ENHANCING BANKING SECURITY THROUGH MULTIMODAL BIOMETRIC AUTHENTICATION SYSTEM

A PROJECT REPORT

Submitted by

T.MONISHA (411620104011)

J.RESHMA (411620104016)

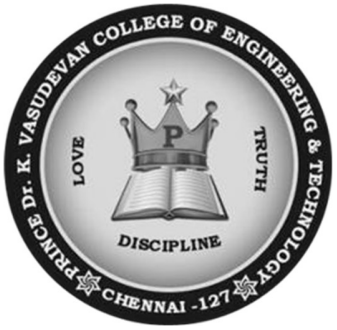
in the partial fulfillment for the award of the degree

of

BACHELOR OF ENGINEERING

IN

COMPUTER SCIENCE AND ENGINEERING



PRINCE Dr.K. VASUDEVAN COLLEGE OF ENGINEERING AND TECHNOLOGY,

PONMAR, CHENNAI-600 127

ANNA UNIVERSITY: :CHENNAI 600 025

MAY 2024

ANNA UNIVERSITY:: CHENNAI 600 025

BONAFIDE CERTIFICATE

Certified that this project report "**ENHANCING BANKING SECURITY THROUGH MULTIMODAL BIOMETRIC AUTHENTICATION SYSTEM"** is the bonafide of **"T.MONISHA (411620104011), J.RESHMA (411620104016)"** who carried out the project work under my supervision.

SIGNATURE

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

HEAD OF THE DEPARTMENT

Department of CSE,
Prince Dr. K. Vasudevan
College of Engineering
And Technology, Ponmar,
Chennai-600127.

SIGNATURE

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

SUPERVISOR

Department of CSE,
Prince Dr. K. Vasudevan
College of Engineering
and Technology, Ponmar,
Chennai-600127.

Submitted for the Project work Viva-voce Examination held on _____

INTERNAL EXAMINER **EXTERNAL EXAMINER**

ACKNOWLEDGEMENT

We wish to express our sincere thanks to our **FOUNDER AND CHAIRMAN, Dr. K. VASUDEVAN, M.A., B.Ed., Ph.D.,** for his endeavor in educating us in his premier institution.

We would like to extend our heartfelt gratitude and sincere thanks to our **VICE–CHAIRMAN, Dr. V. VISHNU KARTHIK, M.D.,** for his keen interest in our studies and the facilities offered in this premier institution.

We would like to express our deep gratitude and sincere thanks to our **ADMINISTRATIVE OFFICER, Er. K. PARTHASARATHY, B.E.,** for his valuable support.

We wish to express our sincere thanks to our **HONOURABLE PRINCIPAL, Dr. T. SUNDER SELWYN, M.E., Ph.D.,** for permitting access to various resources in the college to complete the project work.

We would like to express our sincere thanks, gratitude and indebtedness to our beloved **Mrs.S.SHALINI M.E.,(Ph.D)., HOD** and **our project coordinator, Department of Computer science and Engineering** who motivated and encouraged us for the completion of our project successfully.

We wish to express our great deal of gratitude to our Internal Guide, **Mrs.S.SHALINI M.E.,(Ph.D).,** Department of Computer Science and Engineering for her guidance given throughout this project.

We would like to extend our thanks to all teaching and non-teaching staff of the Department of Computer Science and Engineering for their support.

ABSTRACT

Our 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, an 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.

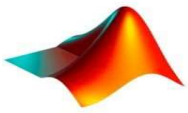
This system revolutionizes ATM transactions by introducing a sophisticated multi-modal biometric authentication approach. Leveraging face recognition, fingerprint, voice, palm, and iris scanning, users can securely access and withdraw money. The system integrates arduino as a microcontroller, RFID technology for user identification, an LCD display for seamless interaction, and MATLAB for biometric processing. This innovative solution enhances security, mitigates risks associated with PINs and card theft, and provides a user-friendly experience.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF SYMBOLS

NAME OF SYMBOLS	SYMBOLS
MATLAB	
OPEN CV	

LIST OF ABBREVIATIONS

ABBREVIATIONS	EXPLANATION OF ABBREVIATION
ATM	Automated Teller Machine
MATLAB	MATrix LABoratory
OPENCV	Open Source Computer Vision
RFID	Radio-Frequency Identification
PIN	Personal Identification Number
GUI	Graphical User Interface
UML	Unified Modelling Language
PAD	Presentation Attack Detection
VAD	Voice Activity Detection
SET	Secure Electronic Transaction

CHAPTER 1

INTRODUCTION

1.1 DOMAIN INTRODUCTION

In the face of ever-evolving cyber threats, cybersecurity professionals must remain vigilant, continuously adapting their strategies to mitigate emerging risks and vulnerabilities. This necessitates a proactive approach that includes robust risk assessment, threat intelligence gathering, and the implementation of effective security controls. Collaboration and information sharing within the cybersecurity community are essential for staying abreast of evolving threats and developing effective countermeasures. Furthermore, cybersecurity is not solely a technical discipline; it also encompasses aspects of organizational culture, governance, and user awareness. Ultimately, in the domain of cybersecurity, the pursuit of innovation must be balanced with a steadfast commitment to safeguarding the confidentiality, integrity, and availability of critical information assets. Face detection is a crucial component of biometric authentication systems, leveraging computer vision algorithms to identify and localize human faces within images or video streams. By analyzing facial features such as the eyes, nose, and mouth, face detection technology enables the recognition and verification of individuals, offering a non-intrusive and user-friendly method to identify users. Fingerprint detection, a cornerstone of biometric authentication, relies on capturing and analyzing unique patterns present in an individual's fingerprints. This module utilizes specialized sensors to capture high-resolution images of fingerprint ridges and valleys, enabling the extraction of distinctive features for identification and verification purposes. With its widespread adoption in various security applications, fingerprint detection offers a reliable and efficient means of confirming user identity. Iris detection involves the

capture and analysis of the unique patterns present in the iris of the human eye. By leveraging the inherent stability and complexity of iris patterns, iris detection provides a highly accurate and secure method for biometric authentication, resistant to spoofing and tampering attempts. Palm detection technology focuses on capturing and analyzing the distinctive characteristics of the palm of the hand for biometric identification and verification. This module utilizes advanced imaging techniques to capture palm prints, including ridges, creases, and unique patterns. Palm detection offers a versatile and reliable biometric authentication solution, particularly suitable for scenarios where other biometric modalities may not be feasible or effective. Voice recognition, also known as speaker recognition, is a biometric authentication method that analyzes and identifies unique vocal characteristics and patterns in an individual's speech. This module employs sophisticated algorithms to extract features such as pitch, tone, and pronunciation from audio samples, enabling the creation of distinctive voiceprints for each user. With its widespread applicability and ease of use, voice recognition provides a convenient and secure means of identity authentication, particularly in hands-free and remote authentication scenarios.

1.2 PROBLEM DEFINITION

In the realm of cybersecurity and financial transactions, the demand for secure and convenient authentication methods continues to escalate. Traditional authentication mechanisms, such as PINs and passwords, are susceptible to various vulnerabilities. In response, there is a pressing need for innovative solutions that bolster security while enhancing user experience. This project seeks to address this need by developing a robust biometric authentication system for ATM transactions. Leveraging multiple biometric modalities including face detection, fingerprint detection, iris detection, palm detection, and voice recognition, the system aims to establish a formidable authentication framework.

Furthermore, the integration of four individual bank cards into a single smart card adds a layer of convenience for users, allowing access to multiple bank accounts seamlessly. Key challenges include ensuring the accuracy, reliability, and security of biometric data, while also adhering to regulatory standards governing financial transactions and data privacy. By addressing these challenges, the project endeavors to redefine the landscape of ATM security, offering a secure, user-friendly, and streamlined authentication experience for individuals and financial institutions alike.

1.3 PROJECT DESCRIPTION

The project involves the development of a comprehensive biometric authentication system tailored for ATM transactions, aimed at bolstering security, improving user experience, and ensuring compliance with regulatory standards. Central to the system's architecture is the conversion of four individual bank cards into a single smart card, which will serve as the gateway to accessing multiple bank accounts securely. In the domain of cybersecurity and transaction security, ensuring the integrity, confidentiality, and availability of digital assets is paramount. Traditional methods of authentication, such as PINs and passwords, are susceptible to various vulnerabilities, including brute force attacks, phishing, and social engineering. To address these challenges and enhance the security of financial transactions, there is a growing demand for innovative biometric authentication solutions. The objective of this project is to design and implement a secure biometric authentication system for ATM transactions, utilizing multiple biometric modalities such as face detection, fingerprint detection, iris detection, palm detection, and voice recognition. Additionally, the project aims to integrate the functionality of four individual bank cards into a single smart card, streamlining access to multiple bank accounts while maintaining robust security measures.

CHAPTER 2

LITERATURE REVIEW

1. 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 : 2023

This paper reviews contemporary user authentication methods in online banking, including Knowledge-Based Authentication (KBA), (BBA) Biometrics-Based Authentication, and Possession-Based Authentication (PBA). It explores associated cyber threats like malware and phishing attacks. Insights from popular banks are examined, emphasizing the evolving need for robust security measures. 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 counts effectively. Authentication algorithms under online banking security. Whether utilizing biometric scans, knowledge-based queries, or possession verification, these algorithms validate user identity. Balancing efficiency and resilience, these algorithms contribute to the evolving landscape of secure online transactions. It delves into related online dangers such as ransomware and phishing campaigns. Strong security measures are increasingly needed, as seen by the insights from well-known businesses that are analyzed. Verifying identity using a variety of techniques, including KBA, BBA, and PBA, is known as user authentication in online banking.

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

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

YEAR : 2023

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.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. Deep learning methods take center stage in this review, showcasing their prevalence in advancing offline handwritten signature recognition. The paper discusses different architectures employed in recent years, highlighting how these algorithms contribute to the identification of individuals through their handwritten signatures. The paper underscores the advantages of incorporating deep learning methods in offline handwritten signature recognition. It acknowledges the evolving nature of research, providing insights into improved identification accuracy, efficiency, and adaptability to diverse document authentication scenarios. The study examines several architectures used recently, emphasizing the ways in which these algorithms aid in the identification of people based on their handwritten signatures. The research emphasizes the incorporation of deep learning techniques while providing a thorough analysis of the state of offline handwritten signature detection.

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

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

YEAR : 2023

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. 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. The study employs Support Vector Machine (SVM) and eXtreme Gradient Boosting (XGBoost) classifiers to authenticate users based on eye movement data. XGBoost demonstrates superior performance with lower equal error rates and higher true acceptance rates compared to SVM. Contactless eye trackers offer a secure and convenient means of user authentication. The study highlights the advantages of employing eye movement features, emphasizing the non-intrusive nature of the technology and its ability to confirm user identity and liveness effectively. With regard to the Covid epidemic in particular, it highlights the benefits of contactless eye trackers as a means of safe identity verification and user liveness confirmation. According to the research, using eye tracking features has several benefits. It also emphasizes how discrete the technology is and how well it can verify user legitimacy and authenticity. Eye trackers that function without contact provide a safe and practical way to authenticate users.

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

AUTHOR: A. Almadan, A. Rattani

YEAR : 2023

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. 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.The study explores various neural network compression techniques, both standalone and in combination, to enhance the efficiency of ocular-based user authentication on smartphones. The algorithms are assessed and benchmarked for their effectiveness in reducing computational complexity and model size. The project highlights the advantages of neural network compression techniques in making ocular-based user authentication models more suitable for on-device deployment on resource-constrained smartphones. Achieving efficiency ensures secure and convenient user authentication without overwhelming computational demands. The efficiency of the techniques in lowering model size and computational complexity is evaluated and compared in an significant manner. This idea seeks to utilize deep learning models for user authentication in a way that strikes a balance between computing efficiency, security, and accuracy.

