use of machine learning and facial recognition to detect fraud patterns in real-time ATM operations.

EXISTING SYSTEM

- Existing ATM authentication method is the use of password-PINs and OTP.
- QR cash withdrawals were enabled so customers could ditch their ATM cards and simply scan a QR-code on ATMs using the QR app to withdraw cash.
- ATM security system architecture that incorporates both the finger print and GSM technology into the existing PIN-based authentication process.

<u>Merits</u>

1. High Security is the eliminates card fraud & PIN hacking.
2. It’s Real-Time Authentication Fast & AI-powered verification.
3. Users can be User-Friendly then No need for cards or PINs.
4. Authenticate the system provide when the verification Sends alerts on suspicious access.

<u>Demerits</u>

1. High Initial Setup Cost requires AI-based ATM infrastructure.
2. Privacy Concerns that can Users may be hesitant to share facial data.
3. Lighting Issues for the Poor lighting or obstructions can affect records.

PROPOSED SYSTEM

- **Face Detection and Recognition:** This module captures the image of the user's face and applies Convolutional Neural Network (CNN) algorithms to detect and recognize the user's face.

- **Face Verification Link Generation:** Once the user's identity is confirmed, this module generates a face verification link and sends it to the authorized account holder's mobile number. The link contains the face image of the user captured at the time of transaction and is used for verification purposes.

- **Mobile based Unauthorized Verification:** This module is responsible for receiving the face verification link on the authorized account holder's mobile number and verifying the link to confirm the user's identity. The link is accessible only for a limited time, and the system sends an alert to the user if the link is not accessed within the specified time.

It’s MERITS

1. The advantages can be found as that the face-id is unique for everybody, it cannot be used by anybody other than the user.

2. It can be used to reduce fraudulent attempts.

3. To prevent theft and other criminal activities.

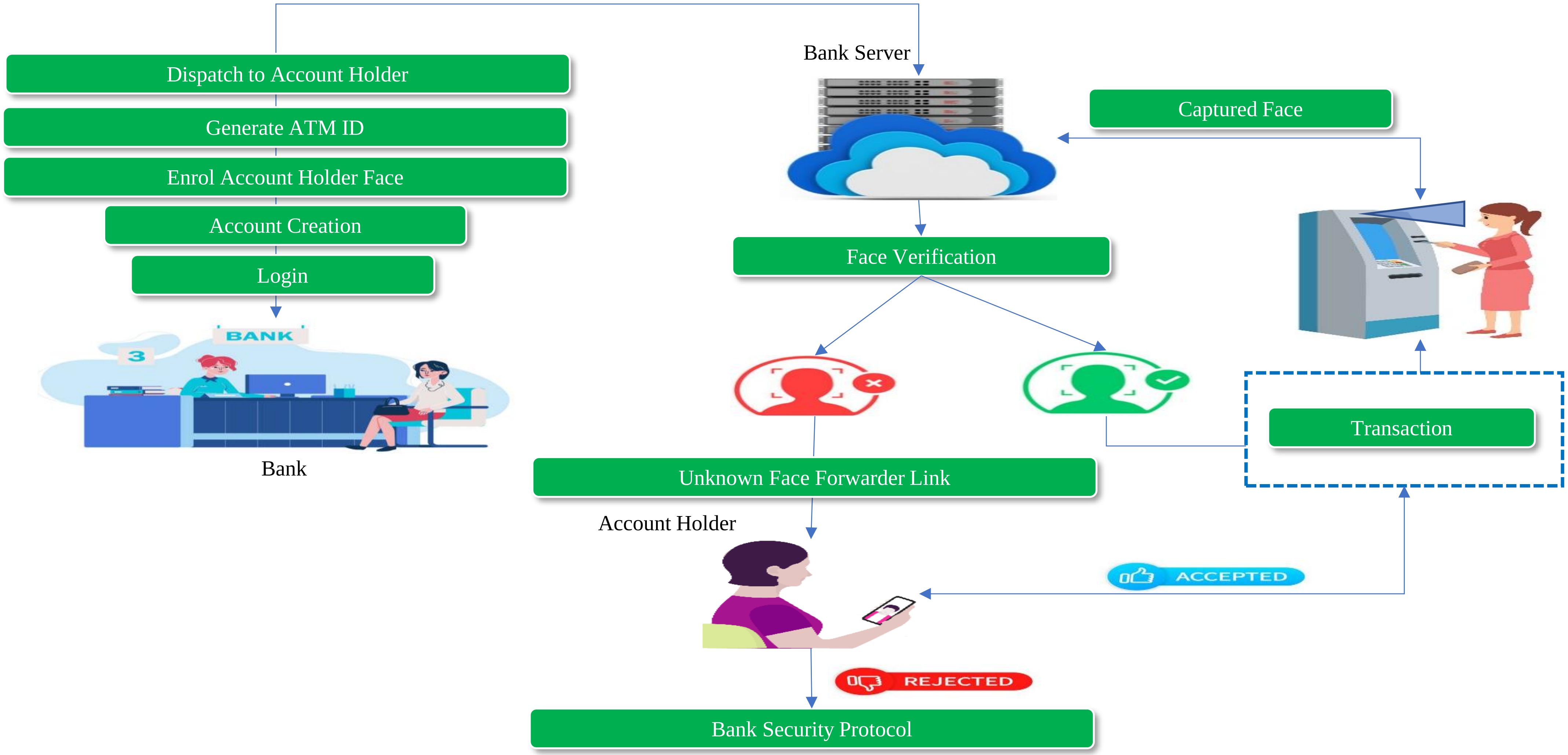
4. Secure facial authentication platform that users can trust

5. Provide safe and secure lifestyle infrastructure

6. Prevent unauthorized access using Face verification Link.

7. Fast and Accurate Prediction

SYSTEM ARCHITECTURE



Dispatch to Account Holder

Generate ATM ID

Enrol Account Holder Face

Account Creation

Login

Bank

Bank Server

Captured Face

Face Verification

Transaction

Unknown Face Forwarder Link

Account Holder

Bank Security Protocol

TOOLS AND TECHNOLOGIES

Frontend:

- **Technology:**
  HTML,
  CSS,
  JavaScript,
  Face API
- **Functions:**
  Display the user interface for facial recognition and transaction processing, providing a responsive, user-friendly ATM interaction.

