PRINCE DR. K. VASUDEVAN COLLEGE OF ENGINEERING AND TECHNOLOGY

Department of Computer Science and Engineering

TITLE

ENHANCING BANKING SECURITY THROUGH MULTIMODAL BIOMETRIC AUTHENTICATION SYSTEM

DOMAIN : CYBER SECURITY

Guided and Coordinated By :

Mrs. Shalini.S M.E, (Ph.D).,

Head of the Department

Presented By :

Monisha T

(411620104011)

Reshma J

(411620104016)

AIM AND OBJECTIVE

- The aim of this project is to enhance ATM transaction security by implementing a multi-modal biometric authentication system using face recognition, iris scanning, fingerprint, voice, and palm authentication.

- The primary objective is to develop a robust, user-friendly solution that reduces the vulnerability associated with traditional PIN-based methods, offering a more secure means of user identification.

ABSTRACT

This project proposes a comprehensive multi-modal biometric authentication system for ATM transactions, integrating face recognition, fingerprint, voice, palm, and iris scanning. Employing arduino as the microcontroller, RFID technology, a LCD display, and MATLAB for processing, the system ensures robust security. Users can initiate money withdrawals by presenting their unique biometric features, enhancing authentication accuracy. The system's integration of diverse biometric modalities enhances security and user convenience. The arduino efficiently manages data processing, while MATLAB provides a versatile platform for biometric recognition. The RFID technology and LCD interface contribute to a seamless user experience, making the proposed system a reliable and advanced solution for ATM transactions.

EXISTING SYSTEM

- The existing system for ATM transactions typically relies on traditional authentication methods, primarily PIN numbers and magnetic stripe cards.

- While effective to some extent, these methods pose security challenges, such as PIN theft and card skimming.

- The reliance on single-factor authentication makes the system vulnerable to unauthorized access.

- Additionally, the lack of advanced biometric features limits user authentication options.

DRAWBACKS OF EXISTING SYSTEM

- The existing ATM system relies heavily on single-factor authentication, such as PINs and magnetic stripe cards, making it susceptible to security breaches like PIN theft and card skimming.

- Lack of advanced biometric features limits security measures, potentially compromising user accounts and transactions due to the vulnerability of traditional authentication methods.

PROPOSED SYSTEM

- We proposed a comprehensive approach to a multifaceted financial service system, leveraging RFID technology, Arduino microcontrollers, biometric authentication, and motor control to streamline banking interactions and enhance user convenience and security.
- The proposed system integrates multiple bank services into a single RFID card-based interface, facilitated by an Arduino-based control unit.
- Upon card presentation, users undergo a multistep authentication process, including PIN entry and biometric verification such as facial, fingerprint, palm, iris, and voice recognition.
- Following successful authentication, users can select their desired bank and specify the amount for withdrawal.
- This innovative solution enhances security, mitigates risks associated with PINs and card theft, and provides a user-friendly experience.

ADVANTAGES OF PROPOSED SYSTEM

- The proposed system offers unparalleled security through multi-modal biometric authentication, significantly reducing the risk of unauthorized access.

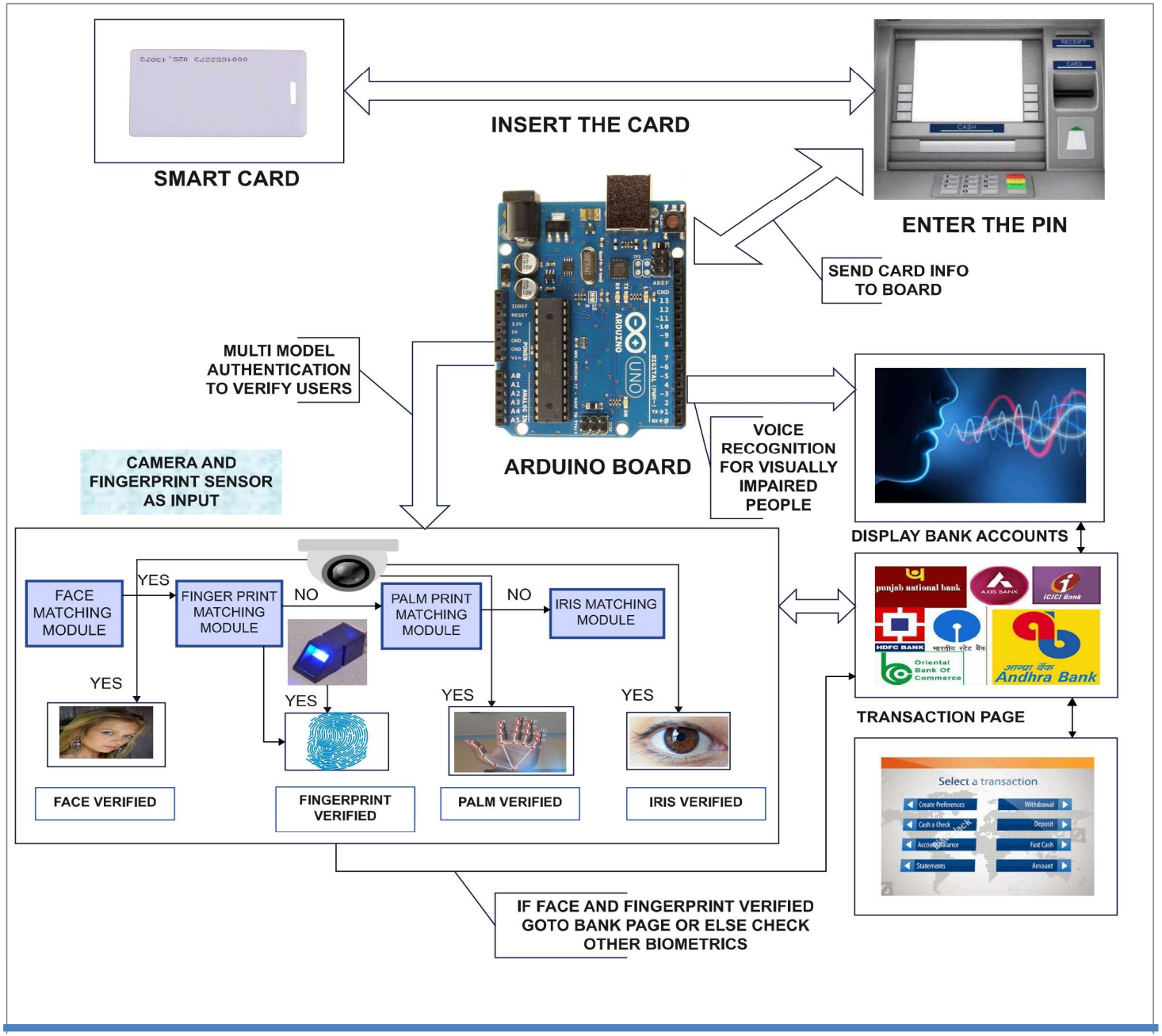
- Its integration of face recognition, fingerprint, palm, voice, and iris scanning enhances user convenience.

- The arduino microcontroller, RFID technology, LCD display, and MATLAB processing collectively ensure a robust, user-friendly, and advanced solution for ATM transactions.

ALGORITHMS USED

- **PAD (Presentation Attack Detection) Algorithm -** Detecting attempts to spoof or deceive a biometric system by presenting fake or altered biometric data, such as fake fingerprints, faces, or iris patterns.
- **Secure Electronic Transaction Algorithm -** Utilizing a secure electronic transaction algorithm, the system captures biometric data (face, fingerprint, iris, voice, palm), converts them into hash values using cryptographic methods, and compares these hashes with stored ones in the database.This approach safeguards against unauthorized access by validating multiple biometric identifiers before authorizing any financial activity.
- **CNN Algorithm -** For face recognition, iris scanning, voice recognition, and palm authentication, CNN processes image and audio data, extracting intricate features for accurate identification.

SYSTEM ARCHITECTURE



SOFTWARE REQUIREMENTS

- **OPERATING SYSTEM** : Windows7 SP1,8,8.1
- **TOOLS USED** : Matlab R2021a
- **FRONT END** : GUI
- **CODING LANGUAGE** : Python, Embedded C
- **BACK END** : Embedded system

HARDWARE REQUIREMENTS

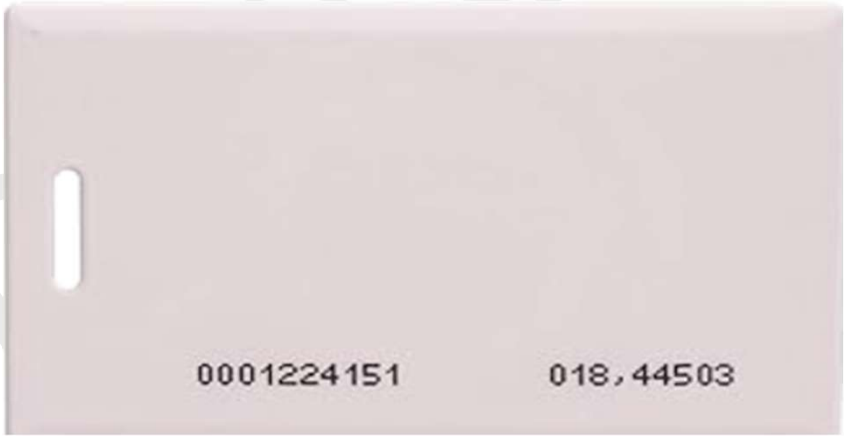
- **PROCESSOR** : Intel i3, i5, i7
- **HARD DISK** : 140GB
- **SENSOR** : Fingerprint, Camera, RFID
- **RAM** : 4GB(minimum)
- **KEYBOARD** : 110 Keys enhanced.
- **BOARD** : ARDUINO

MODULE DESCRIPTION

MODULE 1:

CARD INSERTION:

The Card Insertion module initiates the authentication process when the user inserts their smart card into the system. This phase involves reading and extracting relevant information from the inserted card, such as the user's account details, to establish a secure connection with the bank's database.



SINGLE SMART CARD

MODULE 2 :

ENTER PIN:

Upon successful card insertion, the system automatically you to enter your PIN using the keypad provided on the ATM module. Ensure that you input the correct PIN to authorize the transaction securely. After entering your PIN, follow the on-screen instructions to complete your desired transaction.

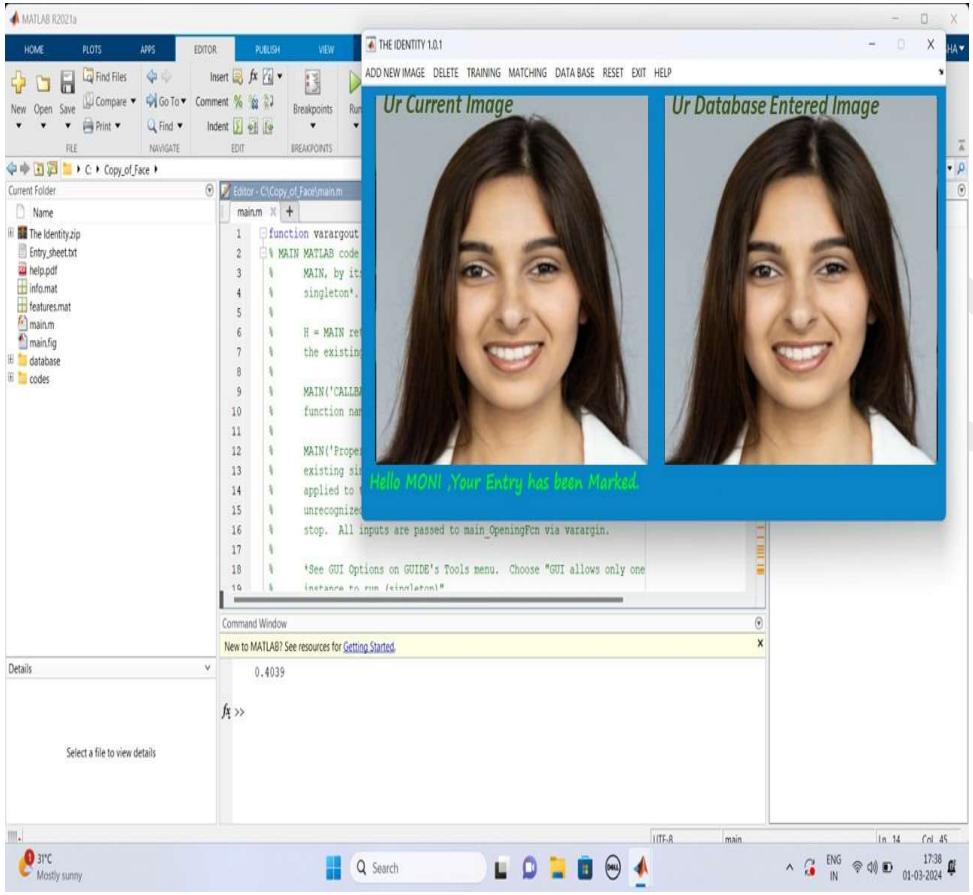
ENTERING PIN

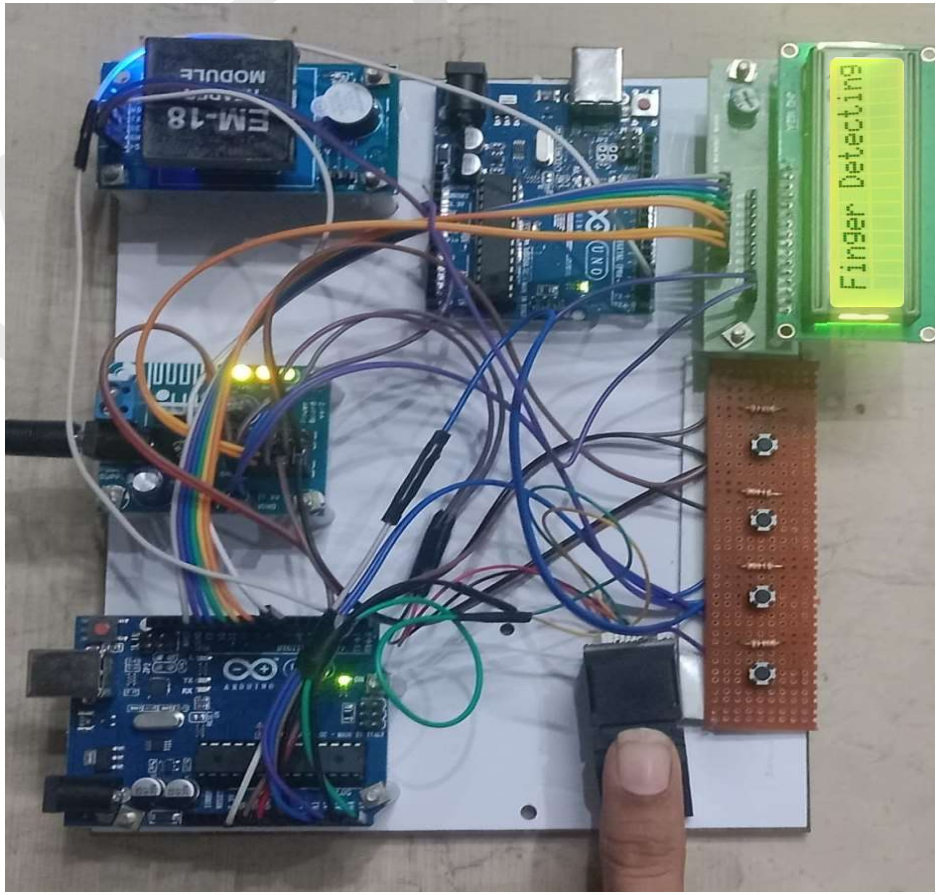
ATM PIN GETS VERIFIED

MODULE 3 :

BIOMETRIC AUTHENTICATION

The Biometric Authentication module leverages both sensors and cameras to verify the user's identity. After entering the PIN, the system activates the biometric verification process. This phase primarily focuses on facial recognition using the camera system as the initial step.