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

AUTHOR: B. Liu , W. Mu

YEAR : 2023

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.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.AAT-VAD employs a novel method integrating adaptive width attention learning into the transformer framework. This involves processing MFCC features through transformer encoder layers with attention heads, ultimately enhancing the efficiency and accuracy of voice activity detection in diverse noise conditions. AAT-VAD exhibits substantial advantages, achieving a 12.8% higher F1-score compared to DCU-10 and a 0.6% higher F1-score compared to Tr-VAD in the presence of different noise interferences. Additionally, the method significantly reduces the average detection cost function (DCF) and test time, outperforming existing VAD approaches. Voice Assignment Recognition through the transformer framework's integration of an adaptive width attention learning technique. This method seeks to improve lengthy audio signal performance.

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

AUTHOR: C. Busch, B. Liu

YEAR : 2023

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. 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.The System-on-Chip (SoC) implant employs a reconfigurable in-body rectenna, an energy-efficient strain sensing front-end, AES-GCM security, and closed-loop wireless programming. These features collectively enhance functionality, adaptability to surrounding tissues, and secure data transmission for in-body strain sensing. The proposed SoC implant offers advancements in in-body strain sensing with features like reconfigurable rectenna, energy-efficient sensing, and secure data transmission. It achieves area-efficient random number generation and faster settling times below 2 seconds, providing a robust and versatile solution for long-term biomedical monitoring. When combined, these characteristics improve functioning, tissue adaptation, and secure data transfer for in-body stress detection. By introducing a System-on-Chip (SoC) implant intended for in-body strain monitoring, the initiative innovates.

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

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

YEAR : 2023

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.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.The project utilizes computer vision algorithms and Generative Adversarial Networks (GANs) for synthetic ID card image generation. These algorithms enable the creation of realistic-looking images, augmenting datasets for training fraud-detection networks without relying on real identity documents, thus addressing privacy concerns. Synthetically generated ID card images supplement training datasets for fraud-detection networks without compromising privacy. The project demonstrates improved performance in detecting fake identity documents, maintaining efficiency in print/scan Presentation Attack Instrument Species (PAIS) and minimal performance loss in screen capture PAIS scenarios. It investigates techniques for creating ID card images artificially in order to supplement datasets used in fraud-detection network training, hence improving performance without sacrificing privacy.In order to strengthen datasets for training fraud-detection networks.

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

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

YEAR : 2022

This project revisits e-banking security after a decade, examining the evolution of authentication schemes and legislation, notably the impact of the Payment Services Directive (PSD2) in the European Union. The study provides an overview of current authentication methods, their compliance with international standards, resistance against attacks, and multi-factor authentication schemes in line with PSD2 requirements. An e-banking attacks taxonomy is introduced to enhance understanding in this evolving field.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.While specific algorithms are not mentioned, the project focuses on evaluating authentication methods and multi-factor authentication schemes in the context of e-banking security. It emphasizes compliance with international standards, resistance to attacks, and alignment with PSD2 requirements. The study provides an updated understanding of e-banking security, considering the evolution of authentication schemes and the impact of PSD2. It offers a comprehensive tool, the e-banking attacks taxonomy, to navigate through the complexities of e-banking security, addressing a broad audience from business executives to specialists. The effort provides a thorough analysis of existing authentication mechanisms, their conformity with worldwide requirements, and their resilience against attacks. It also reassesses the security of online banking with PSD2, or the Payments.

9. 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 : 2021

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.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. The project employs deep learning models, specifically convolutional neural networks (CNN) and a hybrid CNN-ConvLSTM model. These models compute a three-tier probability for detecting alterations to biometric modalities, providing accuracy in identifying pristine, adulterated, and fake biometrics in 5G-based smart cities.The proposed system ensures secure transactions and protects user identities in 5G-based smart cities. Utilizing deep learning, it achieves high accuracy in detecting alterations to biometric modalities, particularly excelling in identifying central rotation alteration to fingerprints, making it a robust solution for biometric authentication applications. In 5G-based smart city applications, the technology provides improved security and authentication by evaluating the likelihood of biometric manipulation.A hybrid CNN-ConvLSTM model and convolutional neural networks (CNN) are the deep learning models used in this research.

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

AUTHOR : Jun-Rong Wu, Ching-Hung Lee

YEAR : 2021

We introduce device identification using the light fingerprint by a MCU-based deep learning approach. At first, we observe that minor differences exist for individual components of lighting equipment. 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. The screen light of the mobile phone is analyzed to obtain the features of unique light fingerprints. We utilize the convolutional neural network, the improved multi-class greedy autoencoder and variational autoencoder with domain adaptation techniques to develop the identification algorithm. Finally, the Bayesian optimization technique is used to optimize the hyper-parameters of models for implementing in the microprocessor. The corresponding comparisons are introduced to demonstrate the performance. The multi-class greedy autoencoder algorithm produces results with an overall accuracy rate and abnormal sample detection rate of 99.67% and 99.85%, respectively. 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. Also, there is increased flexibility in real-world applications and room to grow into new domains, such robotics automation and smart buildings.

CHAPTER 3

SYSTEM ANALYSIS

3.1 EXISITING SYSTEM

The current system for ATM transactions predominantly relies on conventional authentication methods, primarily centered around Personal Identification Numbers (PINs) and magnetic stripe cards. While these methods have demonstrated a degree of effectiveness, they are not without their shortcomings, particularly concerning security. Challenges such as PIN theft and card skimming have emerged as significant concerns, highlighting vulnerabilities inherent in the system. Moreover, the reliance on single-factor authentication, namely the combination of PINs and magnetic stripe cards, leaves the system susceptible to unauthorized access and fraudulent activities. Furthermore, the absence of advanced biometric features in the authentication process limits the range of options available for user verification, hindering the implementation of more robust security measures. As such, there exists a pressing need for the adoption of more secure and sophisticated authentication methods to enhance the security and integrity of ATM transactions. In addition to the security vulnerabilities posed by traditional authentication methods in ATM transactions, there are further concerns regarding the potential for technological advancements to outpace the security measures in place. As cyber threats evolve and become more sophisticated, the existing system may struggle to keep pace with emerging security challenges. Moreover, the reliance on static identifiers such as PINs and magnetic stripe cards makes the system inherently less adaptable to dynamic security requirements. Furthermore, the lack of multi-factor authentication in the current system means that compromised credentials can result in significant security breaches with minimal barriers for malicious actors. This underscores the importance of

implementing more robust security measures, such as biometric authentication or token-based authentication, to fortify the system against emerging threats and safeguard sensitive user information. Additionally, enhancing user awareness and education about security best practices can further mitigate the risks associated with ATM transactions and foster a more secure banking environment for all users.

3.1.1 DISADVANTAGES OF EXISTING SYSTEM

The current ATM system is heavily reliant on single-factor authentication methods, predominantly centered around Personal Identification Numbers (PINs) and magnetic stripe cards. While these methods have been effective to some extent in verifying user identity, they also present significant security vulnerabilities. PIN theft and card skimming have emerged as notable concerns within the existing system, highlighting the susceptibility of these traditional authentication methods to exploitation by malicious actors. Moreover, the absence of advanced biometric features further compounds the security challenges, as it limits the effectiveness of security measures in preventing unauthorized access and fraudulent transactions. This reliance on static identifiers leaves user accounts and transactions vulnerable to compromise, posing risks to both individuals and financial institutions. As such, there is a pressing need for the adoption of more robust authentication mechanisms, such as biometric authentication, to bolster security and enhance user trust in the ATM system. Although these techniques have been somewhat successful in confirming the identity of users, they also have serious security flaws. PIN stealing and card skimming have become prominent issues in the current system, indicating how vulnerable these conventional authentication techniques are to abuse by malevolent parties.

3.2 PROPOSED SYSTEM

The proposed system marks a groundbreaking shift in ATM transactions through the implementation of a sophisticated multi-modal biometric authentication approach. By harnessing various biometric modalities including face recognition, fingerprint, voice, palm, and iris scanning, users can securely access and withdraw money, significantly enhancing security and user authentication. The integration of Arduino as a microcontroller, RFID technology for user identification, an LCD display for intuitive interaction, and MATLAB for biometric processing further solidifies the system's robustness and usability. This innovative solution not only addresses the inherent vulnerabilities associated with traditional PINs and card theft but also provides a seamless and user-friendly experience for ATM users. The Arduino microcontroller efficiently manages data processing tasks, while MATLAB ensures the accuracy and reliability of biometric authentication, signifying a significant advancement in both ATM security and usability. In addition to its multi-modal biometric authentication capabilities, the proposed system offers several other notable features that enhance its functionality and usability. One such feature is the integration of RFID (Radio Frequency Identification) technology for user identification, which adds an extra layer of security by verifying the user's identity through a unique RFID tag or card. Furthermore, the utilization of an LCD display facilitates clear and intuitive interaction, providing users with prompts and feedback throughout the transaction process. Moreover, the incorporation of MATLAB for biometric processing ensures not only the accuracy and reliability of authentication but also enables advanced data analysis and pattern recognition techniques to further enhance security. Additionally, the system's reliance on Arduino as a microcontroller enables efficient data management and processing, ensuring smooth operation and real-time responsiveness.

3.2.1 ADVANTAGES OF PROPOSED SYSTEM

The proposed system represents a groundbreaking advancement in ATM security, offering unparalleled levels of protection through its innovative multi-modal biometric authentication approach. By integrating various biometric modalities such as face recognition, fingerprint scanning, palm recognition, voice recognition, and iris scanning, the system establishes a comprehensive and highly secure authentication framework, significantly reducing the risk of unauthorized access and fraudulent transactions. This multi-modal approach not only enhances security but also prioritizes user convenience by providing multiple options for biometric identification, catering to individual preferences and accessibility needs. Moreover, the system's utilization of advanced technologies such as the Arduino microcontroller, RFID (Radio Frequency Identification) technology, LCD display, and MATLAB processing further reinforces its robustness and usability. The Arduino microcontroller ensures efficient data management and processing, while RFID technology enables secure user identification. The LCD display facilitates clear and intuitive interaction, guiding users through the transaction process with ease. Additionally, MATLAB processing ensures the accuracy and reliability of biometric authentication, employing advanced algorithms and techniques to analyze biometric data effectively. Collectively, these components work in tandem to deliver a secure, user-friendly, and technologically advanced solution for ATM transactions, setting a new standard for ATM security and usability in the financial industry. By offering several choices for biometric identification, this multi-modal strategy not only prioritizes user convenience over security but also takes into account personal tastes and needs for accessibility.

3.3 FEASIBILITY STUDY

The feasibility of the project is analyzed in this phase and business proposal is put forth with a very general plan for the project and some cost estimates. During system analysis the feasibility study of the proposed system is to be carried out. This is to ensure that the proposed system is not a burden to the company. For feasibility analysis, some understanding of the major requirements for the system is essential. The key considerations are:

- ECONOMIC FEASIBILITY
- TECHNICAL FEASIBILITY
- SOCIAL FEASIBILITY

3.3.1 ECONOMIC FEASIBILITY

This study is carried out to check the economic impact that the system will have on the organization. The amount of fund that the company can pour into the research and development of the system is limited. The expenditures must be justified. Thus the developed system as well within the budget and this was achieved because most of the technologies used are freely available. Implementing a Single Smart card for accessing multiple bank accounts and integrating advanced biometric authentication methods in ATM systems presents economic feasibility on several fronts. Firstly, it streamlines the user experience by reducing the need for individuals to carry multiple cards, potentially reducing production costs for banks and minimizing the environmental impact associated with card production. Secondly, the enhanced security features provided by multi-layered biometric authentication can mitigate financial losses stemming from fraudulent activities, such as

unauthorized transactions and identity theft, thereby safeguarding the financial interests of both banks and customers. Additionally, the potential reduction in fraud-related expenses and operational costs associated with card management and security measures can contribute to long-term cost savings for financial institutions. Overall, the economic benefits derived from improved efficiency, reduced fraud risks, and enhanced security justify the investment in developing and implementing such a system.