Backend:

- **Technologies:** Python-OpenCV, Framework - Flask, WampServer
- Backend checks the recognized face against the stored facial database to authenticate the user and grant access to the ATM system.

APIs and Database :

- CNNs it is use for predict the capture images
- FaceNet API for real-time face recognition
- SQLite to stored images or video in the databases

SYSTEM REQUIREMENTS

1. **Operating System**: Windows 10 or higher.

2. **Python**: Computer vision . OpenCV for the image and video data in ATM camera.

3. **Flask**: For creating APIs or a lightweight dashboard to monitor transactions.

4. **MySQL**: For more scalable solutions to store account and transaction data.

5. **Python Packages**: Numpy, Pandas, Matplotlib, and Scikit-learn

6. **Web Server**: Apache Web Server (in WampServer)

MODULE DESCRIPTION

1. User Interface Modules

2. Face Recognition Modules

3. Face Identification Modules

4. Face Verification Link Generation Modules

5. Face verification Process Modules

6. Notification Process Modules

1.User Interface Modules

1.1 ATM System

Cardholder Interaction

Upon inserting their ATM card into the interface, users kick-start transactions. The system promptly reads the card details to facilitate seamless transaction processing.

Facial Recognition

Simultaneously, the system employs advanced facial recognition technology to capture the user's face. This captured image is then meticulously compared with the pre-trained face model stored in the system's database.

Face Verification Link

For added security, the system generates a Face Verification Link. This link is promptly dispatched to the mobile number linked to the card account, ensuring an extra layer of identity confirmation.

1.2. ATM User/Account Holder Interaction

Cash Withdrawal

When an ATM user seeks to withdraw cash, they simply insert their card, initiating a streamlined process. The system then verifies the user through multi-factor authentication.

Secure Login

Bank employees gain access to the system through a secure login process, ensuring that only authorized personnel can manage the ATM functionalities.

Account Management

Equipped with secure access, bank employees can seamlessly create new bank accounts, streamlining the on boarding process for customers.

Generate ATM ID, Dispatch to Account Holder

Upon the creation of a new account, the system generates a unique ATM ID. This ID is dispatched to the account holder, completing the account creation process

2.Face Recognition Modules

Dataset Creation: Account Holder Face by Recording Live Video

The process begins with actively creating a comprehensive dataset by recording a live video of the account holder's face.

Face Detection

This module identifies potential face regions within the pre-processed images. RPN excels at proposing regions likely to contain facial features, laying the groundwork for subsequent processing. It streamlines the computational effort by focusing on regions of interest, enhancing efficiency in face recognition.

Face Feature Extraction

This module focuses on extracting relevant features from the detected face regions using GLCM captures statistical information about pixel intensity relationships, offering a rich set of features for subsequent classification. It serves as a robust method for characterizing facial textures and patterns. An using CNN concern of the system allocation when the problem to solve the module in face authentication process.

3.Face Identification Modules

ATM Captures User's Face

The Face Identification module commences with the ATM employing integrated cameras or sensors to capture a live image of the user's face during a transaction. This process is crucial for obtaining a real-time representation of the user's facial features, capturing nuances such as facial expressions, contours, and unique identifiers.

Extract Features

Following the capture of the facial image, the system moves to the extraction phase where it identifies and isolates key features from the user's face. These features include but are not limited to facial landmarks, texture patterns, and distinctive attributes that collectively contribute to a comprehensive and unique facial profile.

4.Face Verification Link Generator

Generate Face Verification Link

In response to non-matching faces, the system promptly generates a Face Verification Link. This link is designed to serve as a secure and temporary reference for the user's facial profile, introducing an extra layer of security for subsequent verification steps.

Link Transmission to User's Mobile Number

The Face Verification Link is swiftly transmitted to the user's mobile number, enhancing security by sending the link to the device associated with the authorized account holder. This proactive step ensures that the user is promptly informed and involved in the verification process.

5.Face Verification Process

Link Access and View User

The authorized account holder receives the Face Verification Link on their mobile device. By clicking the link, they are directed to a secure page displaying the captured image of the user at the ATM.

Enter Amount and PIN

Upon approving the user, the account holder proceeds to enter the desired withdrawal amount and their unique Personal Identification Number (PIN). This step confirms their intention to proceed with the transaction.

Confirmation and Money Dispensation

With the entered amount and PIN, the account holder confirms the transaction. The ATM machine, recognizing the approved user, dispenses the requested amount of money.

6.Notification Modules

- The Notification Module is triggered by various events within the system. These events could include successful transactions, security alerts, account activity updates, or any other significant occurrences requiring user attention.

- The module supports different types of notifications, such as in-app alerts, SMS messages, or email notifications. Users are notified in real-time about successful or unsuccessful transactions.

- Transaction alerts include details such as transaction amount, date, time, and the location of the transaction. These alerts may include unauthorized access attempts, unusual spending patterns, or any activity that deviates from normal user behaviour.