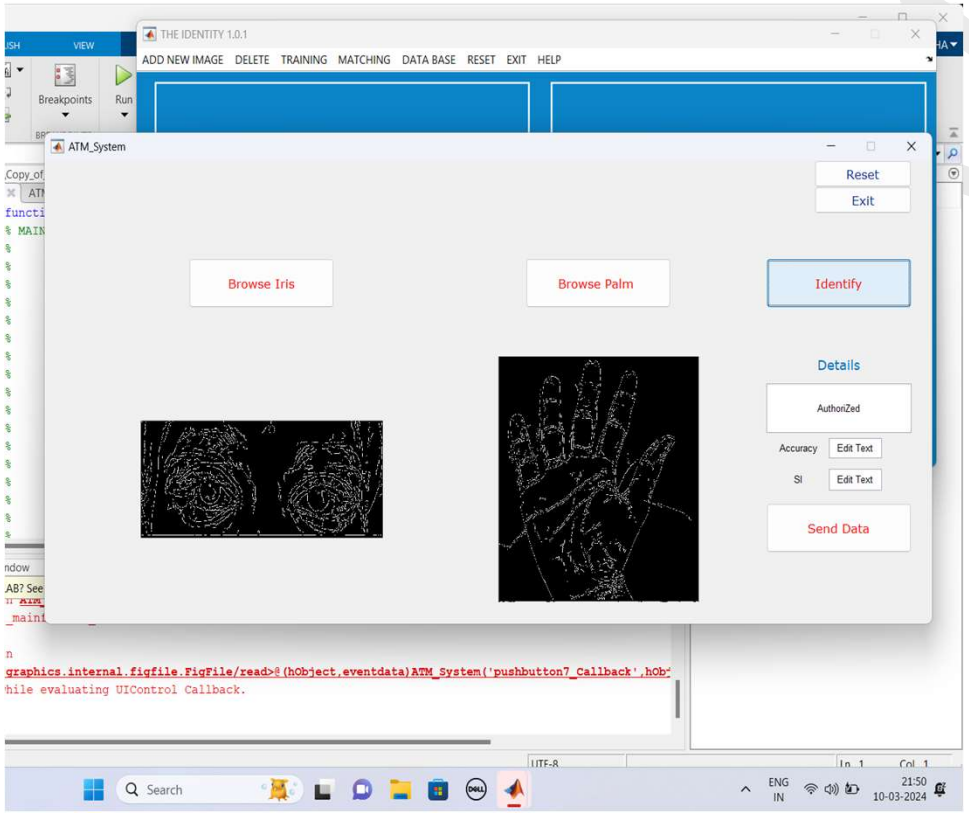


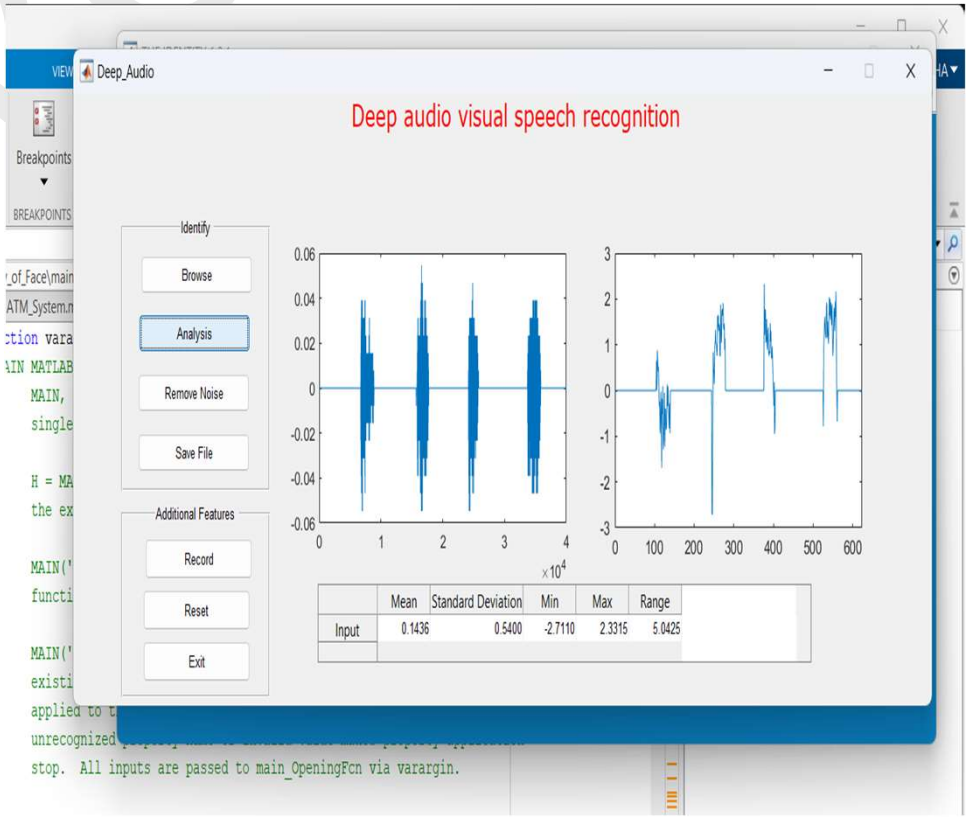


MODULE 4 :

BIOMETRIC VERIFICATION

This module employs multi-modal biometric verification techniques to enhance security. Initially, the system verifies the user's face using the camera. If successful, it proceeds to fingerprint verification using a sensor. If both verifications pass, the user is granted direct access to the Bank Account Page. In case of failure, additional biometric data such as palm, iris, and voice are verified sequentially before allowing access.

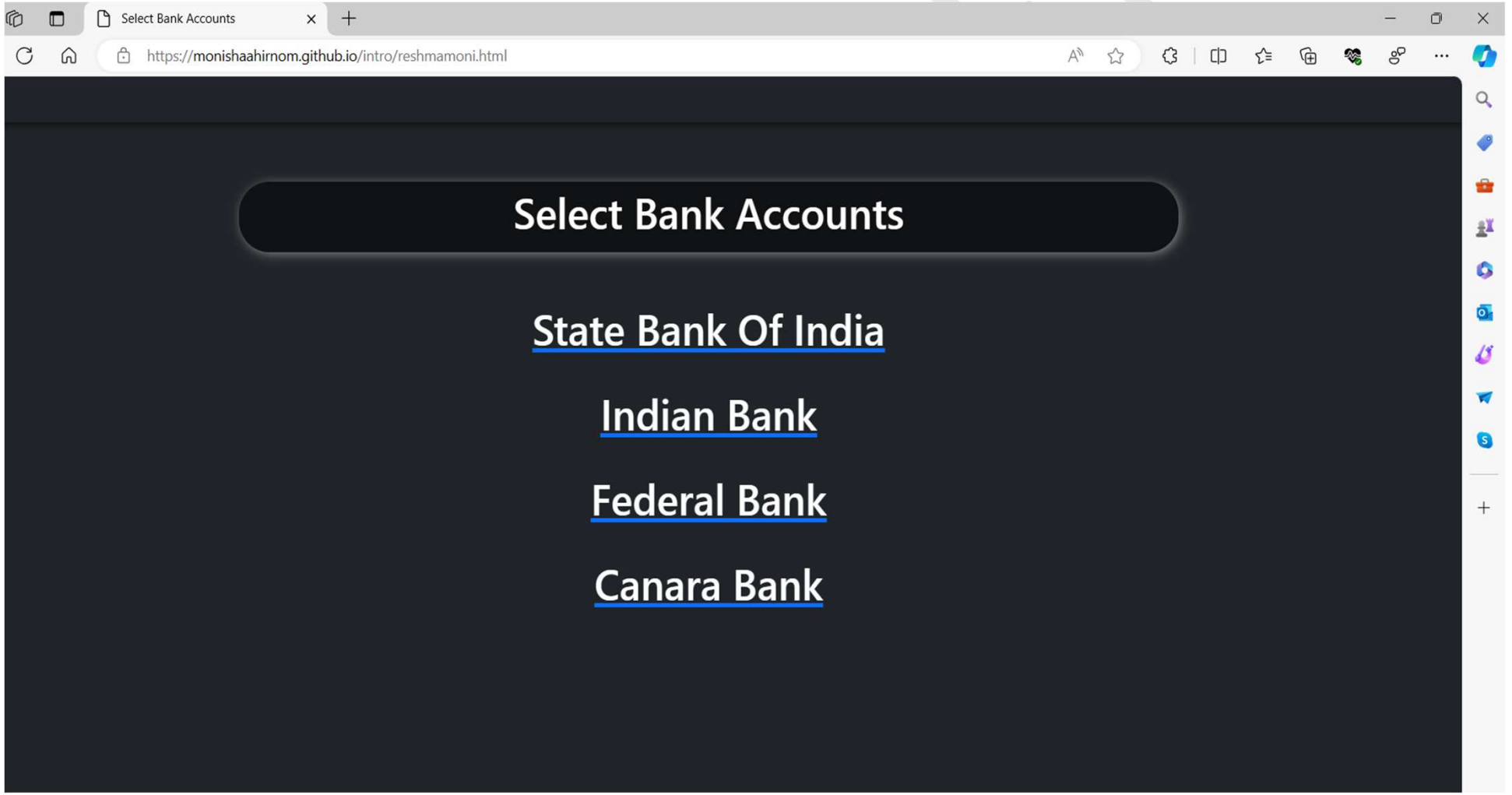




MODULE 5 :

SELECT BANK ACCOUNTS

The Bank Account module showcases the user's selected account, providing an interface for various banking transactions. This page displays the account balance, recent transactions, and other relevant details. Users can perform actions such as fund transfers, bill payments, and account management from this secure interface.



LITERATURE SURVEY

PAPER 1

TITLE : "Utilizing Biometric System for Enhancing Cyber Security in Banking Sector: A Systematic Analysis"

AUTHOR : F. Khan, H. U. Khan, M. Z. Malik, S. Nazir

YEAR : July 2023

ABSTRACT:

The paper explores the growing importance of biometric authentication in cybersecurity, focusing on its role in safeguarding the banking sector. It addresses cyber threats, emphasizing the reliability of biometrics for individual identification in online financial services.

CONCEPT RELATED TO THE PROJECT:

The study delves into the intersection of biometric security and cyber banking, highlighting the increasing significance of safeguarding digital spaces from hackers. It emphasizes the role of biometric authentication in countering security threats and enhancing safety in financial transactions.

ALGORITHMS USED:

- **Biometric Cryptosystems Algorithm -** This approach leverages unique biological traits such as fingerprints, iris patterns, or facial features for user authentication, combined with cryptographic mechanisms for secure data encryption and decryption. By using biometric data as cryptographic keys or for authentication purposes.

ADVANTAGES :

- Unparalleled accuracy in verifying individuals.
- Convenient and efficient authentication method.
- Enhanced user experience and productivity.

DISADVANTAGES:

- Biometric data can be compromised.
- Accessibility issues for certain individuals.
- Implementation costs and technical challenges.

PAPER 2

TITLE : "Online Banking User Authentication Methods: A Systematic Literature Review"

AUTHOR : W. K. Abdulraheem , M. Alshinwan , A. -K. Al-Banna , H. Kanaker , O. A. Khashan and N. A. Karim.

YEAR : December 2023.

ABSTRACT:

This paper reviews contemporary user authentication methods in online banking, including Knowledge-Based Authentication (KBA), Biometrics-Based Authentication (BBA), and Possession-Based Authentication (PBA). It explores associated cyber threats like malware and phishing attacks. Insights from popular banks are examined, emphasizing the need for robust security measures.

CONCEPT RELATED TO THE PROJECT:

User authentication in online banking involves verifying identity through various methods, such as KBA, BBA, and PBA. The concept centers on striking a balance between usability and security, adapting to technological advancements, and mitigating evolving cyber threats to safeguard customers' online accounts effectively.

ALGORITHMS USED:

- **RSA (Rivest-Shamir-Adleman) -** Asymmetric encryption for security.
- **Diffie-Hellman -** Key exchange for shared secrets.
- **ECC (Elliptic Curve Cryptography) -** Strong security with shorter keys.

ADVANTAGES:

- KBA offers familiarity, BBA uniqueness.
- PBA provides tangible authentication elements.
- Two-factor, multi-factor authentication bolster security.

DISADVANTAGES :

- BBA, biometric methods heighten precision.
- Reducing vulnerability to phishing attacks.
- Enhance overall online banking security.

PAPER 3

TITLE : "Advances in Offline Handwritten Signature Recognition Research: A Review"

AUTHOR : A. Aysa, M. Muhammat, K. Ubul, Z. Wang, N. Yadikar

YEAR : October 2023

ABSTRACT:

This paper reviews the evolution of offline handwritten signature recognition over the past 15 years, focusing on financial, legal, and business document authentication. It explores deep learning methods, emphasizing diverse architectures, challenges, and trends. The review aims to provide a comprehensive understanding for researchers.