3.3.2 TECHNICAL FEASIBILITY

This study is carried out to check the technical feasibility. Any system developed must not have a high demand on the available technical resources. This will lead to high demands being placed on the client. The developed system must have a modest requirement, as only minimal or null changes are required for implementing this system. The technical feasibility of our proposed project lies in leveraging existing advancements in biometric authentication technology and ATM systems. Biometric authentication methods, such as face, fingerprint, iris, voice, and palm recognition, have become increasingly sophisticated, offering high accuracy and reliability. Integrating these biometric modalities into ATM systems requires robust hardware and software infrastructure capable of capturing, processing, and verifying biometric data in real-time. However, given the availability of commercially available biometric sensors and software development kits, as well as standardized protocols for biometric data exchange and authentication, the technical challenges associated with implementing multi-modal biometric authentication are surmountable. Furthermore, advancements in data encryption, secure communication protocols, and system integration frameworks ensure the confidentiality, integrity, and availability of sensitive user information during authentication processes.

3.3.3 SOCIAL FEASIBILITY

Social feasibility refers to the level of acceptance and support a project or system receives from society, including its users, stakeholders, and the broader community. Evaluating the social feasibility of an ATM system involves considering various factors related to societal impact, user acceptance, cultural considerations, and ethical implications. The aspect of study is to check the level of acceptance of the system by the user. This includes the process of training the user to use the system efficiently. The user must not feel threatened by the system, instead must accept it as a necessity. In evaluating the social feasibility of an ATM system, it's essential to assess the system's accessibility and inclusivity, ensuring that it caters to the diverse needs of users across different demographics, including age, gender, and socioeconomic status. Additionally, considering the potential impact of the ATM system on community dynamics and local economies is crucial. For example, the introduction of ATMs in rural areas may enhance financial inclusion and economic development by providing convenient access to banking services. However, it's important to address any concerns regarding job displacement or changes in consumer behavior resulting from the widespread adoption of ATM technology. The social feasibility of our project, which aims to enhance security and convenience in banking transactions through a Single Smart card with multi-layered biometric authentication, is promising. In an era where digital security and personal data protection are paramount concerns for individuals, our solution addresses these anxieties by offering advanced biometric authentication methods like face, fingerprint, iris, voice, and palm recognition. This not only provides a heightened sense of security but also fosters trust and confidence among users, encouraging wider adoption of digital banking services.

CHAPTER 4

SYSTEM DESIGN

4.1 SYSTEM ARCHITECTURE

In our project, First we are going to prepare a Single Smart card for four different bank accounts for access purpose and In ATM system we're going to insert that smart card and then choose one bank account in which we want to transfer/withdraw money. After choosing bank account we need to put pin number and biometric authentications like face, fingerprint, iris, voice and palm are need to be matched. If face and fingerprint Matches correctly then it verifies and allow the user to do the transaction process.

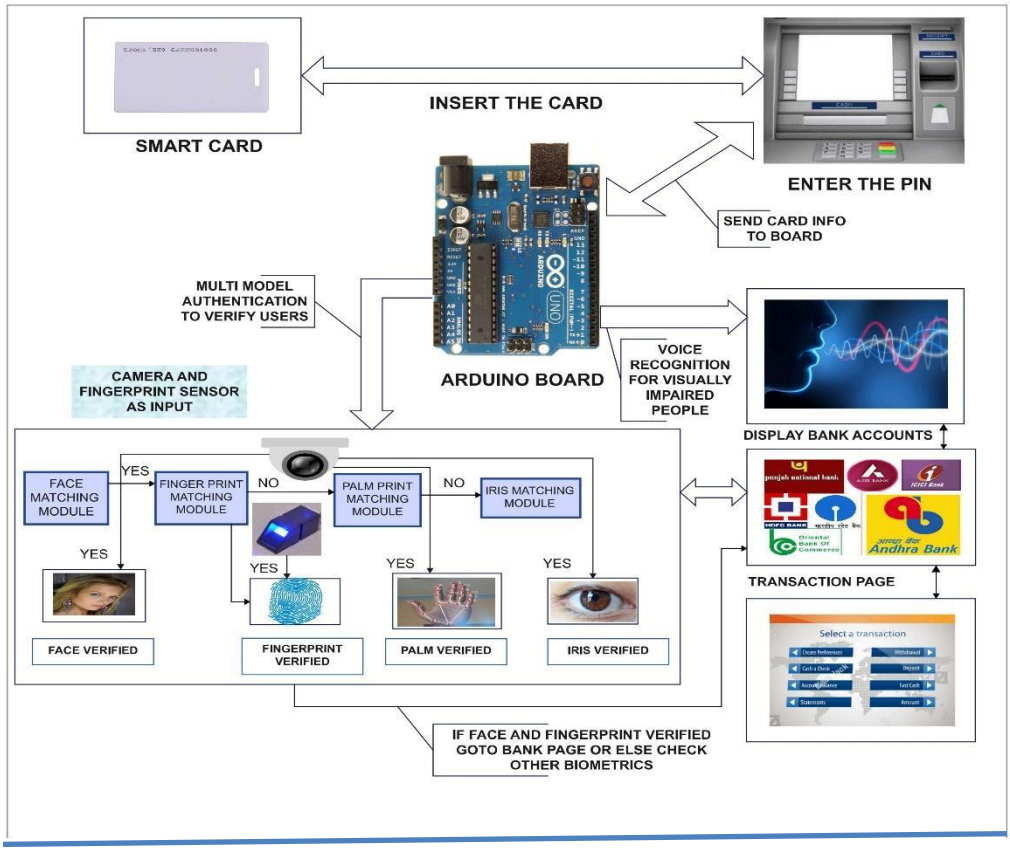


Fig.4.1 SYSTEM ARCHITECTURE

4.2 UML DIAGRAMS

4.2.1 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.

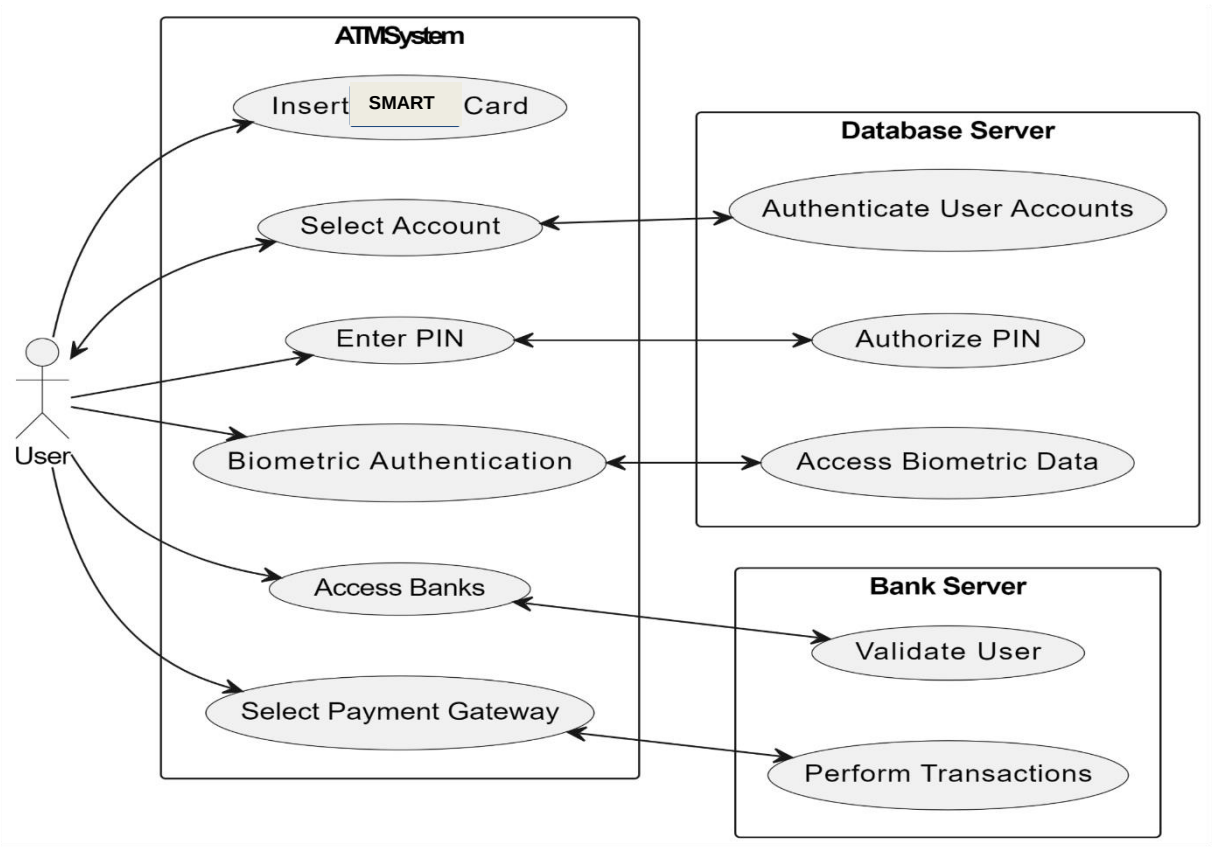


Fig.4.2 USE CASE DIAGRAM

4.2.2 SEQUENCE DIAGRAM

A sequence diagram shows, as parallel vertical lines ("lifelines"), different processes or objects that live simultaneously, and as the horizontal arrows, the messages exchanged between them, in the order in which they occur. This allows the specification of simple run time scenarios in a graphical manner.

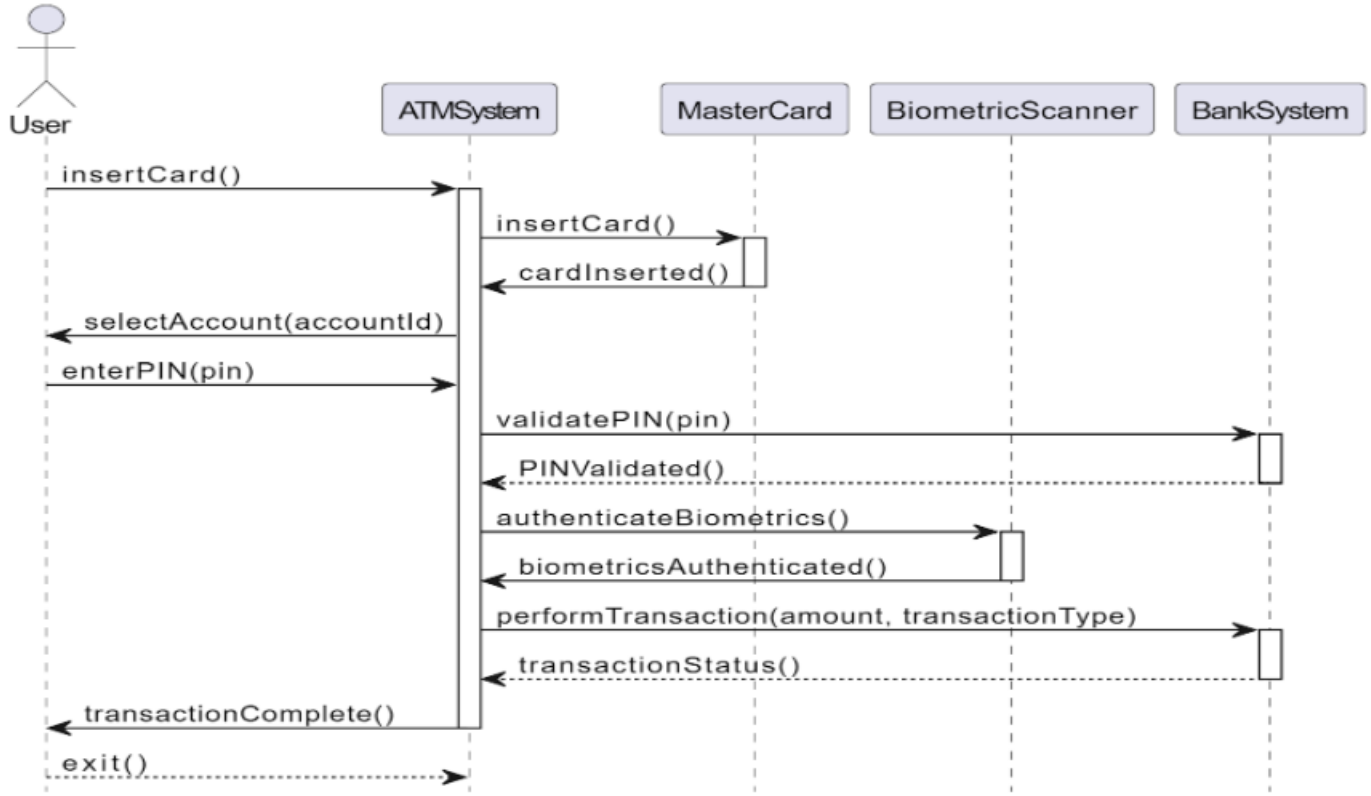


Fig.4.3 SEQUENCE DIAGRAM

4.2.3 ACTIVITY DIAGRAM

Activity diagrams are graphical representations of workflows of stepwise activities and actions with support for choice, iteration and concurrency. In the Unified Modeling Language, activity diagrams can be used to describe the business and operational step-by-step workflow of components in a system. An activity diagram shows the overall flow of control.