IMPLEMENTATION DETAILS

1. **Face Registration** – Users scan their face at the bank/ATM. FaceNet extracts and stores facial features securely.

2. **Face Detection** – When a user approaches the ATM, OpenCV captures and detects their face using the camera.

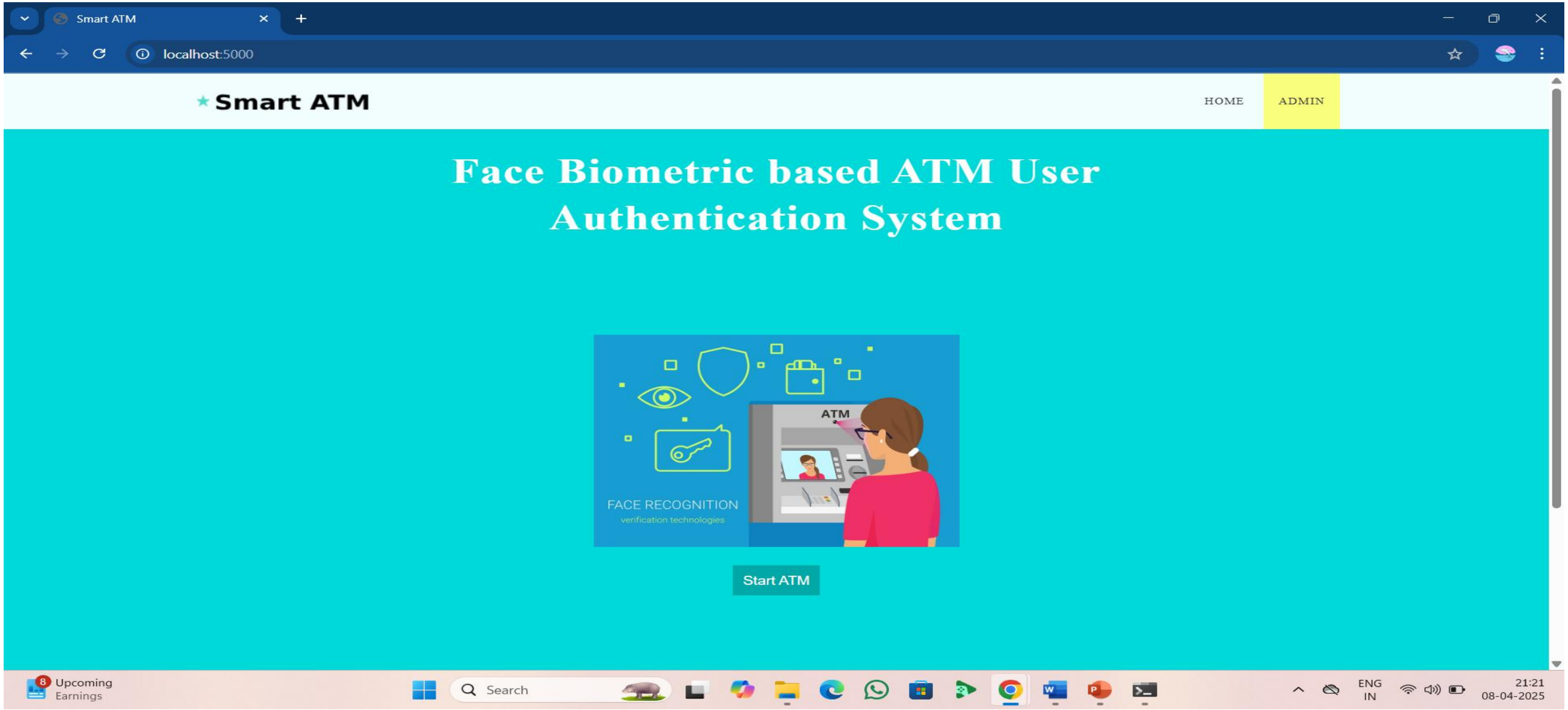
3. **Authentication** – FaceNet + TCN compare the live face with stored data. If it matches, the user gets access.

4. **Fraud Detection** – If an unauthorized face is detected, an unmatched issue to perform when is sent via SMS/Email to the user.

5. **Verification Link:** If the user's face is successfully identified, the system will send a verification link to the user's registered mobile number.