CONCEPT RELATED TO THE PROJECT:

The project comprehensively reviews the landscape of offline handwritten signature recognition, emphasizing the integration of deep learning methods. It explores various stages, including feature extraction and classification, to provide researchers with a detailed understanding of the field's evolution, challenges, and emerging opportunities.

ALGORITHMS USED:

- **CNN Algorithm –** Convolutional neural network for recognition.
- **ADA BOOST Algorithm -** Boosting algorithm for classification.

ADVANTAGES :

- Paper highlights deep learning advantages.
- Improved identification accuracy, efficiency noted.
- Adaptability to diverse authentication scenarios.

DISADVANTAGES :

- Complexity of deep learning methods.
- Resource-intensive training requirements.
- Potential for overfitting in models.

PAPER 4

TITLE : "User Authentication by Eye Movement Features Employing SVM and XGBoost Classifiers"

AUTHOR : A. Czyzewski, F. Gorski, P. Odya.

YEAR : August 2023

ABSTRACT:

The project explores the use of low-cost eye trackers for biometric authentication in banking kiosks. Leveraging 20 features from eye movement data, the study employs Support Vector Machine (SVM) and eXtreme Gradient Boosting (XGBoost) classifiers, demonstrating XGBoost's superior performance in authentication accuracy.

CONCEPT RELATED TO THE PROJECT:

The project focuses on utilizing eye movement features as a biometric modality for user authentication in banking kiosks. It emphasizes the advantages of contactless eye trackers, especially in the context of the Covid pandemic, providing a solution for both secure identity verification and confirming user liveness.

ALGORITHMS USED:

- **Support Vector Machine -** Classifies eye movement data.
- **Nu-Support Vector -** Variant of SVM classifier to classify the input data.
- **Machine, Random Forest -** Ensemble learning for classification.
- **Multi-Layer Perceptron -** Neural network for classification.

ADVANTAGES :

- Contactless eye trackers offer security.
- Convenient means of user authentication.
- Emphasizes non-intrusive nature, effectiveness.

DISADVANTAGES :

- Potential concerns about privacy invasion.
- Accuracy may vary based on conditions.
- Limited accessibility for certain users.

PAPER 5

TITLE : "Benchmarking Neural Network Compression Techniques for Ocular-Based User Authentication on Smartphones"

AUTHOR : A. Almadan, A. Rattani

YEAR : April 2023

ABSTRACT:

This project addresses the challenge of deploying efficient ocular-based user authentication on smartphones. It benchmarks neural network compression techniques for lightweight models, considering the increasing reliance on smartphones for secure transactions. The study utilizes UFPR and VISOB 2.0 datasets for comprehensive experimental validation.

CONCEPT RELATED TO THE PROJECT:

The project revolves around optimizing ocular-based user authentication on smartphones. Given the limitations of smartphone resources, the focus is on evaluating neural network compression techniques. This concept aims to balance accuracy, security, and computational efficiency in the deployment of deep learning models for user authentication.

ALGORITHMS USED:

- **Distillation Algorithm -** Neural network knowledge distillation.
- **KD Algorithm -** Knowledge distillation compression technique.

ADVANTAGES :

- Project emphasizes neural network compression.
- Making ocular-based authentication suitable.
- Ensuring secure, convenient user authentication.

DISADVANTAGES :

- Complexity of compression techniques.
- Potential loss of model accuracy.
- Compatibility issues with certain devices.

PAPER 6

TITLE : "Voice Activity Detection Optimized by Adaptive Attention Span Transformer"

AUTHOR : B. Liu , W. Mu

YEAR : March 2023

ABSTRACT:

This project introduces AAT-VAD, an innovative Voice Activity Detection (VAD) method. By integrating an adaptive width attention learning mechanism into the transformer framework, AAT-VAD overcomes common limitations in existing VAD approaches, achieving superior F1-scores and reduced detection cost function (DCF) values.

CONCEPT RELATED TO THE PROJECT:

AAT-VAD revolutionizes Voice Activity Detection by incorporating an adaptive width attention learning mechanism into the transformer framework. This approach, aimed at enhancing performance for long audio signals, involves Mel-scale Frequency Cepstral Coefficients (MFCC) extraction, attention masking, and transformer encoder layer processing for classification.

ALGORITHMS USED:

- **Speech Recognition Algorithm -** Converts spoken words into text. Here, the words are first recognized into a each words and it forms sentences , then it converts it from the voice to understandable texts.

ADVANTAGES :

- AAT-VAD achieves higher F1-score for voice recognition.
- Outperforms DCU-10, Tr-VAD.
- Reduces average detection cost.

DISADVANTAGES :

- Complexity of implementation.
- Dependency on noise interference levels.
- Potential variability in real-world performance.

PAPER 7

TITLE : "Design of a Batteryless, Wireless, and Secure System-on-Chip Implant for In-Body Strain Sensing"

AUTHOR : C. Busch, B. Liu

YEAR : March 2023

ABSTRACT:

The project addresses the demand for wireless and batteryless implants for long-term biomedical monitoring. It introduces a novel System-on-Chip (SoC) implant for in-body strain sensing, overcoming limitations of existing designs through reconfigurable in-body rectenna, energy-efficient strain sensing, AES-GCM security, and closed-loop wireless programming.

CONCEPT RELATED TO THE PROJECT:

The project innovates by presenting a System-on-Chip (SoC) implant designed for in-body strain sensing. It leverages a reconfigurable in-body rectenna, an energy-efficient strain sensing front-end, AES-GCM security, and closed-loop wireless programming, addressing challenges in wireless and batteryless implants for long-term biomedical monitoring.

ALGORITHMS USED:

- **Counter-Mode Encryption -** unique initialization vector (IV) to be used with each new block of data.

ADVANTAGES :

- SoC implant offers in-body strain sensing.
- Features reconfigurable rectenna, energy efficiency.
- Achieves robust biomedical monitoring solution.

DISADVANTAGES :

- Potential compatibility issues with devices.
- Reliability concerns over long-term usage.
- Complexity in implementation and maintenance.

PAPER 8

TITLE : "Synthetic ID Card Image Generation for Improving Presentation Attack Detection"

AUTHOR : D. Benalcazar, C. Busch, S. Gonzalez, J. E. Tapia

YEAR : March 2023

ABSTRACT:

The project addresses the challenge of remote biometric authentication amidst the digitization of processes, especially during the COVID-19 pandemic. It explores methods for synthetically generating ID card images to augment datasets for training fraud-detection networks, achieving improved performance without compromising privacy.

CONCEPT RELATED TO THE PROJECT:

The project explores synthetic image generation methods to bolster datasets for training fraud-detection networks, specifically targeting fake identity documents. By leveraging computer vision algorithms and Generative Adversarial Networks (GANs), the concept aims to increase the quantity of training data without zompromising the sensitive nature of personal identity documents.

ALGORITHMS USED:

- **Image Processing Algorithm -** Processing up of the images comparing it with the existing models.
- **PAD (Presentation Attack Detection) Algorithm -** detecting attempts to spoof or deceive a biometric system by presenting fake or altered biometric data, such as fake fingerprints, faces, or iris patterns. PAD techniques aim to ensure the integrity and security of biometric authentication systems by distinguishing between genuine biometric data and presentation attacks.

ADVANTAGES :

- Synthetic ID card images supplement datasets.
- Improve fraud detection network performance.
- Maintain efficiency across various scenarios.

DISADVANTAGES :

- Potential limitations in representing real-world data.
- Dependency on accurate synthesis algorithms.
- Challenges in adapting to evolving fraud tactics.

PAPER 9

TITLE : "E-Banking Security Study—10 Years Later"

AUTHOR : P. Hanacek, L. Hellebrandt, O. Hujnak, K. Malinka.

YEAR : February 2022

ABSTRACT:

This project revisits e-banking security after a decade, notably the impact of the Payment Services Directive (PSD2) in the European Union. It provides an overview of current authentication methods, their compliance with resistance against attacks, and multi-factor authentication schemes with PSD2 requirements. An e-banking attacks taxonomy is introduced to enhance understanding in this evolving field.

CONCEPT RELATED TO THE PROJECT:

The project reassesses e-banking security post-PSD2, offering a comprehensive overview of current authentication methods, their compliance with international standards, and resistance against attacks. It introduces an e-banking attacks taxonomy, enhancing the understanding of authenticator threats, with a focus on bridging diverse sources for a holistic view of e-banking security.

ALGORITHMS USED:

- **Homomorphic Encryption -** Perform computations on encrypted data. Homomorphic encryption allows for computations to be performed on encrypted data without decrypting it first, thus enhancing privacy and security in e-banking systems.

ADVANTAGES :

- Study updates e-banking security understanding.
- Considers authentication scheme evolution, PSD2.
- Offers comprehensive e-banking attacks taxonomy.

DISADVANTAGES :

- Complexity in navigating security landscape.
- Potential challenges in implementation.
- Dependency on timely updates and adaptation.

PAPER 10

TITLE : "Deep Learning Modalities for Biometric Alteration Detection in 5G Networks-Based Secure Smart Cities"

AUTHOR : Ahmed Sedik , Ahmed A . Abd El - Latif , Ashraf A. M. Khalaf , Ghada M. El-Banby

YEAR : June 2021

ABSTRACT:

The project addresses secure smart cities in 5G networks, focusing on biometric alteration detection. Utilizing deep learning models, including convolutional neural networks (CNN) and a hybrid CNN-ConvLSTM model, the system distinguishes between pristine, adulterated, and fake biometrics, ensuring robust authentication in smart city applications.

CONCEPT RELATED TO THE PROJECT:

The study introduces a system for detecting alterations to biometric modalities, crucial for secure smart cities. Leveraging deep learning, including CNN and a hybrid CNN-ConvLSTM model, the system assesses the probability of biometric tampering, offering enhanced security and authentication in 5G-based smart city applications.

ALGORITHMS USED:

- **Multi-Algorithm Mean -** Using multiple algorithms for analysis.
- **Linear Discriminant Analysis (LDA) Algorithm -** Classifies data using linear projection.

ADVANTAGES :

- Proposed system ensures secure transactions.
- Protects user identities in 5G-based smart cities.
- Utilizes deep learning for high accuracy.

DISADVANTAGES :

- Potential resource-intensive implementation.
- Complexity in adapting to evolving threats.
- Dependency on network stability and latency.

PAPER 11

TITLE : "Device Light Fingerprints Identification Using MCU-Based Deep Learning Approach"

AUTHOR : Chung-Wen Hung, Jun-Rong Wu, Ching-Hung Lee.

YEAR : May 2021

ABSTRACT:

This project introduce device identification using the light fingerprint by a MCU-based deep learning approach. The corresponding difference produces a unique phenomenon in the frequency spectrum. Therefore, we adopt deep learning approaches for developing a mobile phone light fingerprint identification system and implementing it on a low-cost microcontroller platform.

CONCEPT RELATED TO THE PROJECT:

The screen light of the mobile phone is analyzed to obtain the features of unique light fingerprints. Only a single model needs to be added or deleted for updating new authentication data and this does not affect the identification ability of all models. This results in greater flexibility in real-life applications and potential for expansion to other fields, such as smart buildings and automated robots.

ALGORITHMS USED:

- **Convolution neural network (CNN) -** Image analysis using deep learning.
- **K-nearest neighbors (KNN) algorithms -** Classification based on nearby instances.
- **AE detection algorithm -** Anomaly detection in data.
- **Greedy Algorithm -** Optimization through locally optimal choices.

ADVANTAGES :

- Gaussian and Bayesian optimization methods used.
- Optimize search for higher accuracy.
- Select model with lower memory.

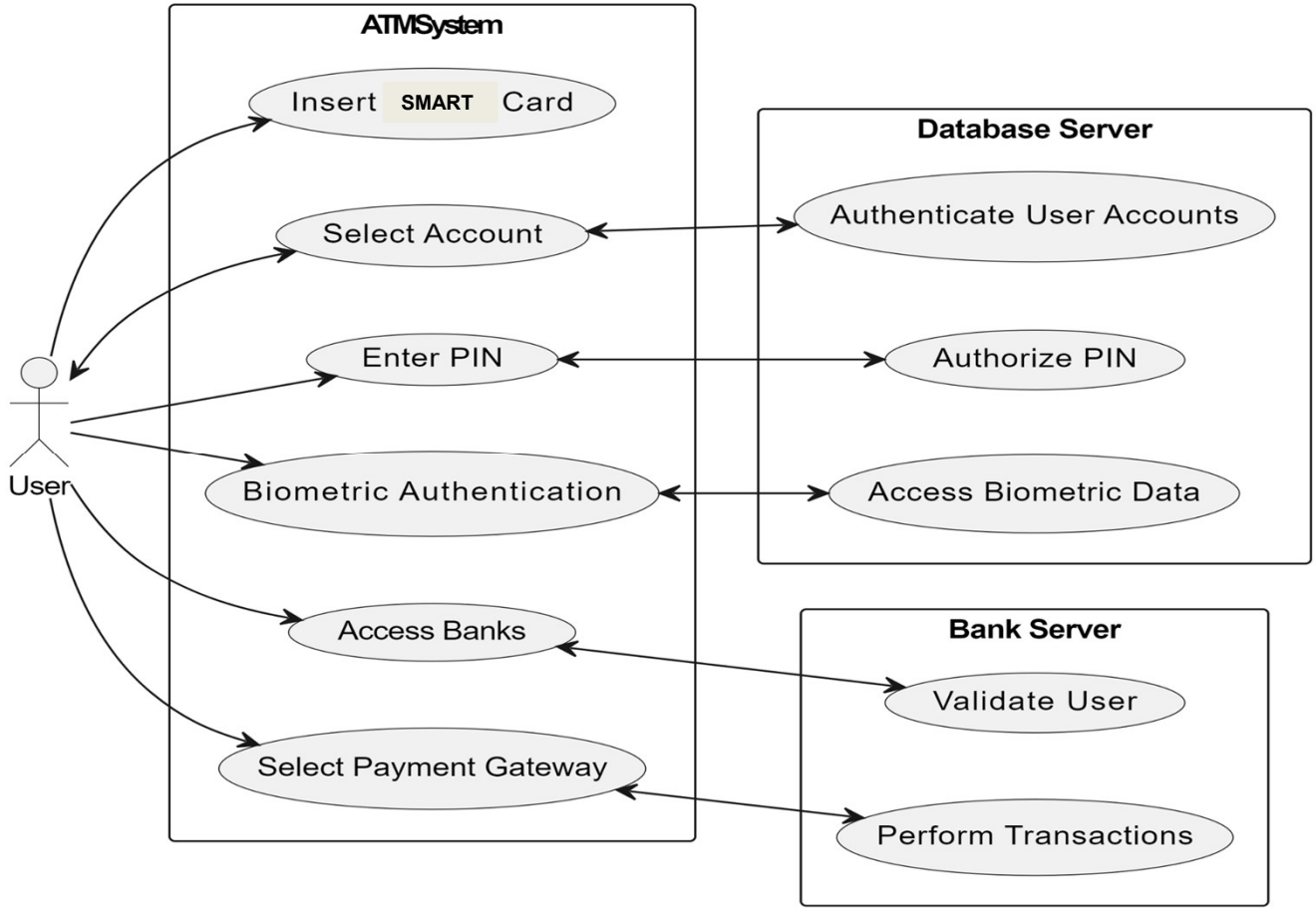
DISADVANTAGES :

- Potential computational complexity.
- Dependency on data quality and quantity.
- Resource-intensive optimization process.