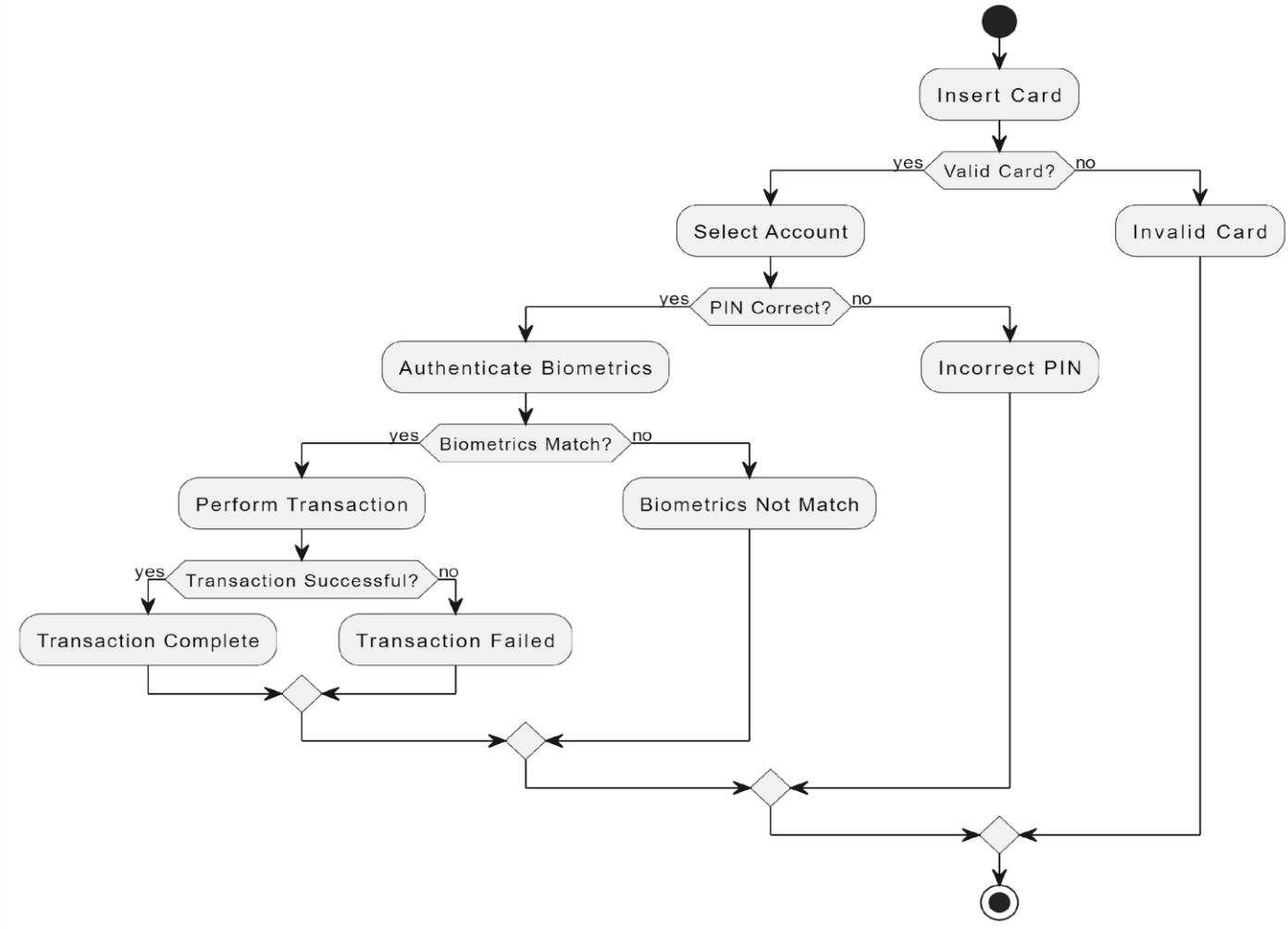


Fig.4.4 ACTIVITY DIAGRAM

4.2.4 CLASS DIAGRAM

Class diagram is UML structure diagram which shows structure of the designed system at the level of classes and interfaces, shows their features constraints and relationships -associations, generalizations, dependencies, etc . 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.

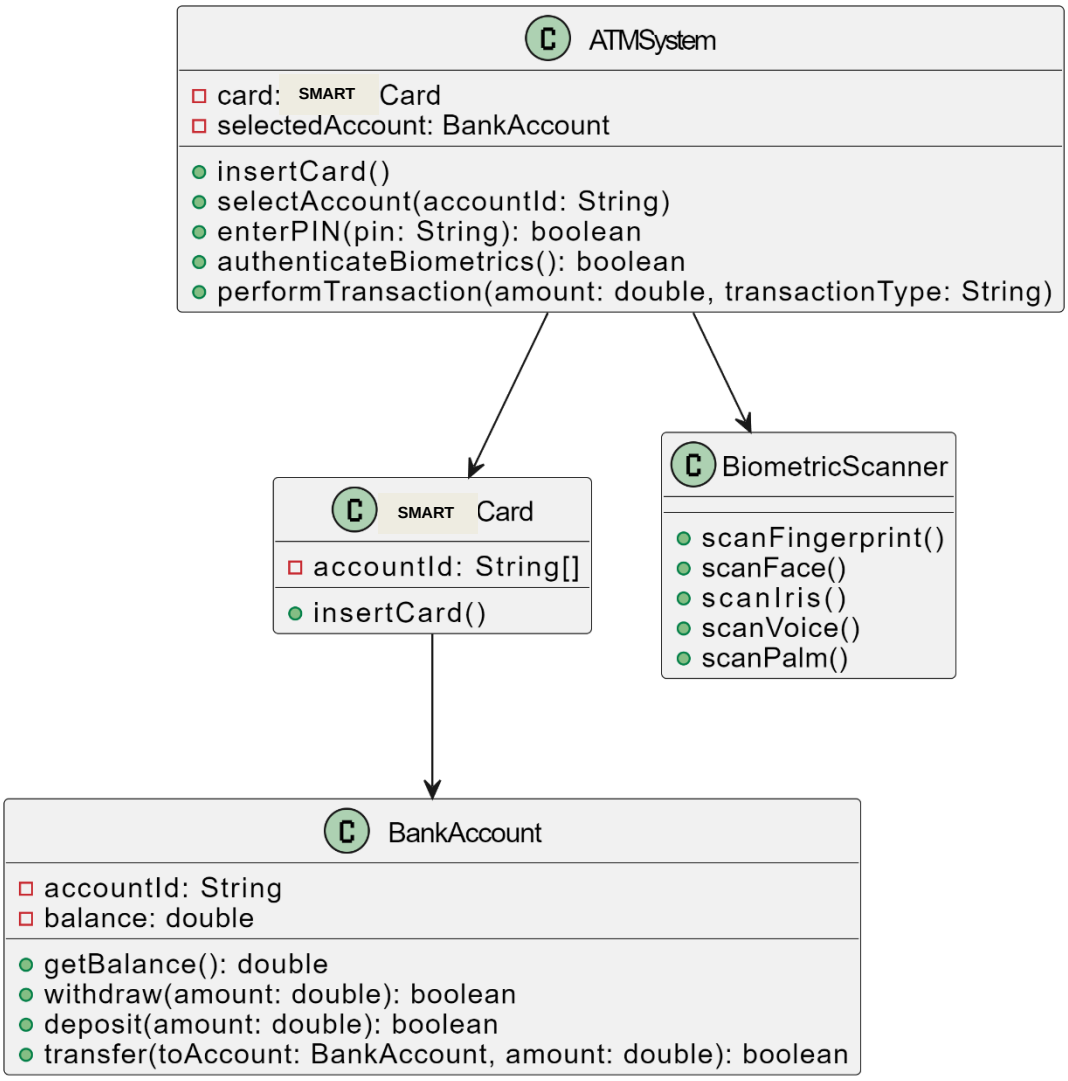


Fig 4.5 CLASS DIAGRAM

4.2.5 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.