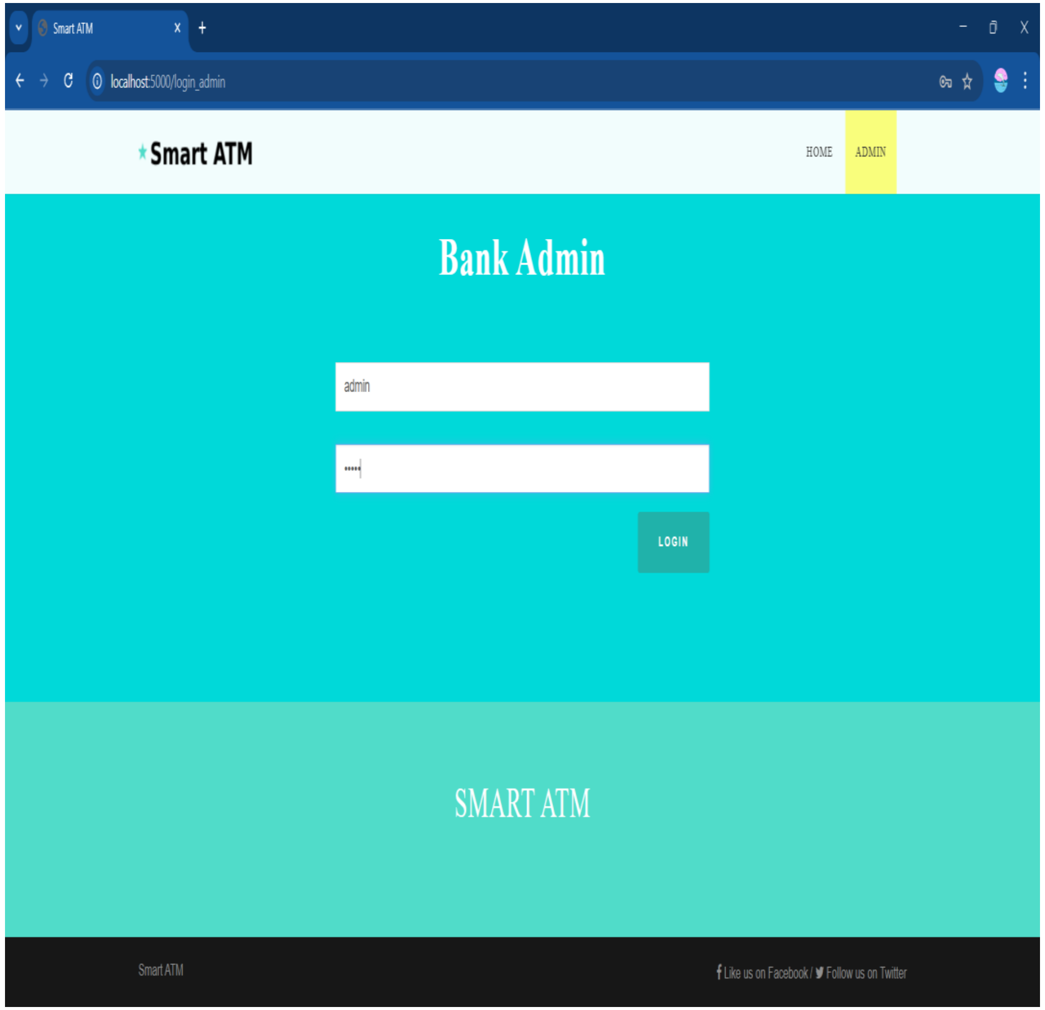
Results and Analysis

Web application analyzed,



Face Biometric based ATM User Authentication System

- First to user can registered to our details from the **Admin** to **user name and passward** to registration. when the **Account Holder** detail block to next.

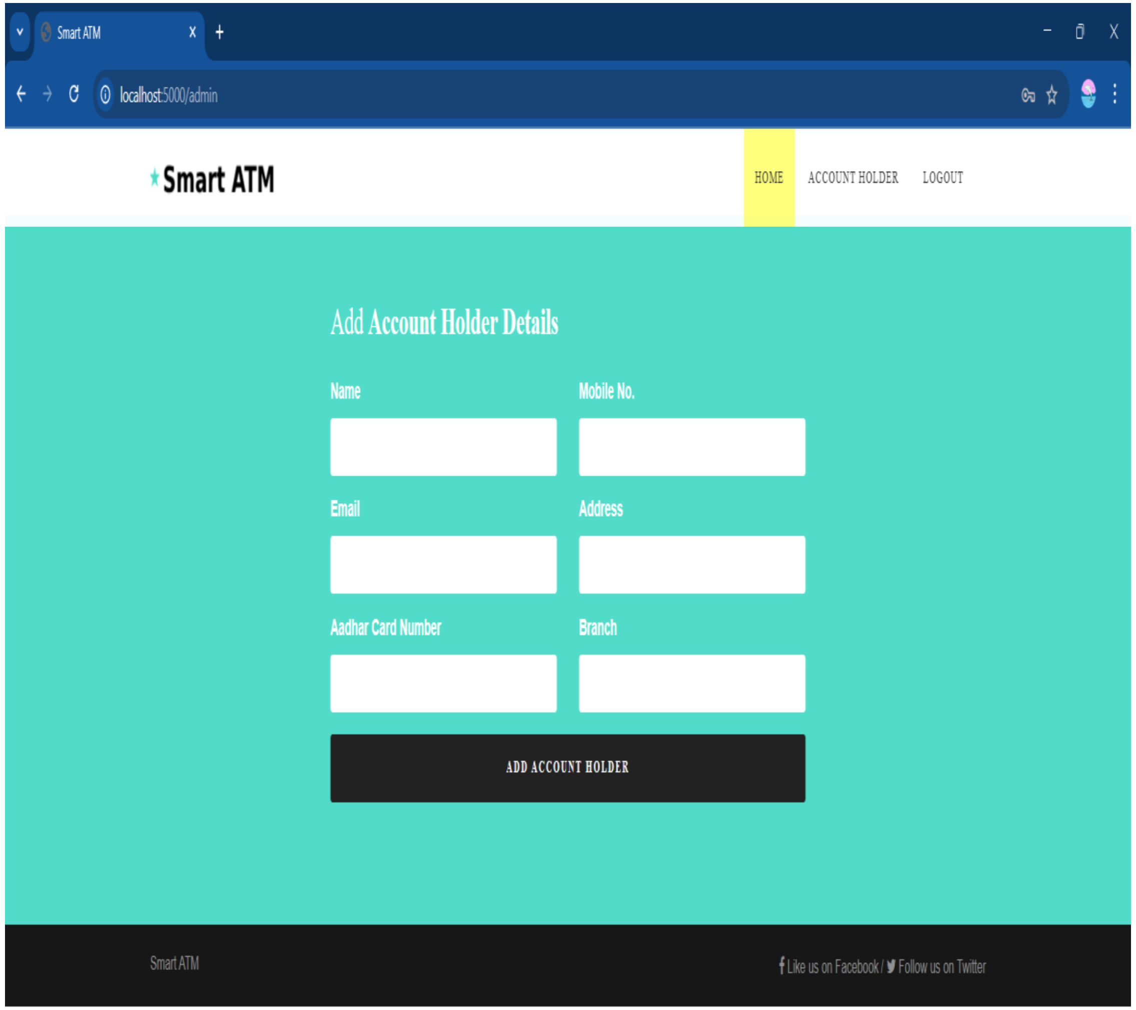


Bank Admin

admin

•••••

Smart ATM
localhost:5000/login_admin
Smart ATM
HOME
ADMIN
LOGIN
SMART ATM
Smart ATM
Like us on Facebook / Follow us on Twitter



Add Account Holder Details

Name

Mobile No.