SYSTEM DESIGN

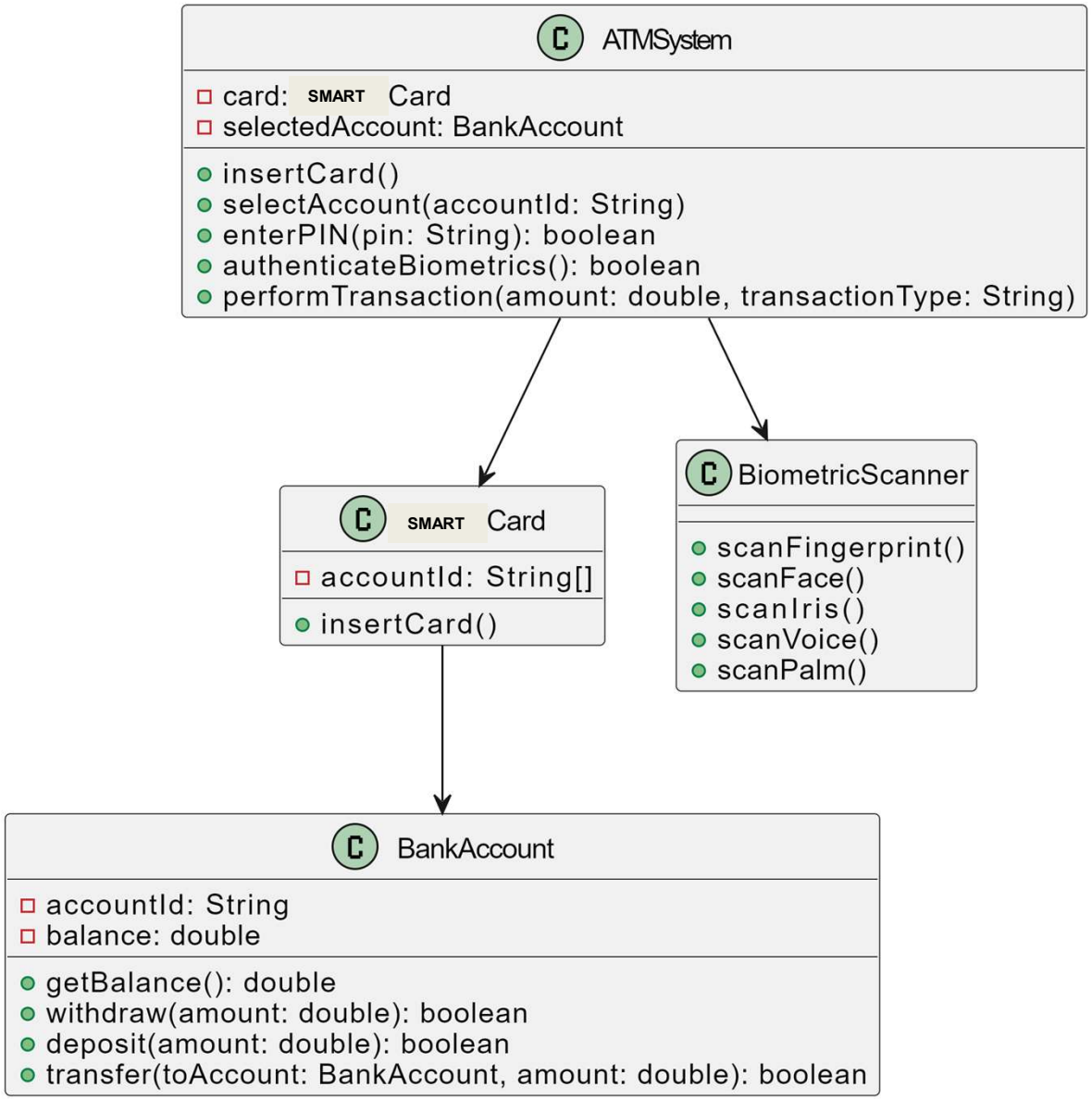
USE CASE DIAGRAM:

A use case diagram is a type of behavioral diagram created from a Use-case analysis. The purpose of use case is to present overview of the functionality provided by the system in terms of actors, their goals and any dependencies between those use cases.



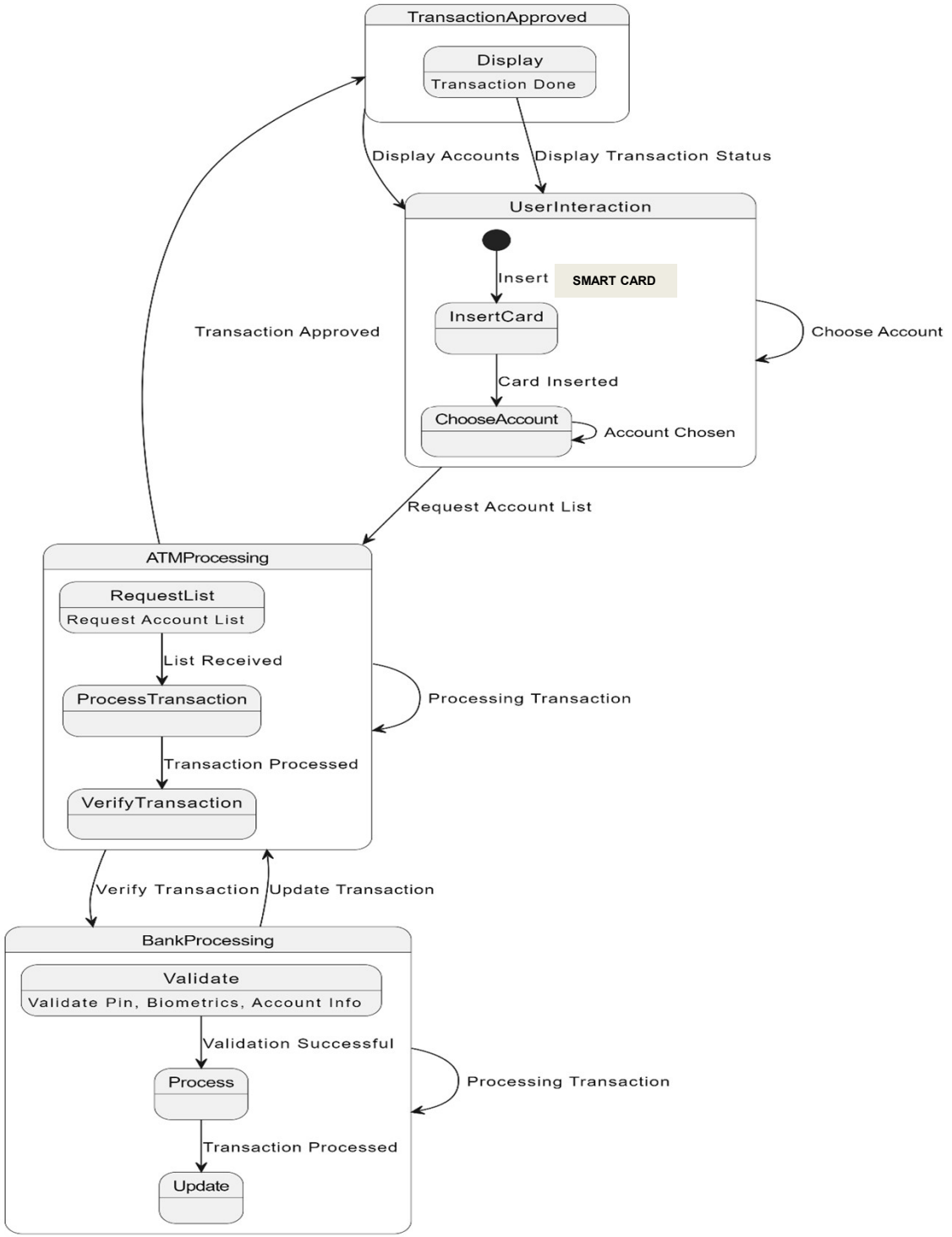
CLASS DIAGRAM:

A class diagram in the UML is a type of static structure diagram that describes the structure of a system by showing the system's classes, their attributes, and the relationships between the classes.



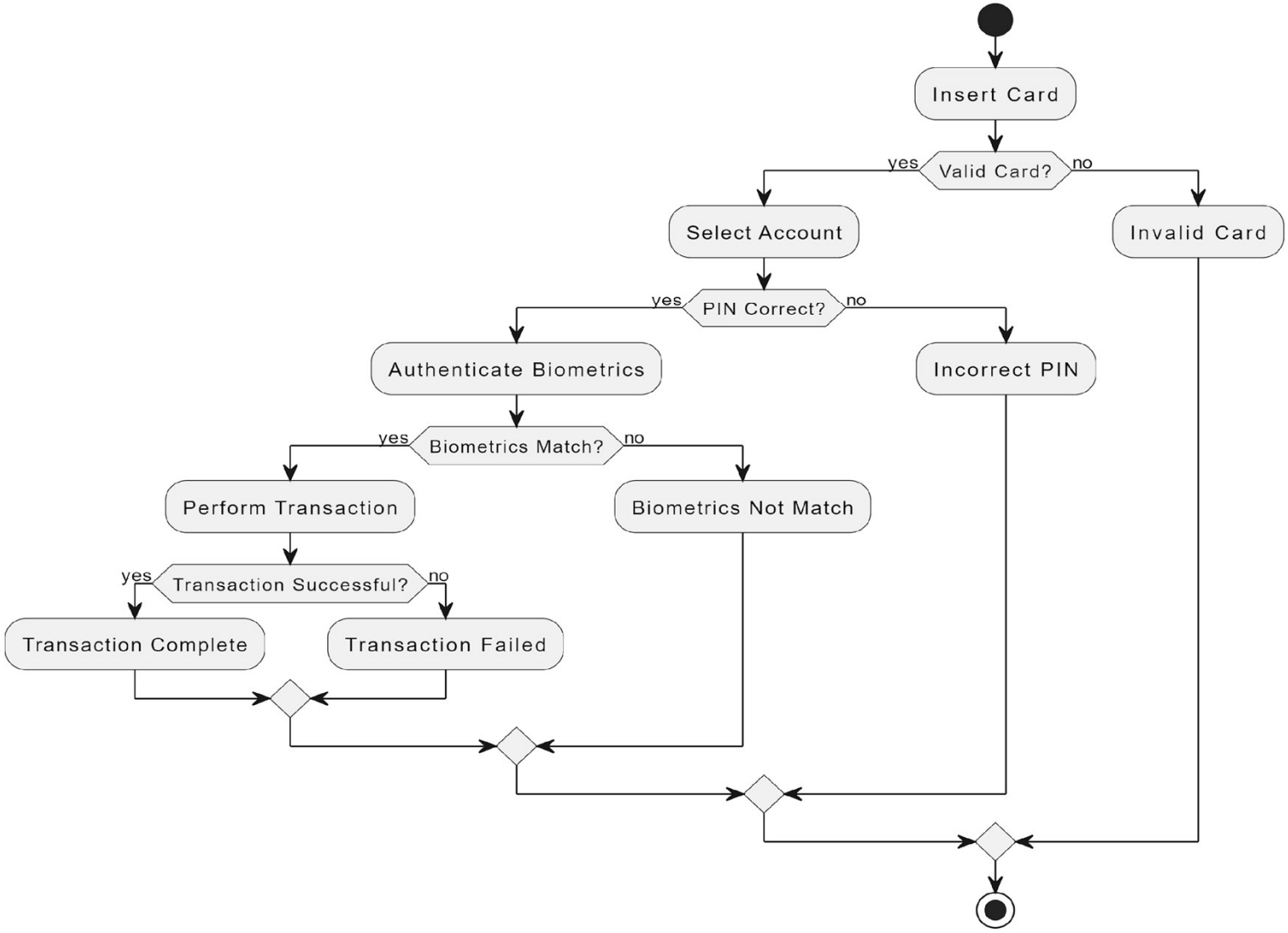
STATE DIAGRAM:

A state diagram is a type of diagram used in computer science and related fields to describe the behavior of systems. State diagrams require that the system described is composed of a finite number of states; sometimes, this is indeed the case, while at other times this is a reasonable abstraction. There are many forms of state diagrams, which differ slightly and have different semantics.