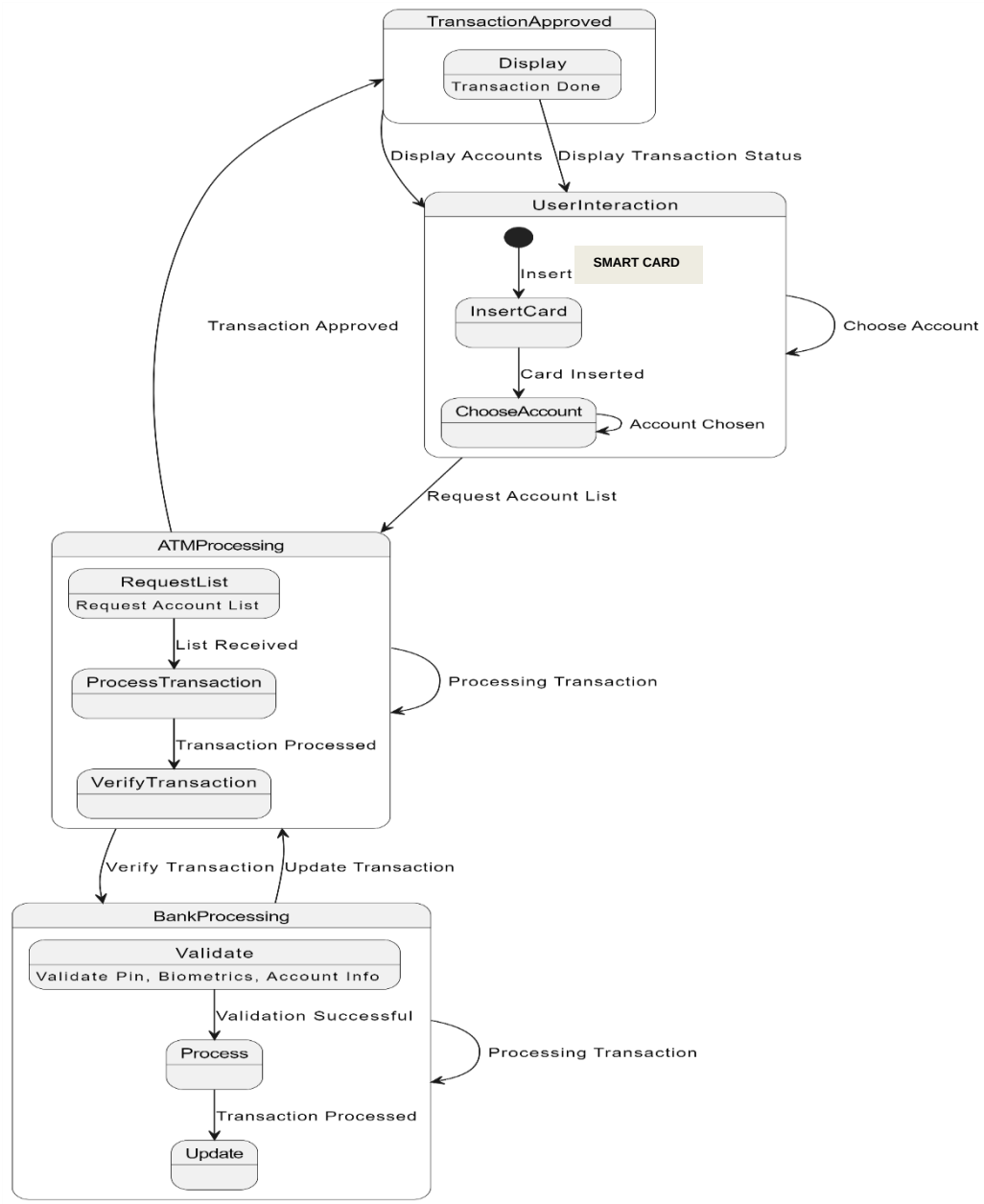


Fig 4.6 STATE DIAGRAM

4.2.6 COLLABORATION DIAGRAM

A collaboration diagram, a key component of Unified Modeling Language (UML), succinctly illustrates how objects or roles within a system interact to achieve defined tasks or scenarios. Using rectangles or ovals to represent participants, arrows to depict communication, and activation bars to signify engagement periods, these diagrams offer a concise visualization of information flow and responsibilities.

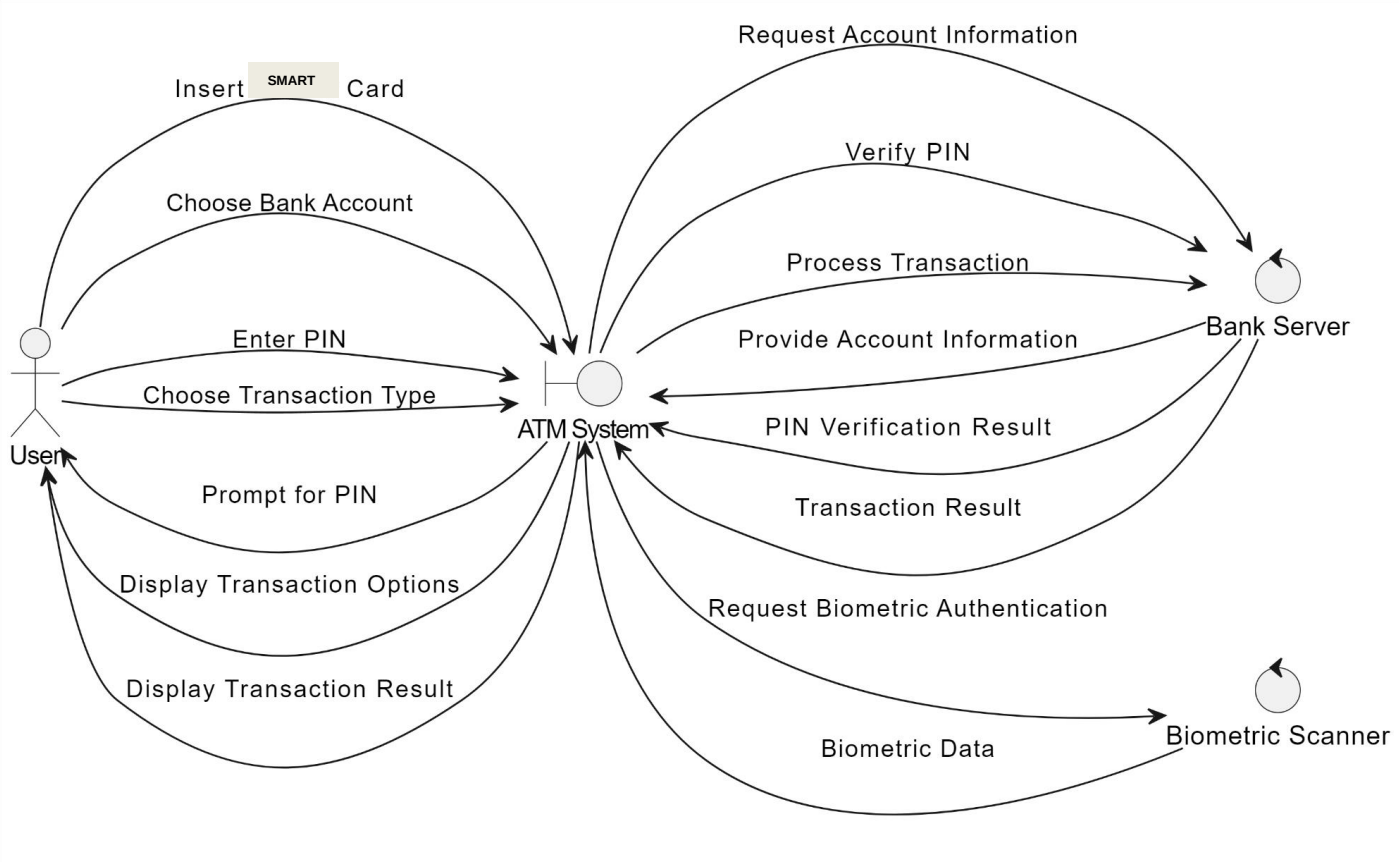


Fig 4.7 COLLABORATION DIAGRAM

4.2.6 COMPONENT DIAGRAM

A component diagram, a fundamental tool in UML modeling, provides a concise overview of a system's architecture by showcasing its constituent components and their relationships. Components, represented as rectangles, encapsulate distinct functionalities within the system, promoting modularity and scalability. Interfaces, depicted as circles or tabs, outline the interactions that components expose to the external environment, fostering clear communication and encapsulation. Dependency arrows between components illustrate their reliance on one another, facilitating a deeper understanding of system dynamics and potential points of failure. Connectors signify interactions between components via their interfaces, elucidating communication channels and method invocations.

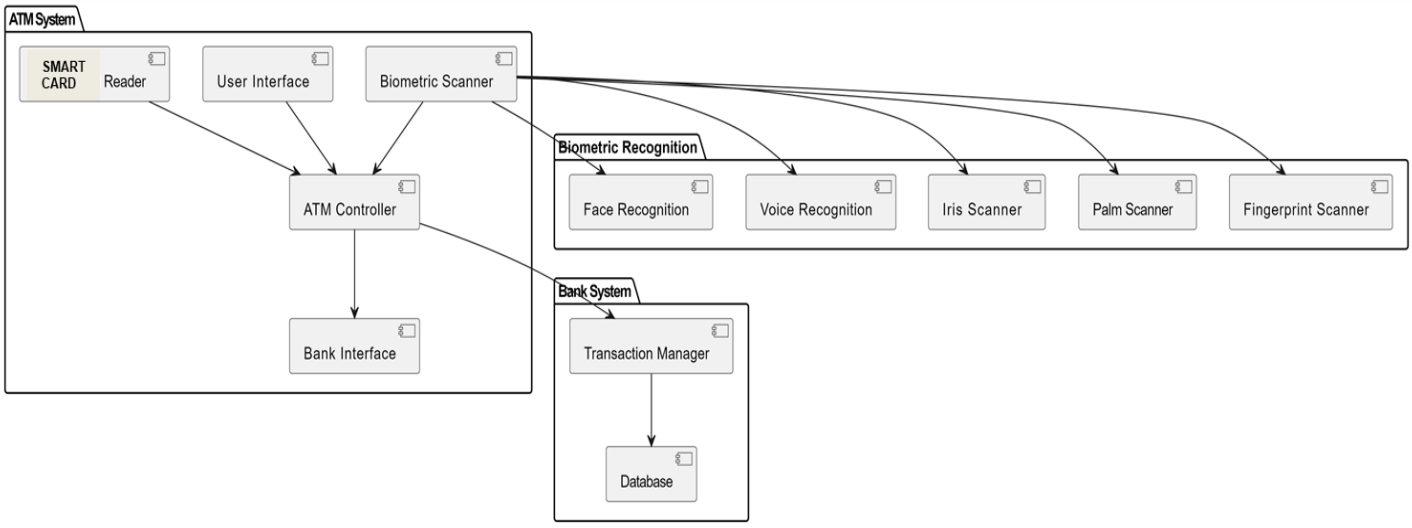


Fig 4.8 COMPONENT DIAGRAM

4.2.7 DEPLOYMENT DIAGRAM

A deployment diagram in UML provides a concise depiction of how software components are distributed across hardware nodes within a system. Nodes, representing physical entities such as servers or devices, are illustrated alongside software artifacts, such as executables or configuration files, which are deployed onto these nodes. Arrows delineate the deployment relationships, clarifying which artifacts reside on which nodes. Optional communication paths between nodes outline network connections or communication channels, enhancing the understanding of inter-component interactions.

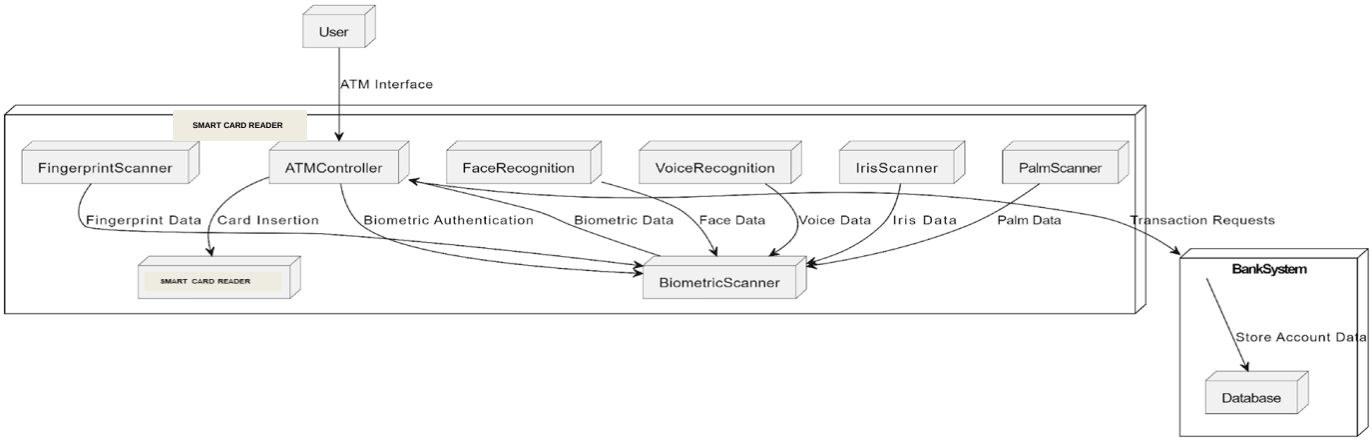
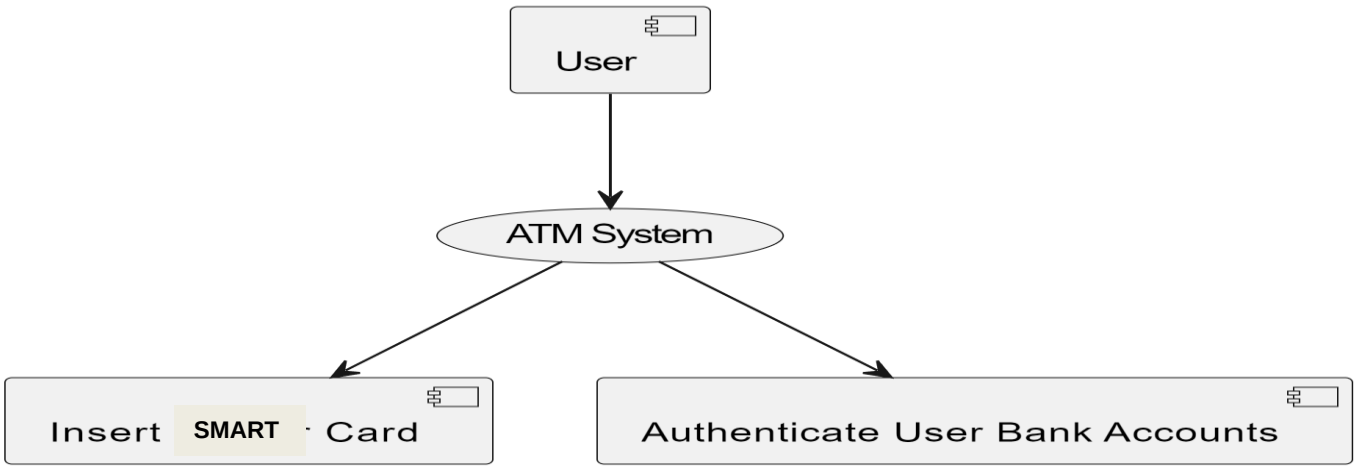