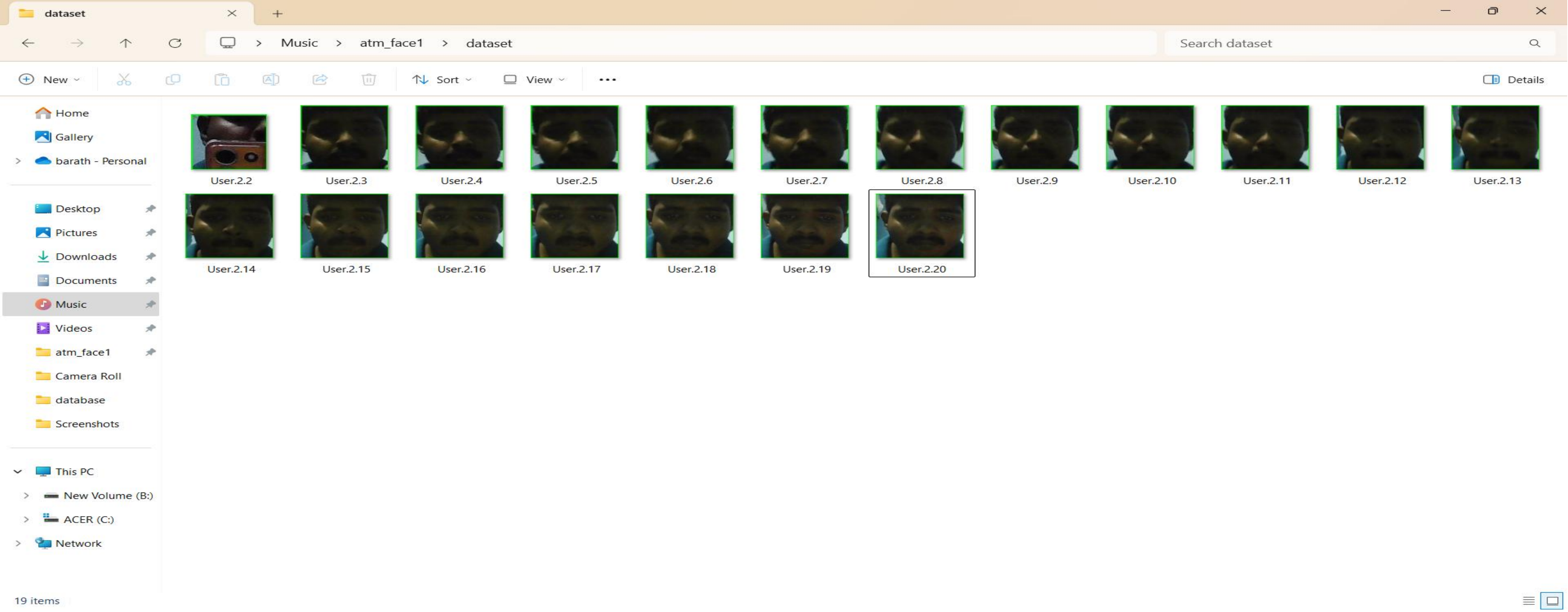
Email

Address

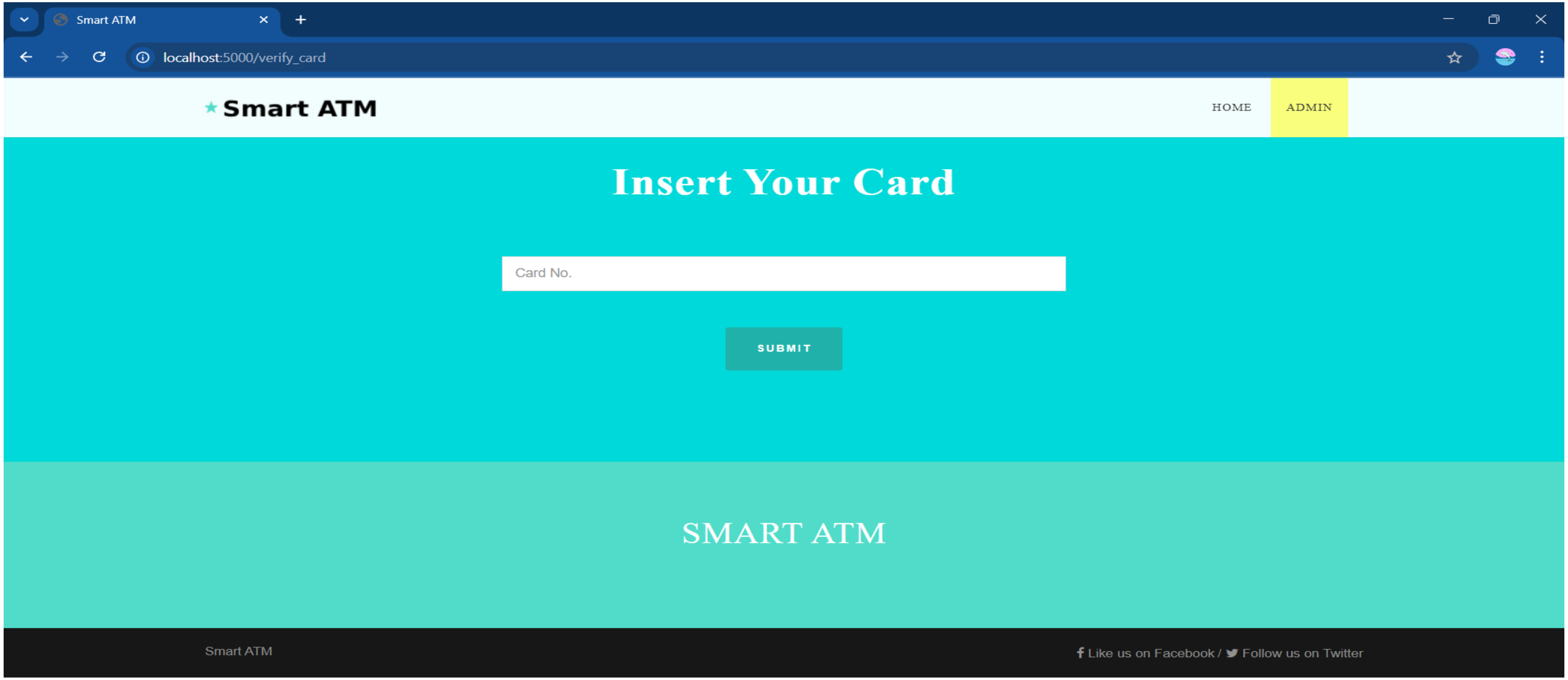
Aadhar Card Number

Branch

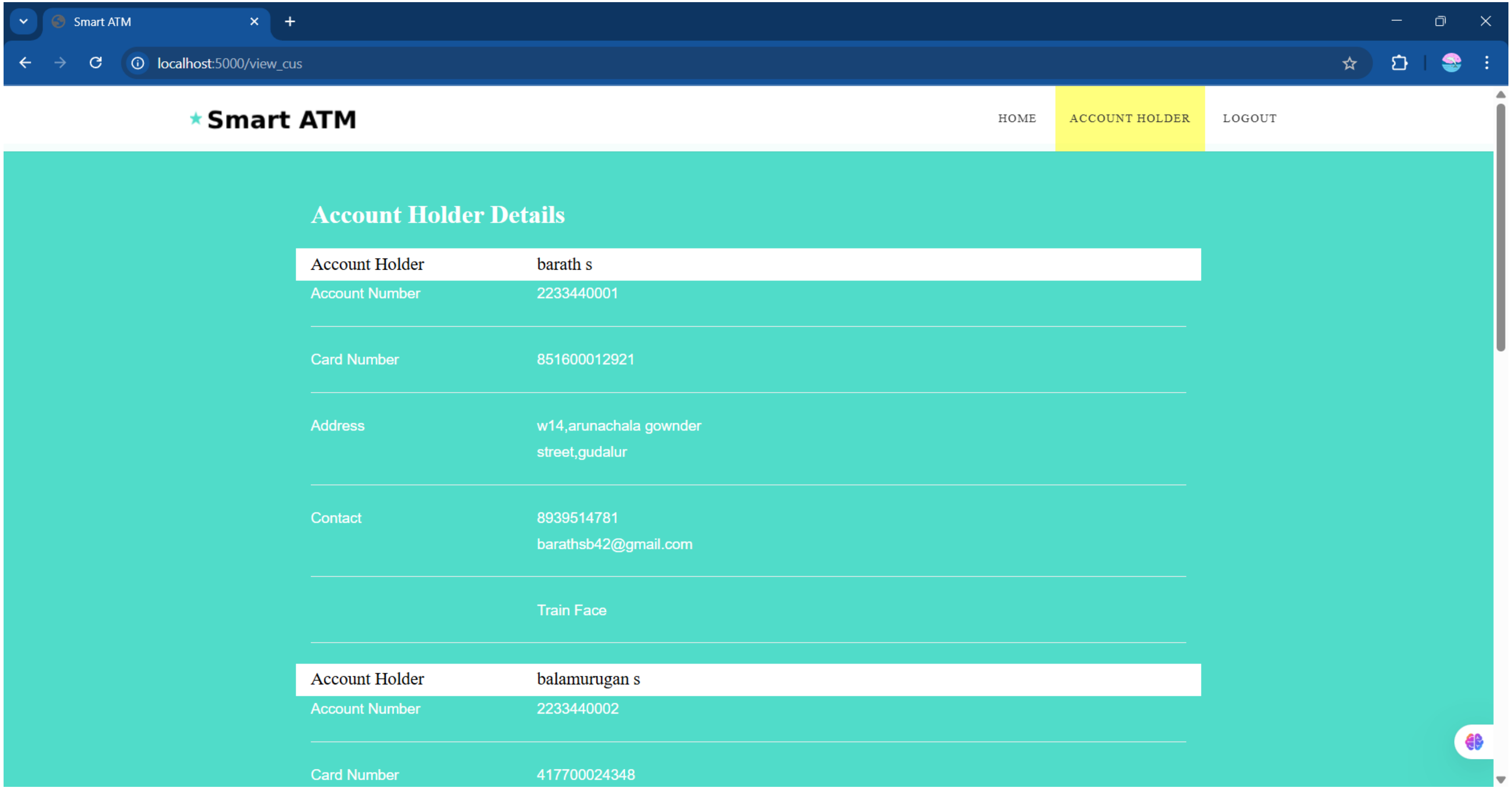
-Next Capture the face to user, then stored databases in files



- Then stored databases of the captured image and then home to start of the ATM. When the put to **pin** numbers.