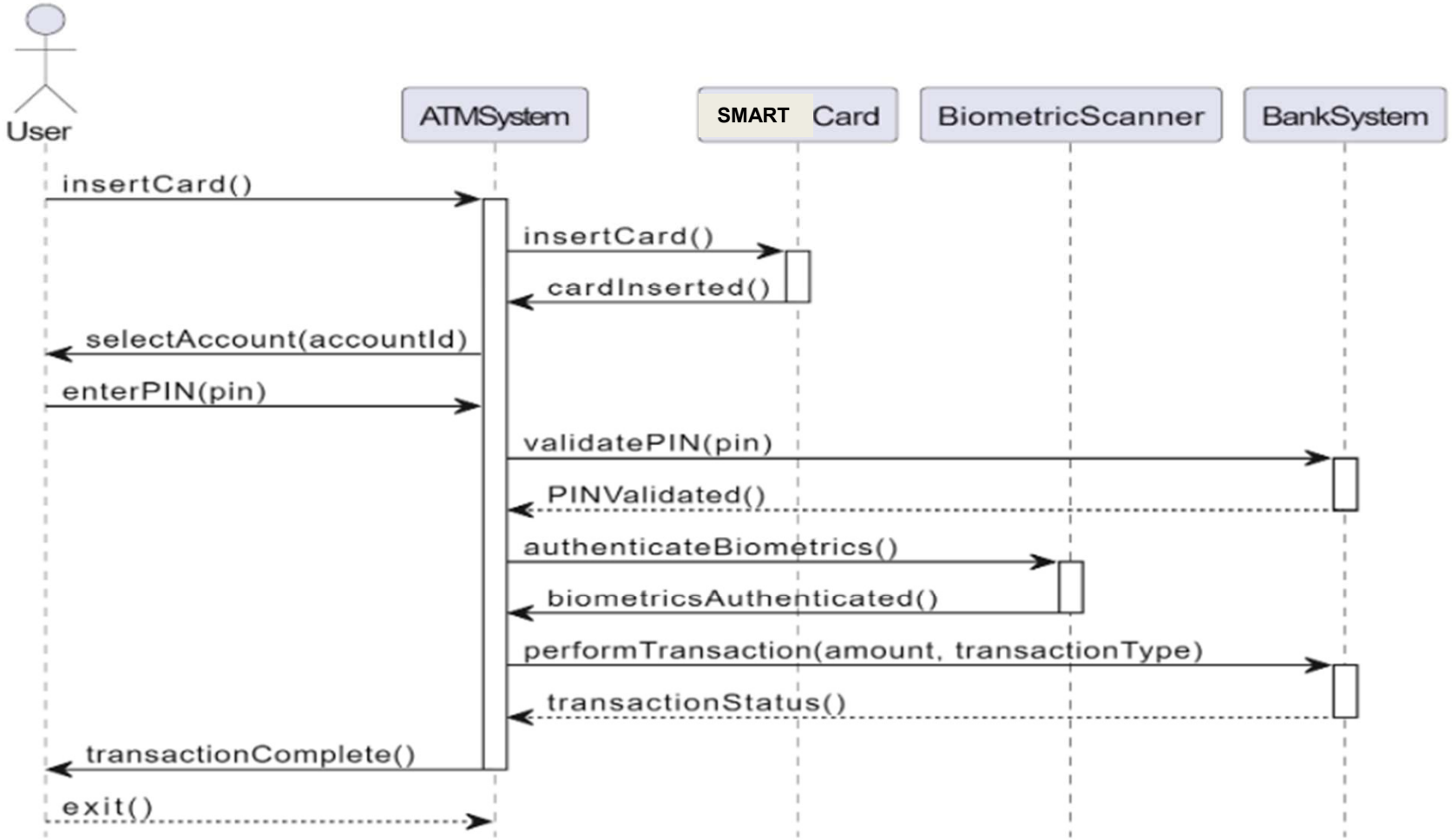
ACTIVITY DIAGRAM:

Activity diagram are a loosely defined diagram to show workflows of stepwise activities and actions, with support for choice, iteration and concurrency. UML, activity diagrams can be used to describe the business and operational step-by-step workflows of components in a system.



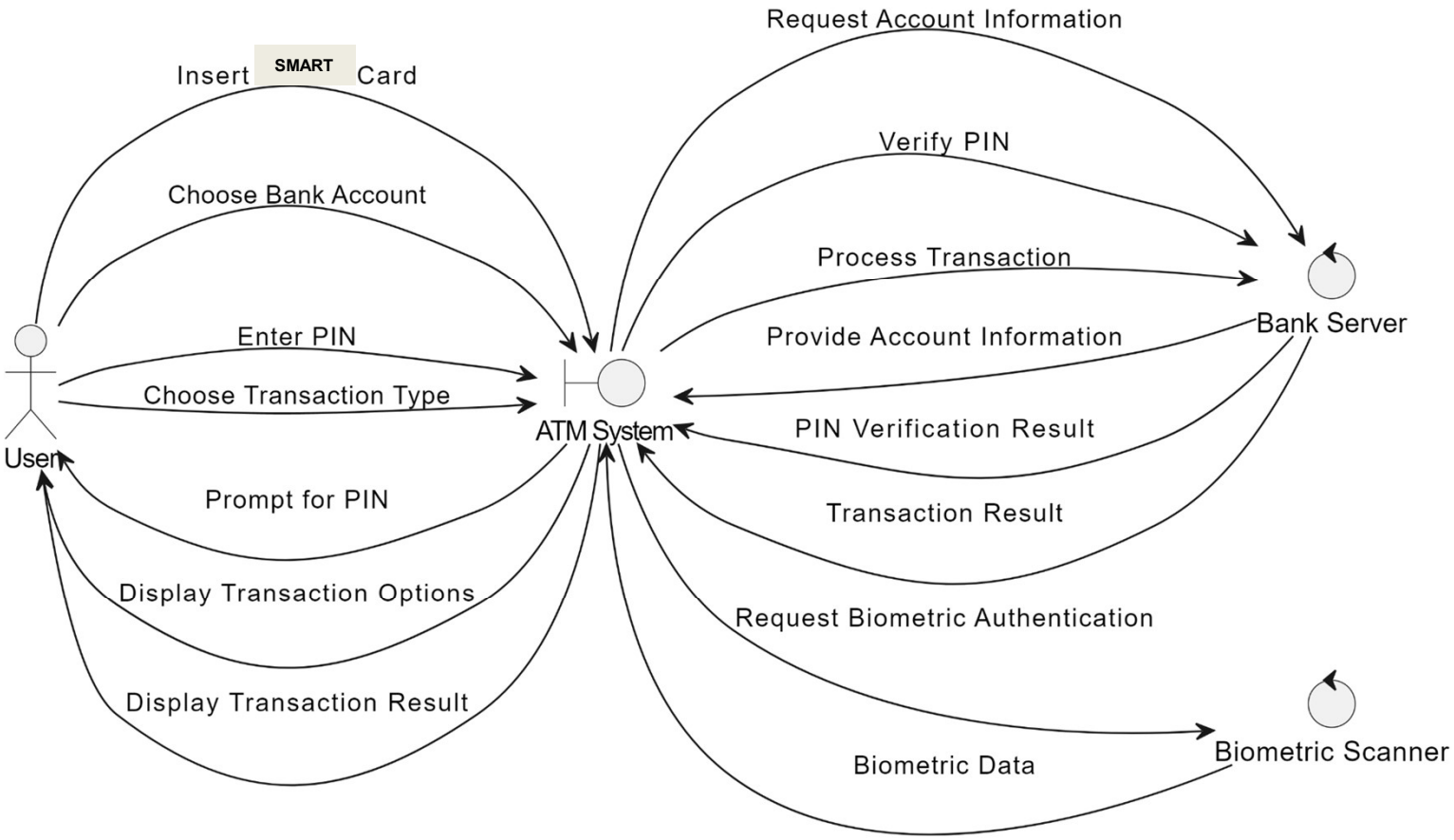
SEQUENCE DIAGRAM:

A sequence diagram in UML is a kind of interaction diagram that shows how the processes operate with one another and in what order.



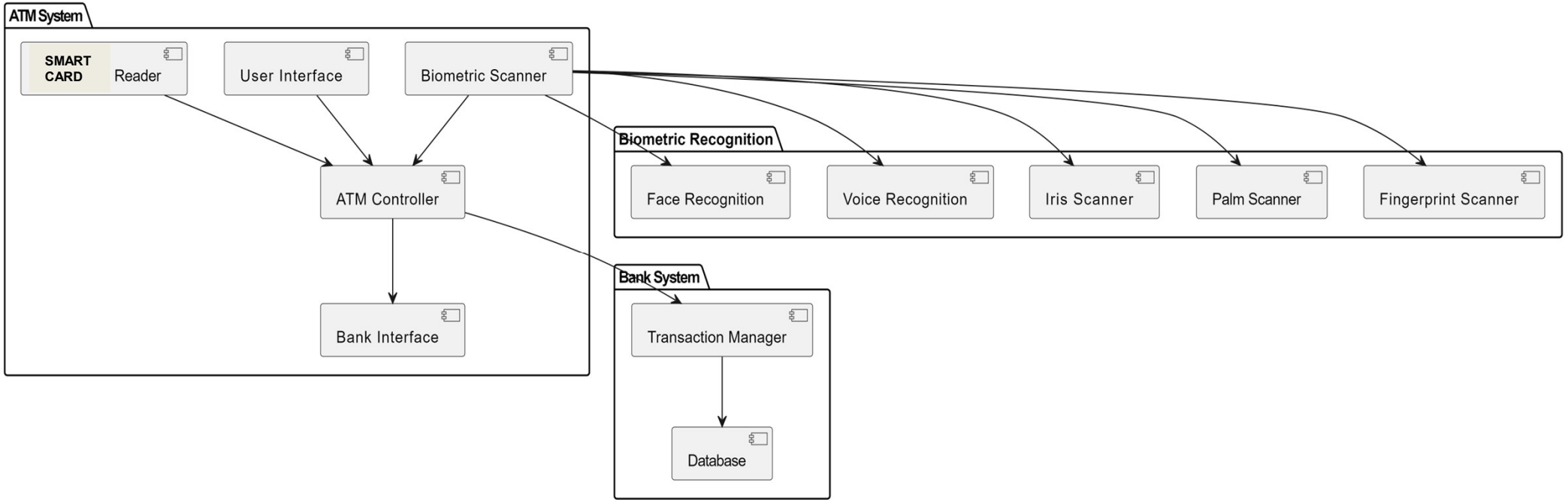
COLLABORATION DIAGRAM:

A collaboration diagram show the objects and relationships involved in an interaction, and the sequence of messages exchanged among the objects during the interaction



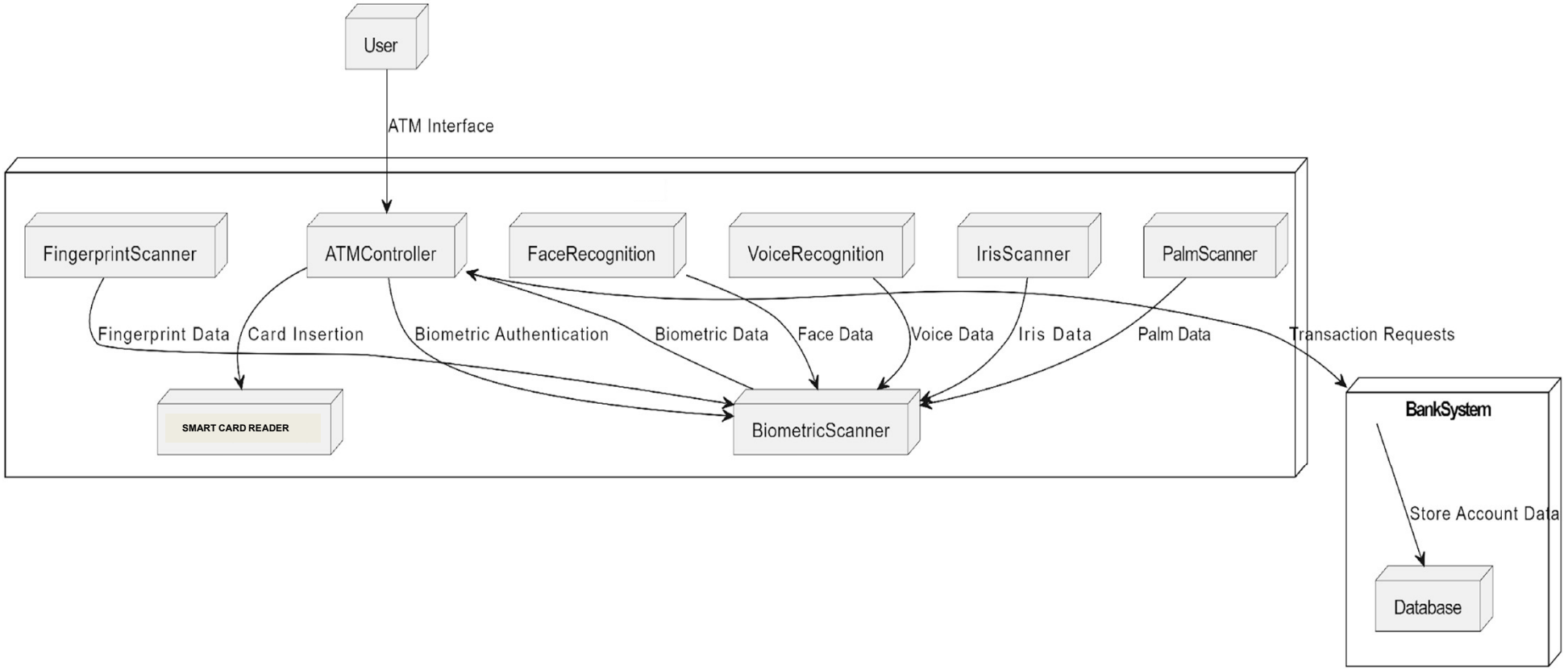
COMPONENT DIAGRAM:

Components are wired together by using an assembly connector to connect the required interface of one component with the provided interface of another component.