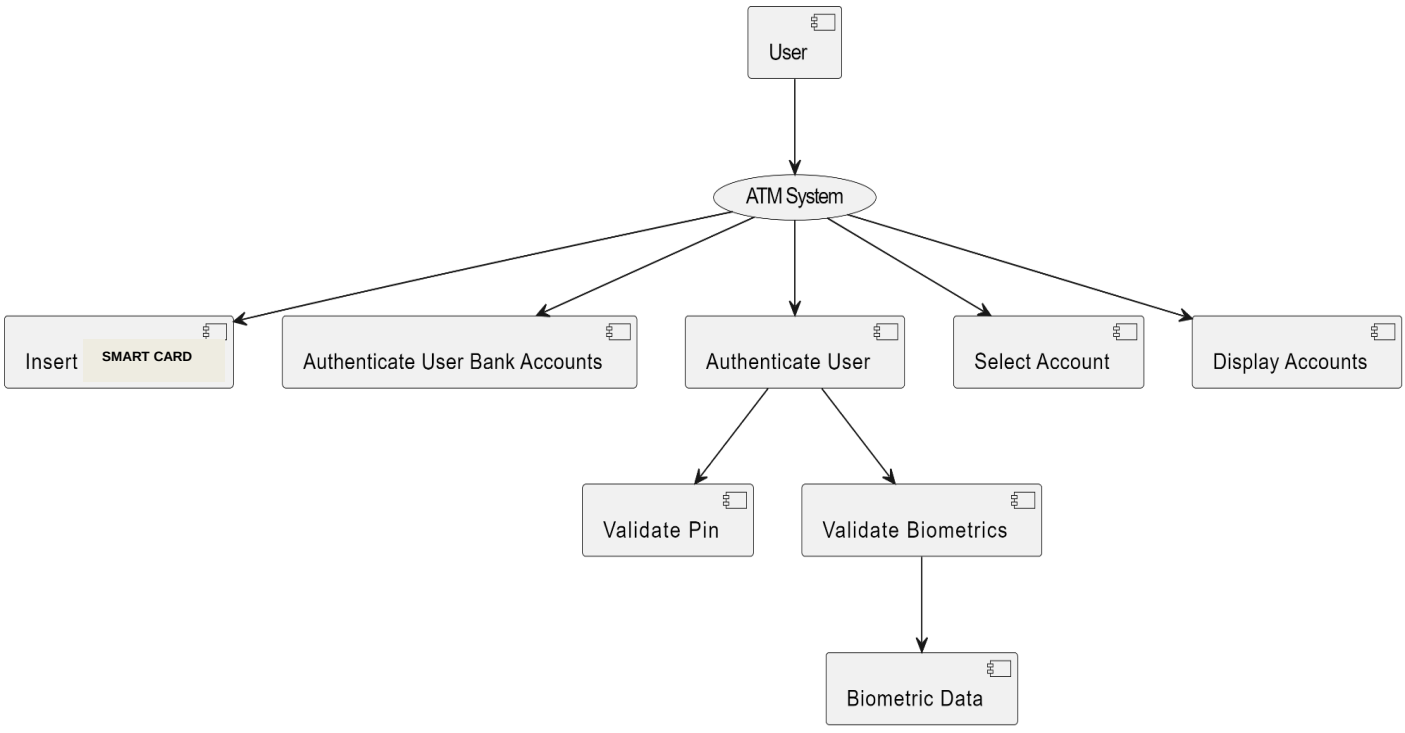
Fig 4.9 DEPLOYMENT DIAGRAM

4.3 DATAFLOW DIAGRAM

LEVEL 0



LEVEL 1



LEVEL 2

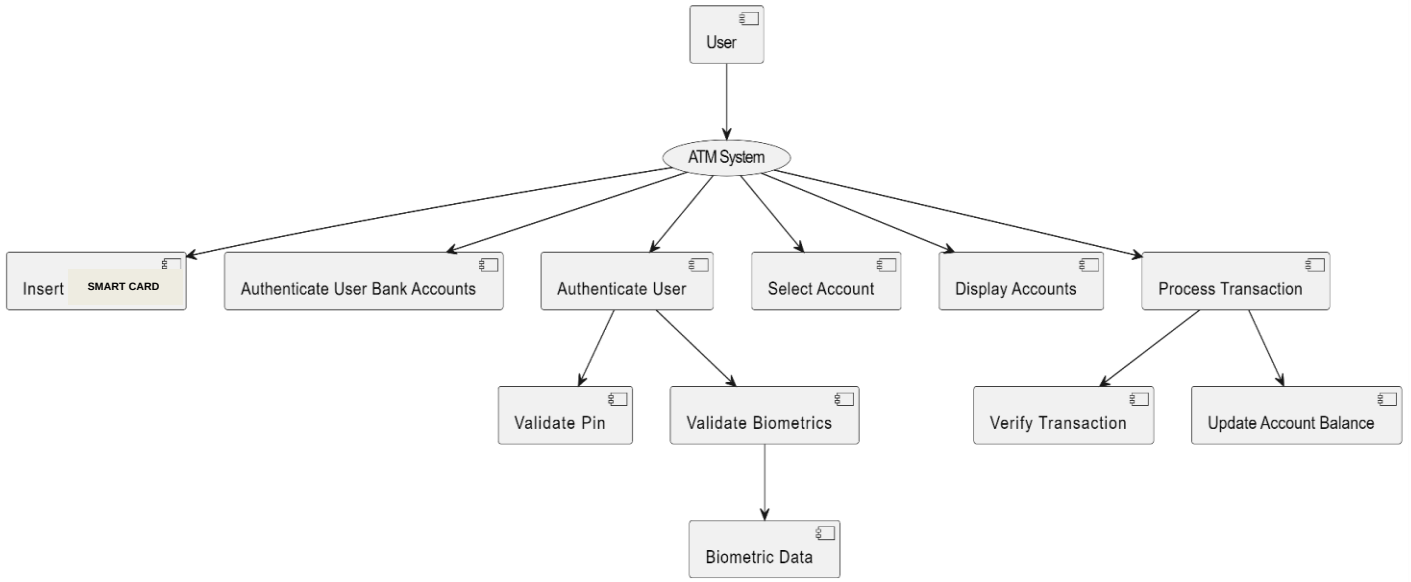


Fig.4.6 DATAFLOW DIAGRAM

CHAPTER 5

SYSTEM REQUIREMENTS

5.1 HARDWARE REQUIREMENTS

The most common set of requirements is defined by the any system or the software application is the physical computer resources, also known as hardware, a hardware requirements list is often accompanied by a Hardware Compatibility List (HCL), especially in case of operating system.

- Processor : Intel I3,I5,I7
- Speed : 3.2 GHz
- RAM : 4 GB (min)
- Hard Disk : 128 GB
- Board Used : Arduino

5.2 SOFTWARE REQUIREMENTS

The software requirements deals with defining software resource requirements and prerequisites that needs to be installed on a computer to provide optimal functioning of an application.

- Operating system : Windows
- Technology Used : Python, PHP
- IDE : Matlab R2021a

5.3 EXTERNAL INTERFACE REQUIREMENTS

5.3.1 PERFORMANCE REQUIREMENTS

The performance requirements for this project encompass several key aspects. Firstly, the biometric recognition accuracy must be high, with minimal false acceptance and rejection rates, ensuring reliable user authentication. Secondly, the system should exhibit prompt response times, facilitating seamless authentication and transaction processing. Additionally, scalability is essential to accommodate a growing user base and transaction volumes without compromising performance. Reliability and availability are paramount, necessitating robust failover mechanisms to minimize downtime and ensure uninterrupted ATM services. Lastly, stringent security measures, usability enhancements, and compliance with regulatory standards round out the performance requirements, guaranteeing a secure, user-friendly, and legally compliant biometric authentication system for ATM transactions.

5.3.2 SAFETY REQUIREMENTS

The software may be safety-critical. If so, there are issues associated with its integrity level. The software may not be safety-critical although it forms part of a safety-critical system. If a system must be of a high integrity level and if the software is shown to be of that integrity level, then the hardware must be at least of the same integrity level. There is little point in producing 'perfect' code in some language if hardware and system software are not reliable. Systems with different requirements for safety levels must be separated. Otherwise, the highest level of integrity required must be applied to all systems in the same environment.

CHAPTER 6

SYSTEM IMPLEMENTATION

6.1 SOFTWARE DESCRIPTION

6.1.1 MATLAB

MATLAB, which stands for "MATrix LABoratory," was created by Cleve Moler, a professor of Computer Science at the University of New Mexico, in the late 1970s. Moler initially developed MATLAB to provide his students with easy access to numerical computing tools for their coursework and research. The first version of MATLAB was written in FORTRAN and ran on the University's mainframe computer. In the early 1980s, Moler, along with Jack Little and Steve Bangert, founded The MathWorks Inc. to further develop and commercialize MATLAB. The company released MATLAB 1.0 in 1984, which was rewritten in C to improve performance and portability across different platforms. Throughout the 1980s and 1990s, MATLAB continued to evolve, with new features and capabilities being added to support a wide range of scientific and engineering applications. The introduction of the MATLAB Graphics System in the mid-1990s significantly enhanced the software's visualization capabilities, making it a powerful tool for data analysis and visualization. In the early 2000s, MATLAB expanded its reach beyond academia and research institutions and gained popularity in industry and commercial sectors. The software's ease of use, extensive library of built-in functions, and support for various toolboxes and extensions made it a preferred choice for engineers, scientists, and analysts worldwide. Over the years, MATLAB has undergone numerous updates and enhancements, incorporating advancements in computational algorithms, programming languages, and hardware technologies.