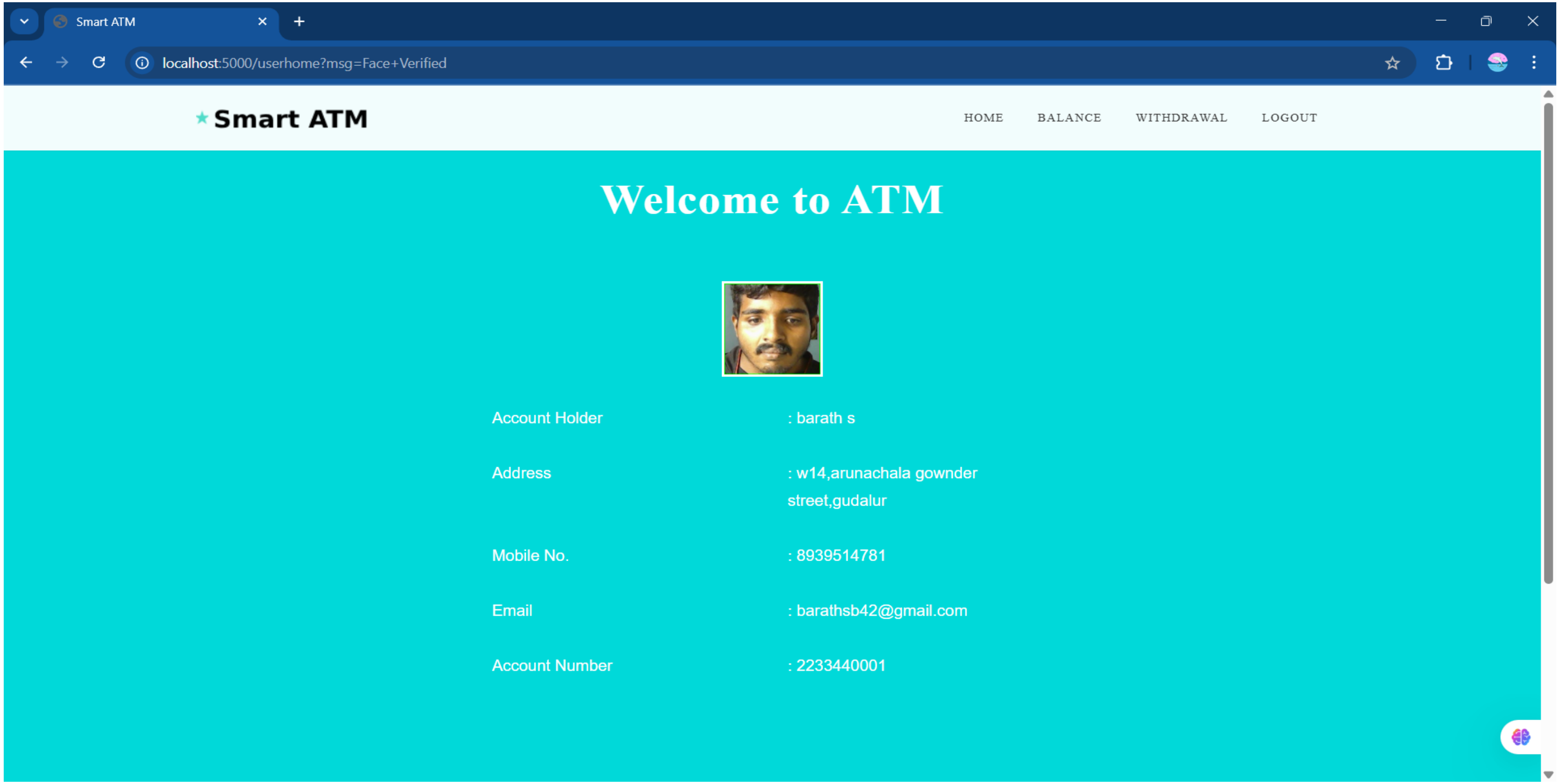
-Then get the account number to copy when we have put the insert ATM card no. page.



Account Holder Details

Account Holder	barath s
Account Number	2233440001
Card Number	851600012921
Address	w14,arunachala gownder street,gudalur
Contact	8939514781 barathsb42@gmail.com
	Train Face
Account Holder	balamurugan s
Account Number	2233440002
Card Number	417700024348