DEPLOYMENT DIAGRAM:

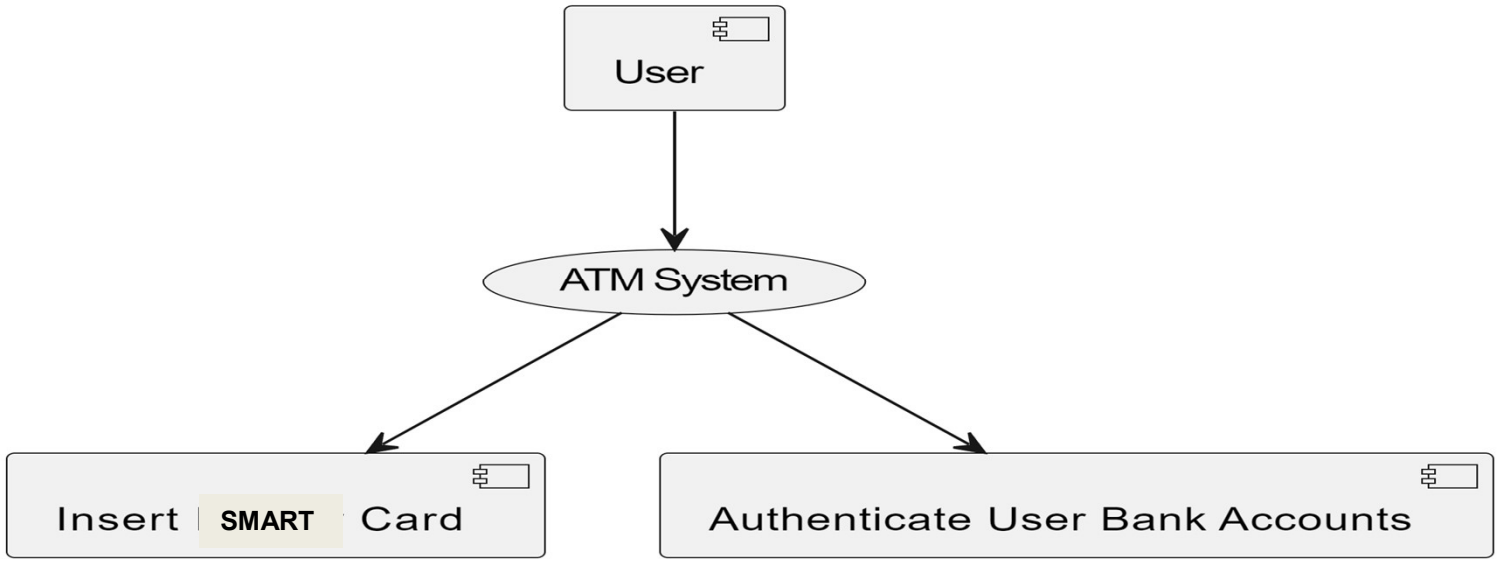
A deployment diagram visually represents the physical deployment of software components on hardware nodes, emphasizing their interconnections and communication paths, offering a concise view of the system's implementation structure.



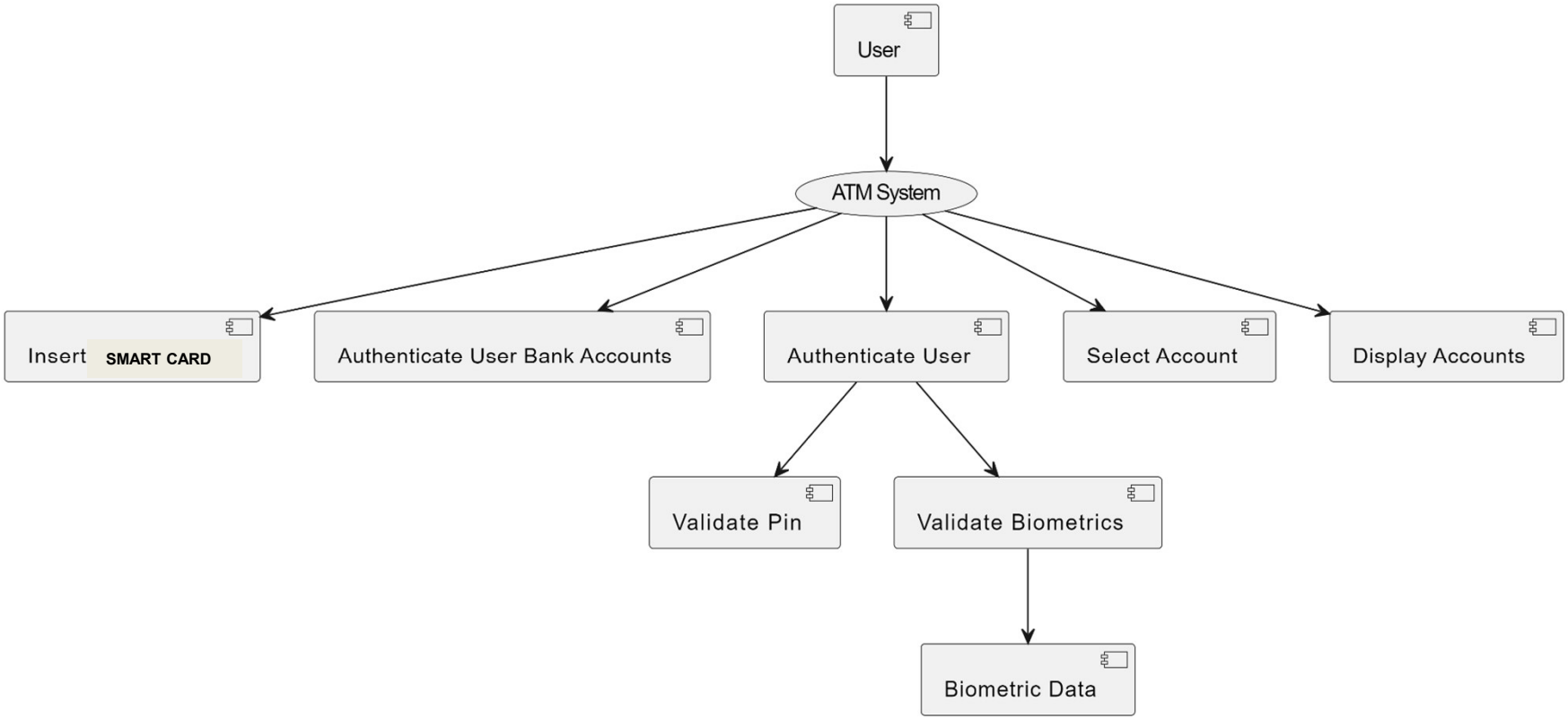
DATA FLOW DIAGRAM:

A data flow diagram (DFD) is a graphical representation of the "flow" of data through an information system. It differs from the flowchart as it shows the data flow instead of the control flow of the program. A data flow diagram can also be used for the visualization of data processing. The DFD is designed to show how a system is divided into smaller portions and to highlight the flow of data between those parts.

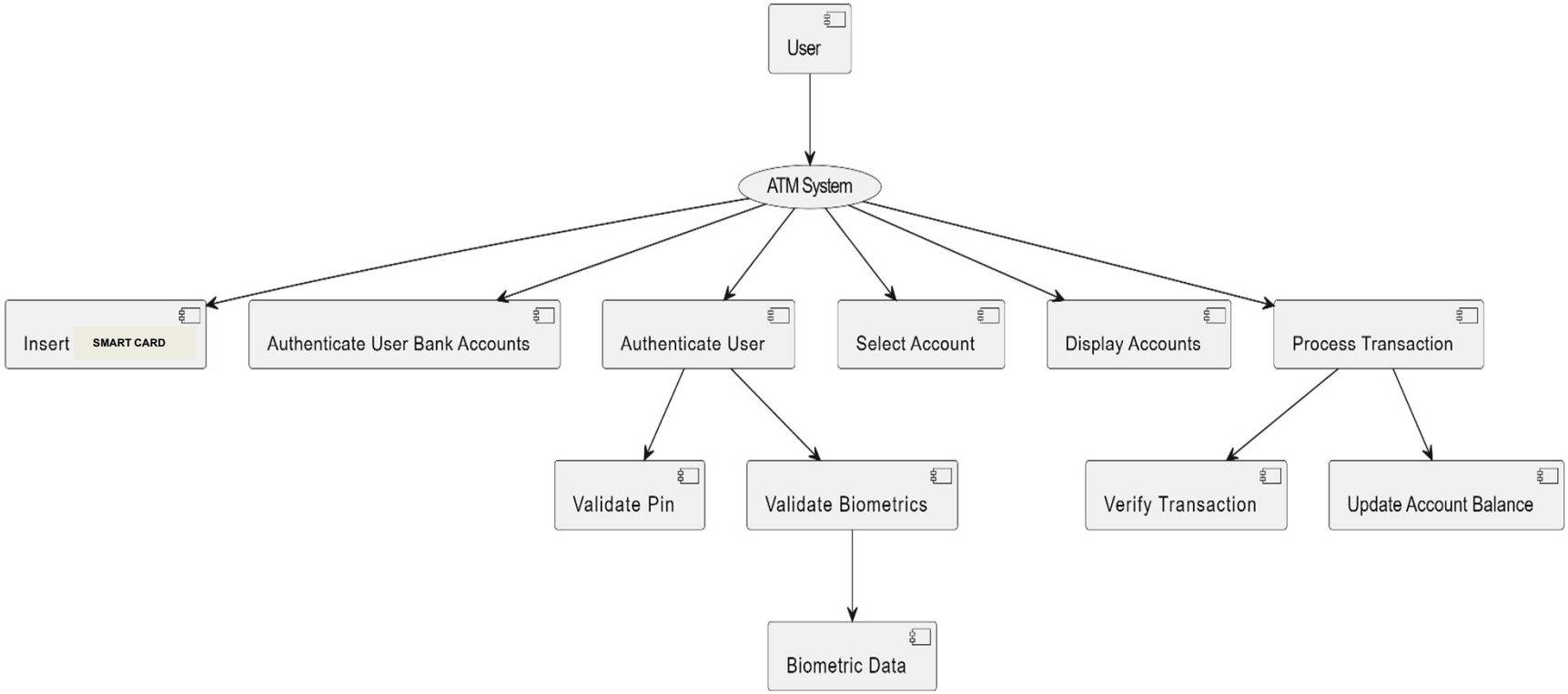
LEVEL 0 : DFD



LEVEL 1 : DFD


User
ATM System
Insert SMART CARD
Authenticate User Bank Accounts
Authenticate User
Select Account
Display Accounts
Validate Pin
Validate Biometrics
Biometric Data

LEVEL 2 : DFD


User
ATM System
Insert SMART CARD
Authenticate User Bank Accounts
Authenticate User
Select Account
Display Accounts
Process Transaction
Validate Pin
Validate Biometrics
Verify Transaction
Update Account Balance
Biometric Data

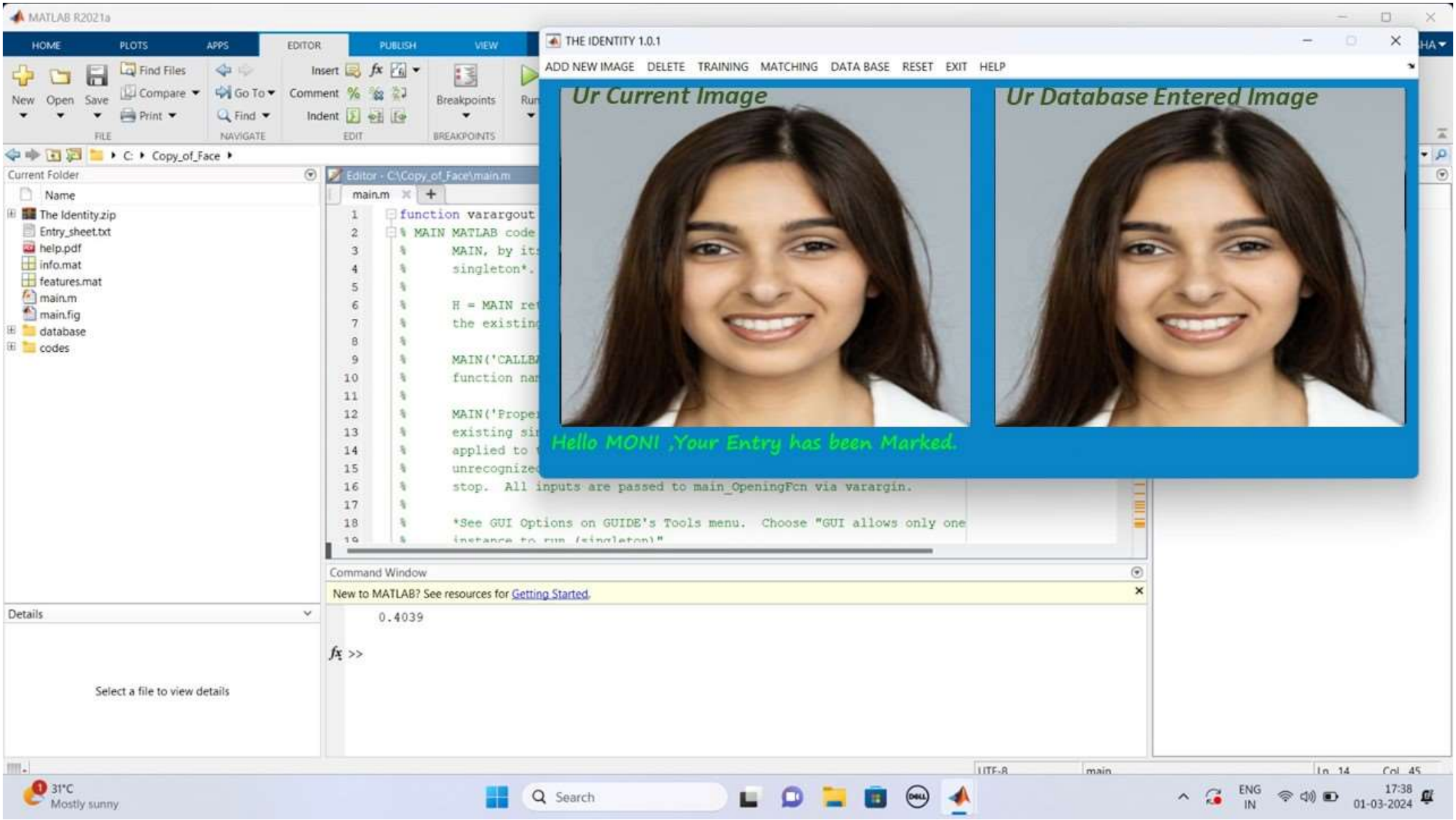
FUTURE ENHANCEMENT

In the future, our project could explore several avenues for enhancement. One potential direction is the incorporation of advanced multi-factor authentication methods to bolster security further. This could involve integrating behavioral biometrics or location-based authentication alongside existing biometric factors like face, fingerprint, iris, voice, and palm recognition. Additionally, you might consider expanding the project's scope to include seamless integration with mobile banking applications, allowing users to manage their accounts and conduct transactions effortlessly from their smartphones. Moreover, leveraging machine learning algorithms could enable the ATM system to deliver personalized user experiences by analyzing individual behavior and preferences. Lastly, staying abreast of emerging biometric technologies, such as vein pattern recognition or heartbeat authentication, could offer even more secure and user-friendly authentication options for future iterations of the project. These enhancements would not only enhance security but also elevate user convenience and satisfaction, shaping the future of banking technology.