6.1.2 MATLAB CHARACTERISTICS

MATLAB is distinguished by several key characteristics that underpin its widespread adoption and utility across diverse fields. At its core, MATLAB excels in matrix operations, offering comprehensive support for efficient manipulation and computation with matrices and vectors, which is foundational for various numerical tasks. Moreover, its extensive library of built-in functions and toolboxes spans a wide range of domains, empowering users with specialized functionality for tasks such as signal processing, image analysis, control systems, and optimization. The interactive nature of MATLAB's environment fosters rapid experimentation and exploration, enabling users to execute commands and scripts in real-time, facilitating algorithm prototyping and debugging. Additionally, MATLAB's robust graphics and visualization capabilities empower users to create compelling visual representations of their data, enhancing analysis and communication. Furthermore, MATLAB's seamless integration with other programming languages and software tools facilitates interoperability, allowing for efficient collaboration and leveraging of external resources. Collectively, these characteristics position MATLAB as a versatile and powerful platform for numerical computation, data analysis, and algorithm development across various disciplines and industries.

6.1.3 APPLICATIONS OF MATLAB

MATLAB finds widespread applications across various domains, including engineering, science, finance, and beyond. In engineering, it is instrumental in tasks such as simulation, modeling, and control system design, making it indispensable in electrical, mechanical, civil, and aerospace engineering. Additionally, MATLAB's robust computational capabilities are harnessed in scientific research, aiding in data analysis, statistical analysis, and visualization across disciplines like physics, chemistry, biology, and

environmental science. In finance, MATLAB is utilized for quantitative analysis, risk management, and algorithmic trading, providing tools for portfolio optimization, time series analysis, and financial modeling. Furthermore, MATLAB finds applications in academic research, educational institutions, and industrial settings, where its versatility and user-friendly interface facilitate a wide range of tasks, from algorithm development to real-time data processing and visualization. Overall, MATLAB's versatility and extensive library of functions make it a valuable tool in various fields, enabling efficient and effective problem-solving and analysis.

6.1.4 OPENCV LIBRARY

OpenCV, which stands for Open Source Computer Vision Library, is an open-source computer vision and machine learning software library. It was originally developed by Intel in 1999 and has since become one of the most widely used libraries for real-time computer vision and image processing applications. OpenCV is written in C++ and optimized for performance, but it also provides bindings for Python, Java, and MATLAB, making it accessible to a wide range of developers.The library offers a vast collection of algorithms and functions for various tasks in computer vision, including image processing, feature detection, object recognition, motion tracking, and machine learning. These algorithms cover a wide range of applications, from simple image manipulation tasks like resizing and filtering to more complex tasks like object detection and

tracking in video streams. OpenCV is known for its efficiency and speed, making it suitable for real-time applications such as robotics, augmented reality, autonomous vehicles, surveillance systems, and medical imaging. It provides support for multiple platforms, including Windows, Linux, macOS, Android, and iOS, making it versatile and widely applicable across different environments. Moreover, OpenCV has a large and active community of developers and contributors, which ensures ongoing development, improvement, and support for the library. The library is released under a BSD license, allowing users to freely use and distribute it for both commercial and non-commercial purposes. In summary, OpenCV is a powerful and versatile library for computer vision and image processing, offering a wide range of algorithms, cross-platform support, and a vibrant community, making it a go-to choice for developers working on various computer vision applications.

6.1.5 FEATURES OF OPENCV

OpenCV (Open Source Computer Vision Library) is a comprehensive toolkit renowned for its diverse array of features catering to computer vision and image processing tasks. It encompasses a wide spectrum of functionalities, including robust image processing capabilities such as filtering, resizing, and color space conversions. Moreover, OpenCV offers sophisticated algorithms for feature detection and description, enabling the identification of keypoints, corners, and edges crucial for tasks like object detection and tracking. Additionally, the library provides pre-trained models and methods for object detection and recognition, incorporating techniques such as Haar cascades and deep learning-based approaches. Furthermore, OpenCV facilitates camera calibration and 3D reconstruction, enabling the estimation of camera parameters and the creation of 3D models from 2D images. With its extensive feature set and versatility, OpenCV serves as an indispensable tool for researchers, developers, and enthusiasts alike, powering a multitude of applications across various domains, including robotics, augmented reality, surveillance, and medical imaging. OpenCV (Open Source Computer Vision Library) is a versatile open-source library primarily designed for real-time computer vision tasks. Its features include a wide array of functionalities for image and video processing, such as image manipulation, object detection and tracking, facial recognition, gesture recognition, and motion estimation. OpenCV provides robust support for various platforms, including Windows, Linux, Android, and iOS, making it accessible for both desktop and mobile applications. It offers bindings for multiple programming languages, including C++, Python, and Java, enabling developers to leverage its capabilities across different development environments.

6.2 LIST OF MODULES

1. CARD INSERTION
2. ENTER PIN
3. BIOMETRIC AUTHENTICATION
4. BIOMETRIC VERIFICATION
5. SELECT BANK ACCOUNTS

6.3 MODULE DESCRIPTION

6.3.1 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.

6.3.2 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.

6.3.3 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.

6.3.4 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.

6.3.5 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.

CHAPTER 7

SYSTEM TESTING

7.1 TESTING OBJECTIVE

In a generalized way, we can say that the system testing is a type of testing in which the main aim is to make sure that system performs efficiently and seamlessly. The process of testing is applied to a program with the main aim to discover an unprecedented error, an error which otherwise could have damaged the future of the software. Test cases which brings up a high possibility of discovering and error is considered successful. This successful test helps to answer the still unknown errors.

7.1.1 TEST CASE

Testing, as already explained earlier, is the process of discovering all possible weak-points in the finalized software product. Testing helps to counter the working of sub-assemblies, components, assembly and the complete result. The software is taken through different exercises with the main aim of making sure that software meets the business requirement and user-expectations and doesn't fails abruptly. Several types of tests are used today. Each test type addresses a specific testing requirement.

7.1.2 TESTING TECHNIQUES

A test plan is a document which describes approach, its scope, its resources and the schedule of aimed testing exercises. It helps to identify almost other test item, the features which are to be tested, its tasks, how will everyone do each task, how much the tester is independent, the environment in which the test is taking place, its technique of design plus the both the end criteria which is used, also rational of choice of theirs, and whatever kind of risk which requires emergency planning. It can be also referred to as the record of the process of test planning.

7.2 TYPES OF TESTING

7.2.1 UNIT TESTING

In unit testing, the design of the test cases is involved that helps in the validation of the internal program logic. The validation of all the decision branches and internal code takes place. After the individual unit is completed it takes place. Plus it is taken into account after the individual united is completed before integration. The unit test thus performs the basic level test at its component stage and test the particular business process, system configurations etc. The unit test ensures that the particular unique path of the process gets performed precisely to the documented specifications and contains clearly defined inputs with the results which are expected.

7.2.2 INTEGRATION TESTING

These tests are designed to test the integrated software items to determine whether if they really execute as a single program or application. The testing is event driven and thus is concerned with the basic outcome of field. The Integration tests demonstrate that the components were individually satisfaction, as already represented by successful unit testing, the components are apt and fine. This type of testing is specially aimed to expose the issues that come-up by the components combination.

7.2.3 FUNCTIONAL TESTING

The functional tests help in providing the systematic representation that functions tested are available and specified by technical requirement, documentation of the system and the user manual.

7.2.4 SYSTEM TESTING

System testing, as the name suggests, is the type of testing in which ensure that the software system meet the business requirements and aim. Testing of the configuration is taken place here to ensure predictable result and thus

analysis of it. System testing is relied on the description of process and its flow, stressing on pre driven process and the points of integration.

7.2.5 WHITE BOX TESTING

The white box testing is the type of testing in which the internal components of the system software is open and can be processed by the tester. It is therefore a complex type of testing process. All the data structure, components etc. are tested by the tester himself to find out a possible bug or error. It is used in situation in which the black box is incapable of finding out a bug. It is a complex type of testing which takes more time to get applied.

7.2.6 BLACK BOX TESTING

The black box testing is the type of testing in which the internal components of the software is hidden and only the input and output of the system is the key for the tester to find out a bug. It is therefore a simple type of testing. A programmer with basic knowledge can also process this type of testing. It is less time consuming as compared to the white box testing. It is very successful for software which are less complex are straight-forward in nature. It is also less costly than white box testing.

7.2.7 ACCEPTANCE TESTING

User Acceptance Testing is a critical phase of any project and requires significant participation by the end user. It also ensures that the system meets the functional requirements.

7.2.8 ALPHA TESTING

Alpha testing is performed at the developer's site by the customer in a closed environment. This is done after the system testing. Alpha testing is one of the most common software testing strategies used in software development. It’s specially used by product development organizations. Alpha testing is typically performed by a group that is independent of the design team, but still

within the company, e.g. in-house software test engineers, or software QA engineers. Alpha testing is final testing before the software is released to the general public.

7.2.9 BETA TESTING

It is also known as field testing. It takes place at customer's sites. It sends the system to users who install it and use it under real-world working conditions. A beta test is the second phase of software testing in which a sampling of the intended audience tries the product out.

7.2.10 SECURITY TESTING

Security testing is basically a type of software testing that's done to check whether the application or the product is secured or not. It checks to see if the application is vulnerable to attacks, if anyone hack the system or login to the application without any authorization. It is a type of non functional testing. It is a process to determine that an information system protects data and maintains functionality as intended. The security testing is performed to check whether there is any information leakage in the sense by encrypting the application or using wide range of software's and hardware's and firewall etc.

7.3 TEST RESULTS

Module	Function	Expected Result	Pass/Fail Criteria
Card Reader	Read card data	Successfully reads card data	PASS
Biometric Sensors	Capture and verify biometric data	Accurately captures biometric data	PASS
PIN Verification	Verify PIN entered by the user	Correct PIN entered	PASS
Bank Account Selection	Select bank account from the card	Successfully selects desired bank account	PASS
Transaction Authorization	Authenticate user via biometrics and PIN	Successful authentication	PASS
Transaction Processing	Transfer/withdraw money from chosen account	Money transferred/withdrawn successfully	PASS
Integration Testing	Ensure components work together	Smooth interaction between card reader, biometrics, etc.	PASS
Regression Testing	Verify recent changes haven't broken system	Existing functionalities not affected by changes	PASS
Black Box Testing	Test system functionality without internals	Inputs produce correct outputs	PASS
Security Testing	Assess system resistance to unauthorized access	Unauthorized access attempts fail	PASS
Performance Testing	Evaluate system responsiveness under load	System remains responsive with multiple users	PASS

Fig 7.1 Test Case Results

CHAPTER 8
RESULTS AND DISCUSSION

Our project aims to develop a Single Master card system for accessing four different bank accounts, integrating multiple biometric authentication methods including face, fingerprint, iris, voice, and palm recognition. The user inserts the master card into the ATM system and selects the desired bank account for transactions. Subsequently, they are required to input a PIN number and undergo biometric authentication. If the face and fingerprint biometrics match accurately, the system verifies the user's identity and allows transaction processing. Our project involves a sophisticated authentication process wherein if the initial face and fingerprint matching fails, the system proceeds to verify the user's identity through alternative biometric methods such as palm and iris recognition. Additionally, for visually abled users, there's a voice recognition system in place to facilitate transaction processes and authentication. This multi-layered approach ensures robust security and inclusivity, catering to a diverse range of users with varying needs and preferences. By offering alternative authentication methods, the system enhances accessibility while maintaining stringent security standards. Nevertheless, the integration of multiple biometric modalities necessitates thorough testing and validation to ensure accuracy, reliability, and seamless user experience. Overall, this comprehensive approach underscores the project's commitment to both security and user inclusivity in the realm of banking transactions. Our project presents several benefits and challenges. On the positive side, it enhances security by employing multiple biometric layers, reducing the risk of unauthorized access and fraud.

CHAPTER 9

CONCLUSION AND FUTURE ENHANCEMENT

9.1 CONCLUSION:

In conclusion, the proposed project aims to enhance convenience, security, and accessibility in banking services through the implementation of a Single Smart 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.

9.2 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.