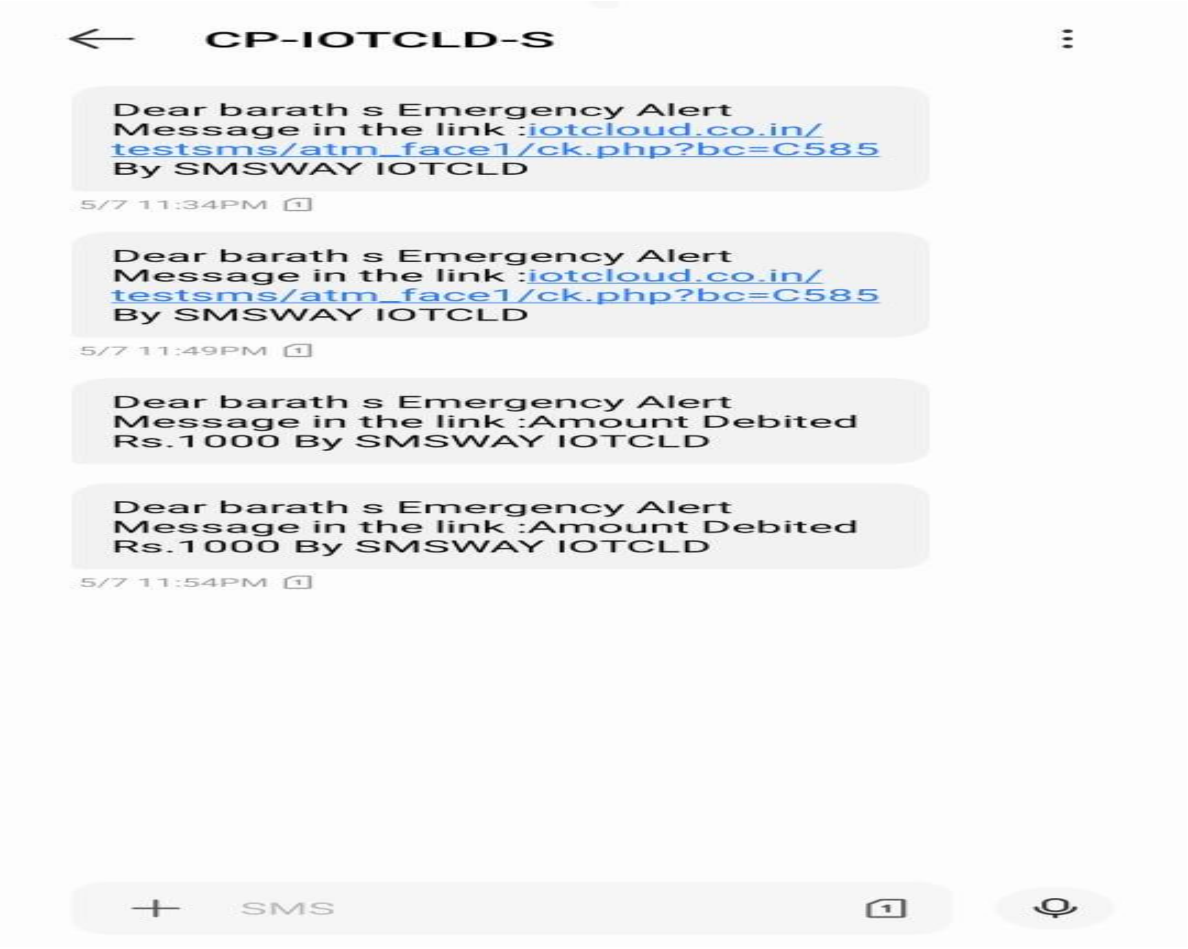
-Verify the face that card no. to account holder when the used for withdraw or balance check.



Welcome to ATM

Account Holder	: barath s
Address	: w14,arunachala gownder street,gudalur
Mobile No.	: 8939514781
Email	: barathsb42@gmail.com
Account Number	: 2233440001

-Otherwise the unmatched face to found the ATM captured face for then notification send to account holder when the accept for request to withdraw the accounter give the amount.



CP-IOTCLD-S

Dear barath s Emergency Alert Message in the link :iotcloud.co.in/testsms/atm_face1/ck.php?bc=C585 By SMSWAY IOTCLD

5/7 11:34PM

Dear barath s Emergency Alert Message in the link :iotcloud.co.in/testsms/atm_face1/ck.php?bc=C585 By SMSWAY IOTCLD

5/7 11:49PM

Dear barath s Emergency Alert Message in the link :Amount Debited Rs.1000 By SMSWAY IOTCLD

Dear barath s Emergency Alert Message in the link :Amount Debited Rs.1000 By SMSWAY IOTCLD

5/7 11:54PM

CONCLUSION

The Face ATM project represents a significant leap in the way financial transactions can be secured and authenticated. By leveraging facial recognition technology, this system ensures enhanced security, reducing the chances of fraud and unauthorized access. Additionally, it offers convenience for users by enabling seamless, contactless transactions. The integration of this system into ATM machines could revolutionize banking services, making them more accessible, faster, and user-friendly. As technology continues to evolve, such innovations have the potential to reshape the future of banking and financial services, offering more efficient and secure ways to interact with money. Facial recognition-based ATM verification is a secure, modern, and user friendly approach to safeguard financial transactions.

FUTURE ENHANCEMENT

1. Implementing Liveness Detection

To prevent spoofing attacks using photos or videos by verifying real-time presence.

2. 3D Camera Integration Upgrading

To 3D facial recognition for improved accuracy and depth-based detection.

3. Full Integration with Mobile Banking Apps

Allow users to manage ATM access, view logs, or enable/disable facial login via their phones.

4. Robust Recognition in Challenging Environments

Improve accuracy in low light, varying angles, and when users wear masks or glasses using advanced deep learning models.

REFERENCES

1.Jain, A. K., Ross, A., & Prabhakar, S. (2004). An introduction to biometric recognition. IEEE Transactions on Circuits and Systems for Video Technology.

2. Li, S. Z., & Jain, A. K. (Eds.). (2011). Handbook of Face Recognition. Springer.

3. Turk, M., & Pentland, A. Eigenfaces for recognition. Journal of Cognitive Neuroscience.

4. Viola, P., & Jones, M. Rapid object detection using a boosted cascade of simple features. CVPR.

5. Parkhi, O. M., Vedaldi, A., & Zisserman, A. (2015). Deep face recognition. BMVC.

6. Schroff, F., Kalenichenko, D., & Philbin, J. (2015). FaceNet: A unified embedding for face recognition and clustering. CVPR.

7. Taigman, Y., Yang, M., Ranzato, M. A., & Wolf, L. (2014). DeepFace: Closing the gap to human-level performance in face verification. CVPR.