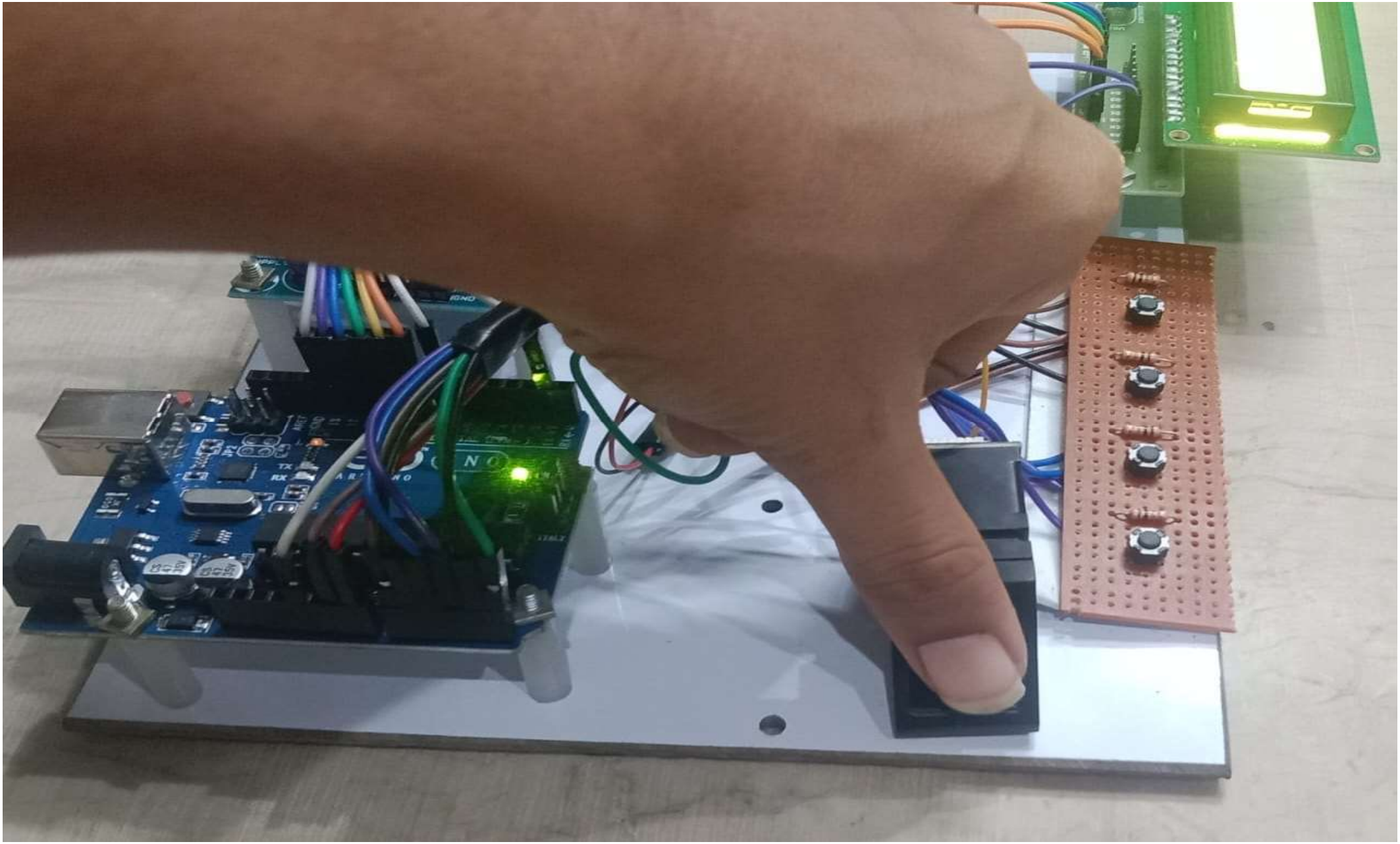
CONCLUSION

In conclusion, the proposed project aims to enhance convenience, security, and accessibility in banking services through the implementation of a Single Master card for multiple bank accounts and advanced biometric authentication at ATMs. By consolidating multiple accounts onto a single card, users can streamline their banking transactions and reduce the need to carry multiple cards.The integration of biometric authentication adds an additional layer of security to ATM transactions, mitigating the risk of unauthorized access and fraud. By requiring multiple biometric factors such as face, fingerprint, iris, voice, and palm recognition, the system ensures a high level of accuracy in verifying the user's identity.Furthermore, the project promotes financial inclusion by making banking services more accessible to individuals from diverse backgrounds, including those with disabilities or limited literacy. The emphasis on user-friendly interfaces and cultural sensitivity in biometric authentication helps to ensure that all users can access and utilize the ATM system effectively.Overall, the project represents a significant advancement in banking technology, offering a secure, efficient, and user-centric solution for managing multiple bank accounts and conducting transactions. As technology continues to evolve, initiatives like this play a crucial role in shaping the future of banking and enhancing the overall customer experience.

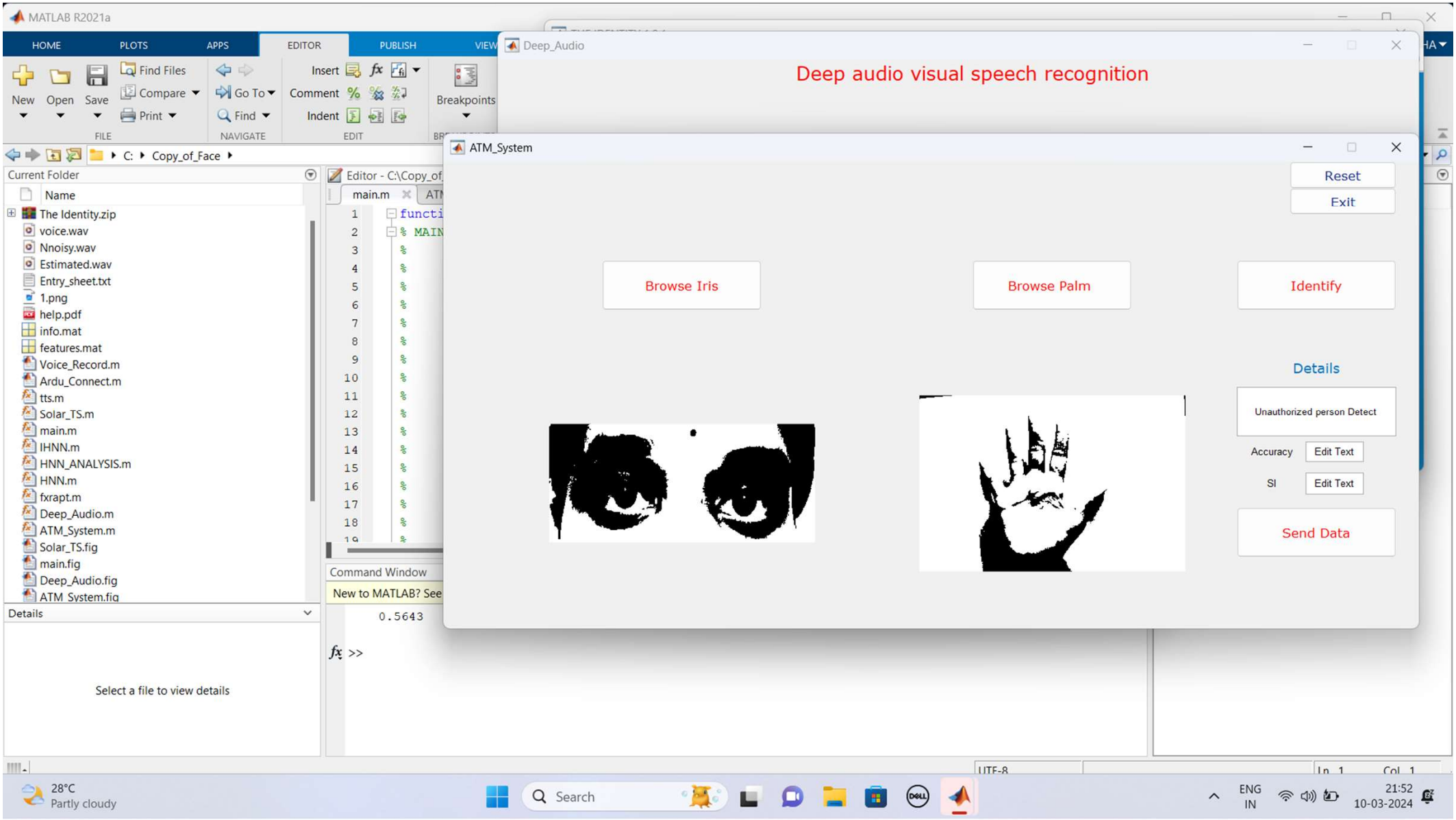
SAMPLE O/P SCREENSHOTS



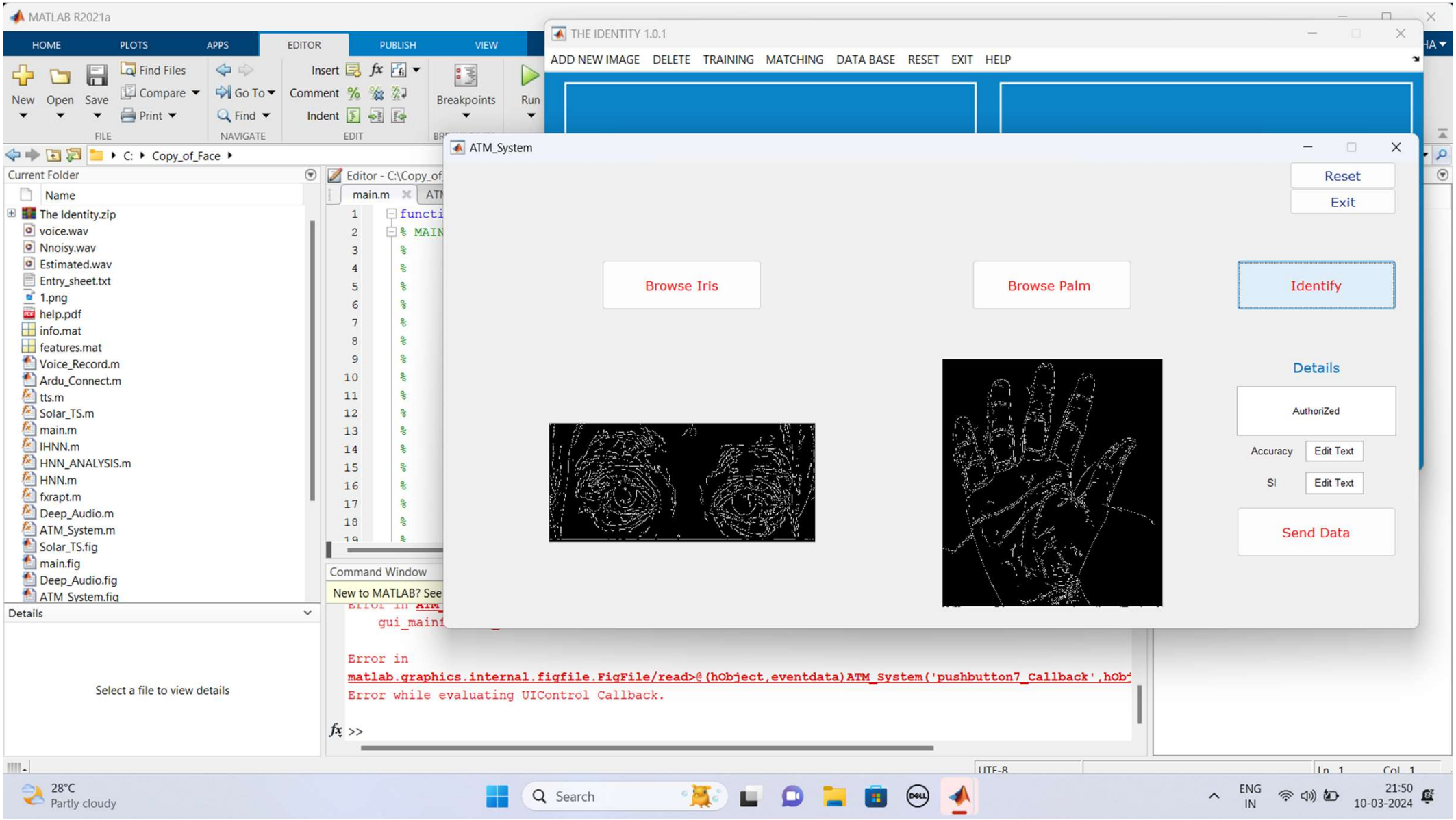
FACE IDENTIFICATION



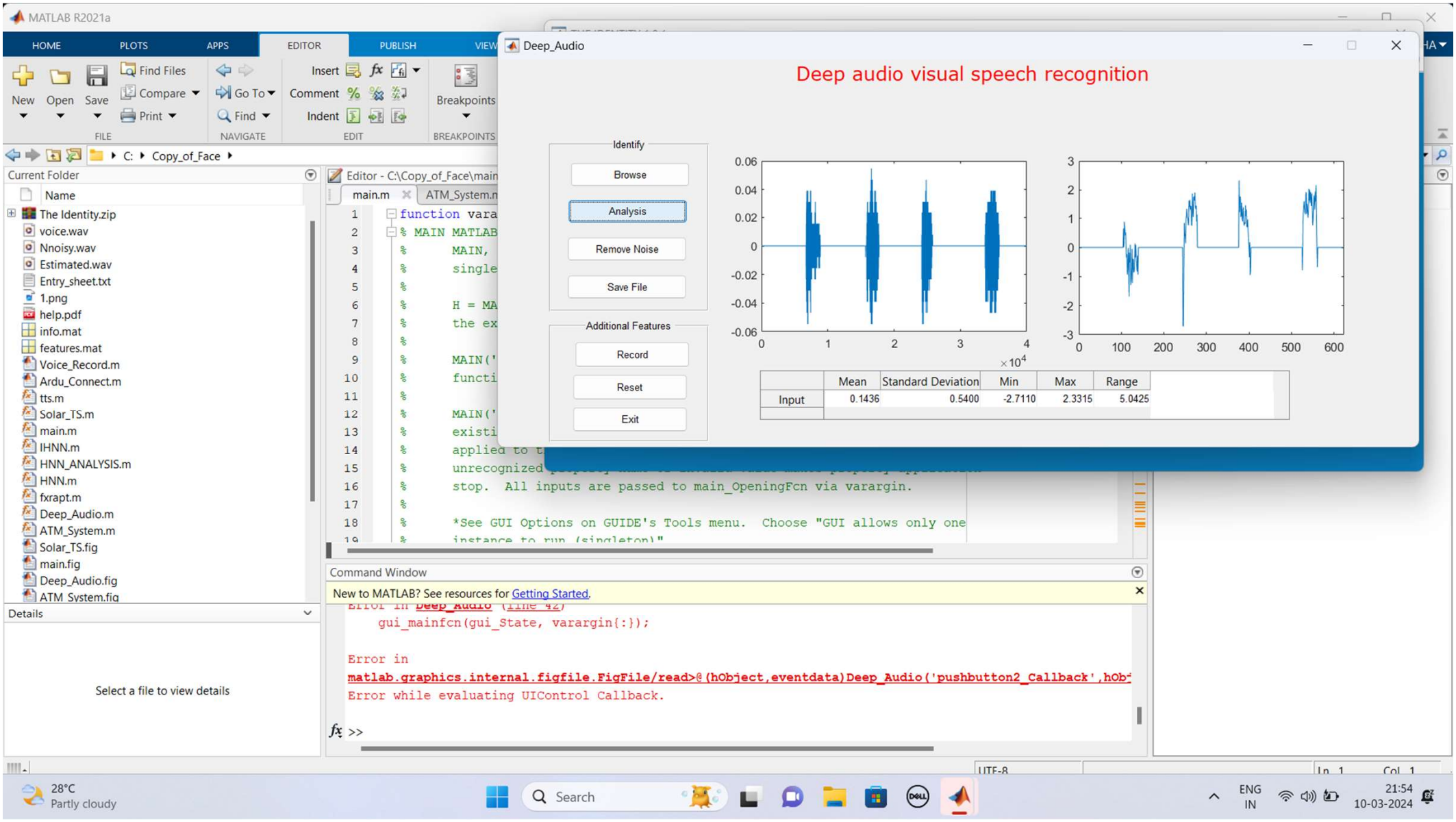
FINGERPRINT IDENTIFICATION



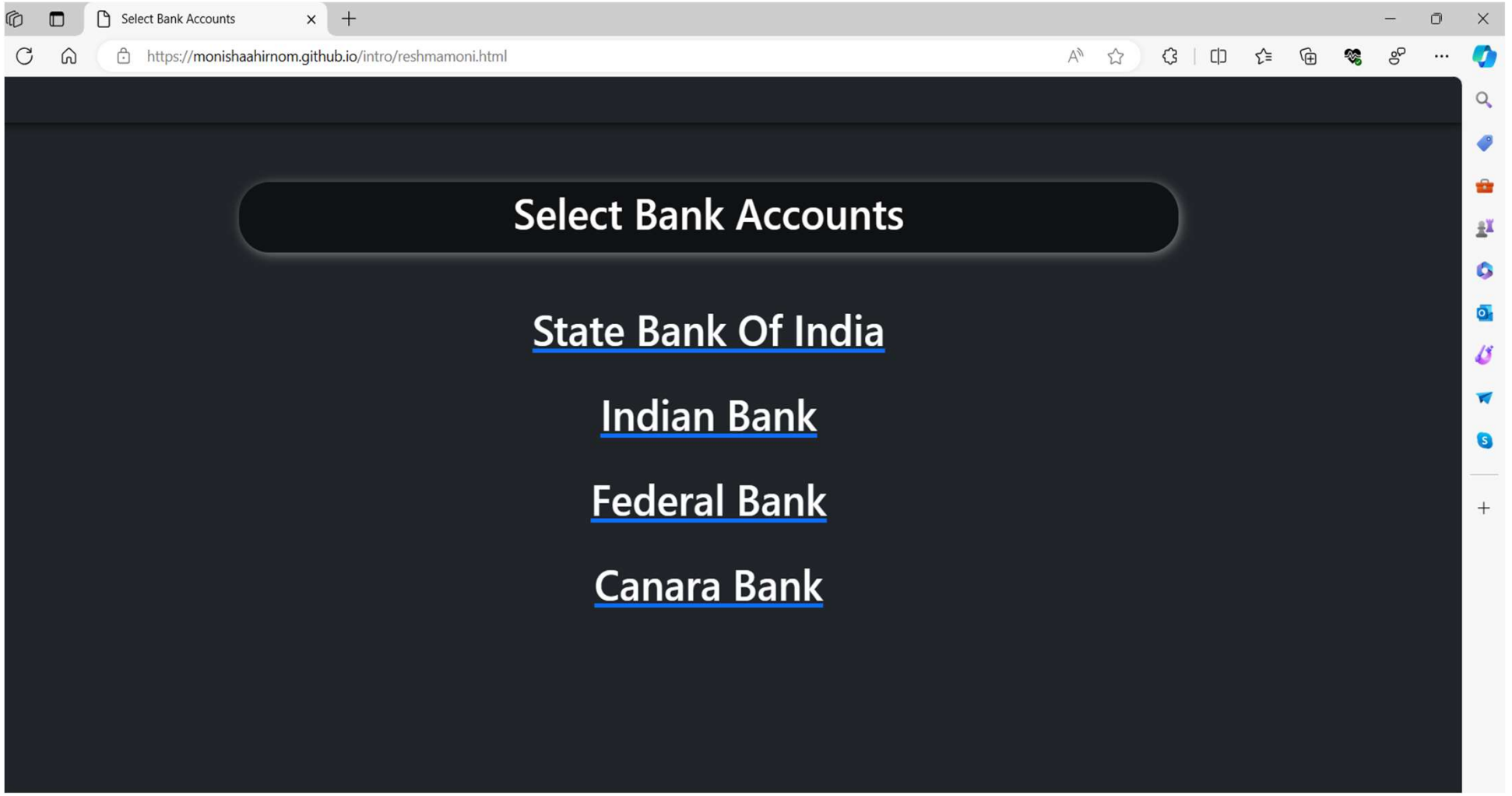
IDENTIFY IRIS AND PALM



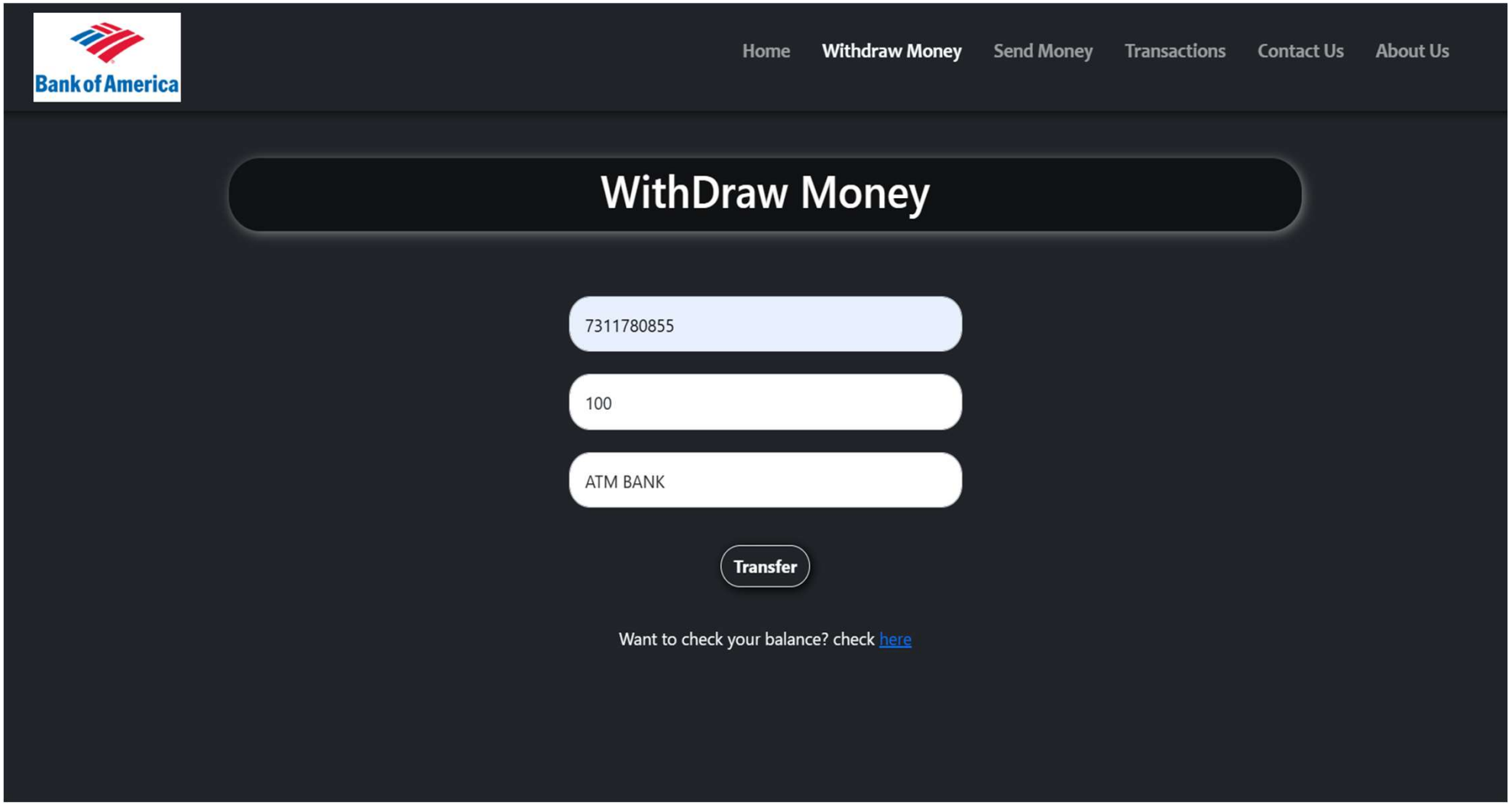
AUTHORIZE IRIS AND PALM



AUDIO AND SPEECH RECOGNITION



SELECTING THE BANK ACCOUNTS



WITHDRAW MONEY FROM ATM

REFERENCES

[1] H. U. Khan, M. Z. Malik, S. Nazir and F. Khan, "Utilizing Bio Metric System for Enhancing Cyber Security in Banking Sector: A Systematic Analysis," in IEEE Access, vol. 11, pp. 80181-80198, 2023, doi: 10.1109/ACCESS.2023.3298824.

[2] N. A. Karim, O. A. Khashan, H. Kanaker, W. K. Abdulraheem, M. Alshinwan and A. -K. Al-Banna, "Online Banking User Authentication Methods: A Systematic Literature Review," in IEEE Access, vol. 12, pp. 741-757, 2024, doi: 10.1109/ACCESS.2023.3346045.

[3] Z. Wang, M. Muhammat, N. Yadikar, A. Aysa and K. Ubul, "Advances in Offline Handwritten Signature Recognition Research: A Review," in IEEE Access, vol. 11, pp. 120222-120236, 2023, doi: 10.1109/ACCESS.2023.3326471.

[4] A. Almadan and A. Rattani, "Benchmarking Neural Network Compression Techniques for Ocular-Based User Authentication on Smartphones," in IEEE Access, vol. 11, pp. 36550-36565, 2023, doi: 10.1109/ACCESS.2023.3265357.

[5] P. Odya, F. Gorski and A. Czyżewski, "User Authentication by Eye Movement Features Employing SVM and XGBoost Classifiers," in IEEE Access, vol. 11, pp. 93341-93353, 2023, doi: 10.1109/ACCESS.2023.3309000.

[6] W. Mu and B. Liu, "Voice Activity Detection Optimized by Adaptive Attention Span Transformer," in IEEE Access, vol. 11, pp. 31238-31243, 2023, doi: 10.1109/ACCESS.2023.3262518.

[7] C. Busch and B. Liu, "Design of a Batteryless, Wireless, and Secure System-on-Chip Implant for In-Body Strain Sensing," 2023 Working Conference on Software Visualization (VISSOFT), Luxembourg, 2023, pp. 125-129, doi: 10.1109/VISSOFT52517.2023.00024.

[8] D. Benalcazar, J. E. Tapia, S. Gonzalez and C. Busch, "Synthetic ID Card Image Generation for Improving Presentation Attack Detection," in IEEE Transactions on Information Forensics and Security, vol. 18, pp. 1814-1824, 2023, doi: 10.1109/TIFS.2023.3255585.

[9] K. Malinka, O. Hujňák, P. Hanáček and L. Hellebrandt, "E-Banking Security Study—10 Years Later," in IEEE Access, vol. 10, pp. 16681-16699, 2022, doi: 10.1109/ACCESS.2022.3149475.

[10] A. Sedik et al., "Deep Learning Modalities for Biometric Alteration Detection in 5G Networks-Based Secure Smart Cities," in IEEE Access, vol. 9, pp. 94780-94788, 2021, doi: 10.1109/ACCESS.2021.3088341.

[11] C. -W. Hung, J. -R. Wu and C. -H. Lee, "Device Light Fingerprints Identification Using MCU-Based Deep Learning Approach," in IEEE Access, vol. 9, pp. 168134-168140, 2021, doi: 10.1109/ACCESS.2021.3135448.

[12] I. Banerjee, S. Mookherjee, S. Saha, S. Ganguli, S. Kundu and D. Chakravarti, "Advanced ATM System Using Iris Scanner," 2019 International Conference on Opto-Electronics and Applied Optics (Optronix), Kolkata, India, 2019, pp. 1-3

[13] S. Gokul, S. Kukan, K. Meenakshi, S. S. V. Priyan, J. R. Gini and M. E. Harikumar, "Biometric Based Smart ATM Using RFID," 2020 Third International Conference on Smart Systems and Inventive Technology (ICSSIT), Tirunelveli, India, 2020, pp. 406-411

[14] D. N. A, A. S, A. Lahari, G. M, P. K N and P. Mugilan, "Smart ATM Card for Multiple Bank Accounts," 2022 International Interdisciplinary Humanitarian Conference for Sustainability (IIHC), Bengaluru, India, 2022, pp. 1228-1232

[15] S. A. Khan and A. A. Abbasi, "Expression-based Security Framework for ATM Networks," 2022 International Conference on Digital Transformation and Intelligence (ICDI), Kuching, Sarawak, Malaysia, 2022, pp. 258-261

QUERIES

THANK YOU