APPENDICES

A. SAMPLE CODE

MULTI MODEL AUTHENTICATION

```
function varargout = main(varargin)
% --- Executes just before main is made visible.
function main_OpeningFcn(hObject, eventdata, handles, varargin)
% This function has no output args, see OutputFcn.
% hObject    handle to figure
% eventdata  reserved - to be defined in a future version of MATLAB
% handles    structure with handles and user data (see GUIDATA)
% varargin   command line arguments to main (see VARARGIN)
```

TRAINING THE DATABASE

```
if exist('features.mat','file') == 0
msgbox('FIRST TRAIN YOUR DATABASE','INFO...!!!','MODAL')
return
end
ff = dir('database');
if length(ff) == 2
h = waitbar(0,'Plz wait Matlab is scanning ur database...','name','SCANNING IS IN PROGRESS');
for k = 1:100
waitbar(k/100)
pause(0.03)
end
```

```
close(h)
msgbox({'NO IMAGE FOUND IN DATABASE';'FIRST LOAD YOUR DATABASE';'USE "ADD NEW IMAGE" MENU'},'WARNING....!!!','WARN','MODAL')
return
end
fd = vision.CascadeObjectDetector();
[f,p] = uigetfile('*.jpg','PLEASE SELECT AN FACIAL IMAGE');
if f == 0
return
end
p1 = fullfile(p,f);
im = imread(p1);
bbox = step(fd, im);
vo = insertObjectAnnotation(im,'rectangle',bbox,'FACE');
r = size(bbox,1);
uiwait
cla(handles.axes1); reset(handles.axes1); set(handles.axes1,'box','on','xtick',[],'ytick',[])
return
end
axes(handles.axes1)
image(vo);
set(handles.axes1,'xtick',[],'ytick',[],'box','on')
bx = questdlg({'CORRECT IMAGE IS SELECTED';'SELECT OPTION FOR FACE EXTRACTION'},'SELECT AN OPTION','MANUALLY','AUTO','CC');
if strcmp(bx,'MANUALLY') == 1
while 1
```

```
fhx = figure(2);
set(fhx,'menubar','none','numbertitle','off','name','PREVIEW')
imc = imcrop(im);
bbox1 = step(fd, imc);
if size(bbox1,1) ~= 1
uiwait
else
close gcf
break
end
imc = imresize(imc,[300  300]);
while 1
fhx = figure(2);
close gcf
imc = imresize(imc,[300 300]);
axes(handles.axes1)
image(imc)
text(20,20,'\bfUr Precaptured image.','fontsize',12,'color','y','fontname','comic sans ms')
set(handles.axes1,'xtick',[],'ytick',[],'box','on')
else
end
immxx = getimage(handles.axes1);
zz = findsimilar(immxx);
zz = strtrim(zz);
fxz = imread(['database/'  zz]);
q1= ehd(immxx,0.1);
q2 = ehd(fxz,0.1);
```

```
q3 = pdist([q1 ; q2]);
disp(q3)
if q3 < 0.5
axes(handles.axes2)
image(fxz)
set(handles.axes1,'xtick',[],'ytick',[],'box','on')
text(20,20,'\bfUr Database Entered Image.','fontsize',12,'color','y','fontname','comic sans ms')
set(handles.axes2,'xtick',[],'ytick',[],'box','on')
xs = load('info.mat');
xs1 = xs.z2;
for k = 1:length(xs1)
st = xs1{k};
stx = st{1};
if strcmp(stx,zz) == 1
str = st{2};
delete(s)
clear s
else
msgbox('YOU ARE NOT A VALID PERSON', 'WARNING','WARN','MODAL')
cla(handles.axes1)
reset(handles.axes1)
cla(handles.axes2)
reset(handles.axes2)

% --------------------------------------------------------------------
```

DETECT FACE, PALM, IRIS

```
function LIVE_CAM_Callback(hObject, eventdata, handles)
% hObject    handle to LIVE_CAM (see GCBO)
% eventdata  reserved - to be defined in a future version of MATLAB
% handles    structure with handles and user data (see GUIDATA)
global co
if exist('features.mat','file') == 0
msgbox('FIRST TRAIN YOUR DATABASE','INFO...!!!','MODAL')
return
end
close(h)
msgbox({'NO IMAGE FOUND IN DATABASE';'FIRST LOAD YOUR DATABASE';'USE "ADD NEW IMAGE" MENU'},
'WARNING....!!!','WARN','MODAL')
return
end
if isfield(handles,'vdx')
vid = handles.vdx;
stoppreview(vid)
delete(vid)
handles = rmfield(handles,'vdx');
guidata(hObject,handles)
cla(handles.axes1)
reset(handles.axes1)
end
info = imaqhwinfo('winvideo');
did = info.DeviceIDs;
```

```
if isempty(did)
msgbox({'YOUR SYSTEM DO NOT HAVE A WEBCAM';' ';'CONNECT A ONE'},'WARNING....!!!!','warn','modal')
return
end
msgbox({'TOO MANY FACES IN FRAME';' ';'ONLY ONE FACE IS ACCEPTED'},'WARNING.....!!!','warn','modal')
uiwait
stoppreview(vid)
delete(vid)
handles = rmfield(handles,'vdx');
guidata(hObject,handles)
cla(handles.axes1)
reset(handles.axes1)
cla(handles.axes2)
reset(handles.axes2)
return
end
kx = kx + 1;
if kx > 10 && ~isempty(bbox)
break
end
function SINGL_PIC_Callback(hObject, eventdata, handles)
% hObject    handle to SINGL_PIC (see GCBO)
% eventdata  reserved - to be defined in a future version of MATLAB
% handles    structure with handles and user data (see GUIDATA)
flist  =  dir('database');
```

```
if length(flist) == 2
msgbox('NOTHING TO DELETE','INFO','modal');
return
end
for k =  3:length(flist)
z = flist(k).name;
z(strfind(z,'.') : end) = [];
nlist(k-2) = str2double(z);
end
% --------------------------------------------------------------------
```

REMOVING A USER

```
[a,b] = listdlg('promptstring','SELECT FILE/FILES TO DELETE','liststring',na1,'listsize',
[125  100]);
if b == 0
return
end
cd ('database')
for k = 1:length(a)
str = na1{k};
delete(str)
end
cd ..
flist  =  dir('database');
if length(flist) == 2
msgbox({'NOTHING TO RENAME';'ALL DELETED'},'INFO','modal');
return
```

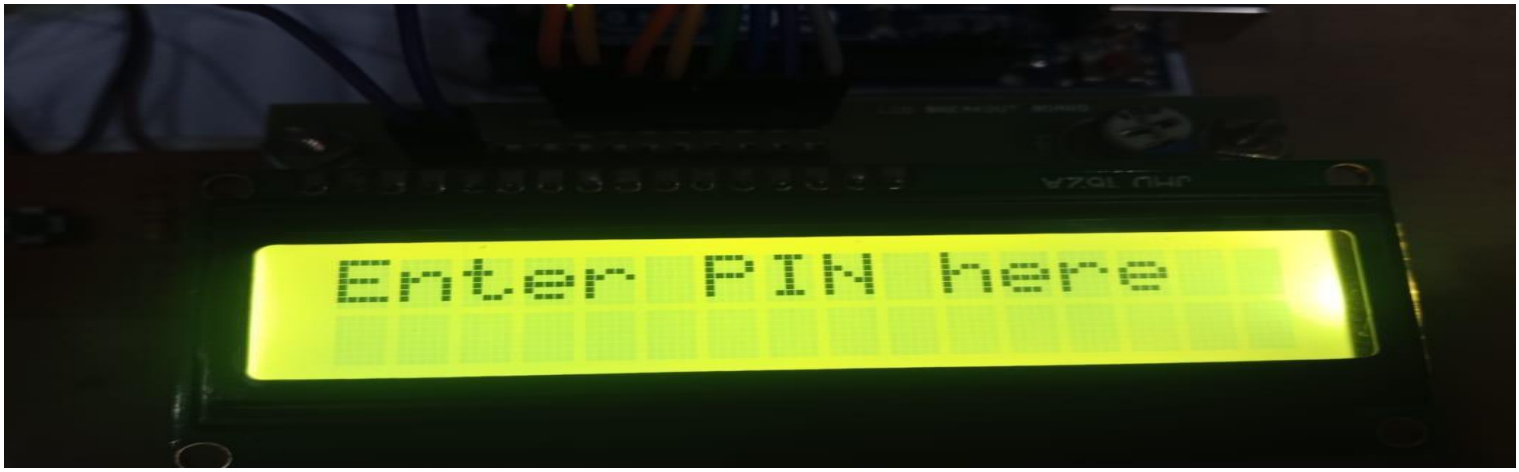
```
end
cd('database')
flist  =  dir(pwd);
for k =  3:length(flist)
z = flist(k).name;
z(strfind(z,'.') : end) = [];
nlist(k-2) = str2double(z);
end
nlist  = sort(nlist);
h = waitbar(0,'PLZ WAIT, WHILE MATLAB IS RENAMING','name','PROGRESS...');
for k = 1:length(nlist)
if k ~= nlist(k)
p = nlist(k);
movefile([num2str(p)  '.jpg']  ,  [num2str(k)  '.jpg'])
waitbar((k-2)/length(flist),h,sprintf('RENAMED  %s   to  %s',[num2str(p)  '.jpg'],
[num2str(k)  '.jpg']))
end
pause(.5)
end
close(h)
cd ..
else
break
end
```

ADD NEW DATA TO THE DATABASE

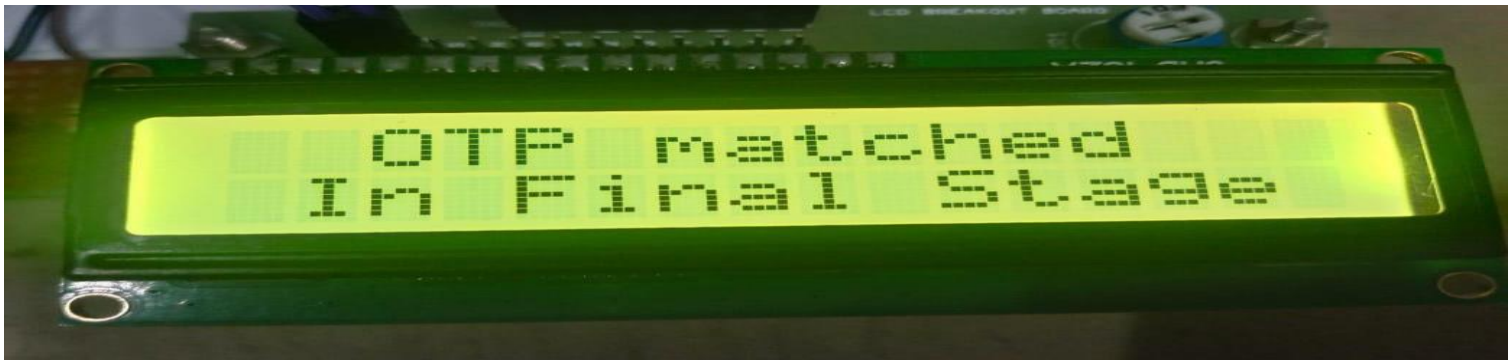
```
msgbox({'NO IMAGE FOUND IN DATABASE';'FIRST LOAD YOUR DATABASE'
;'USE "ADD NEW IMAGE" MENU'},'WARNING....!!!','WARN','MODAL')
return
end
if exist('features.mat','file') == 2
bx = questdlg({'TRAINING HAS ALREDY BEEN DONE';' ';'WANT TO TRAIN
 DATABASE AGAIN?'},'SELECT','YES','NO','CC');
if strcmpi(bx,'yes') == 1
builddatabase
msgbox('TRAINING DONE....PRESS OK TO CONTINUE','OK','modal')
return
else
builddatabase
msgbox('TRAINING DONE....PRESS OK TO CONTINUE','OK','modal')
return
end
```

B. SCREENSHOTS

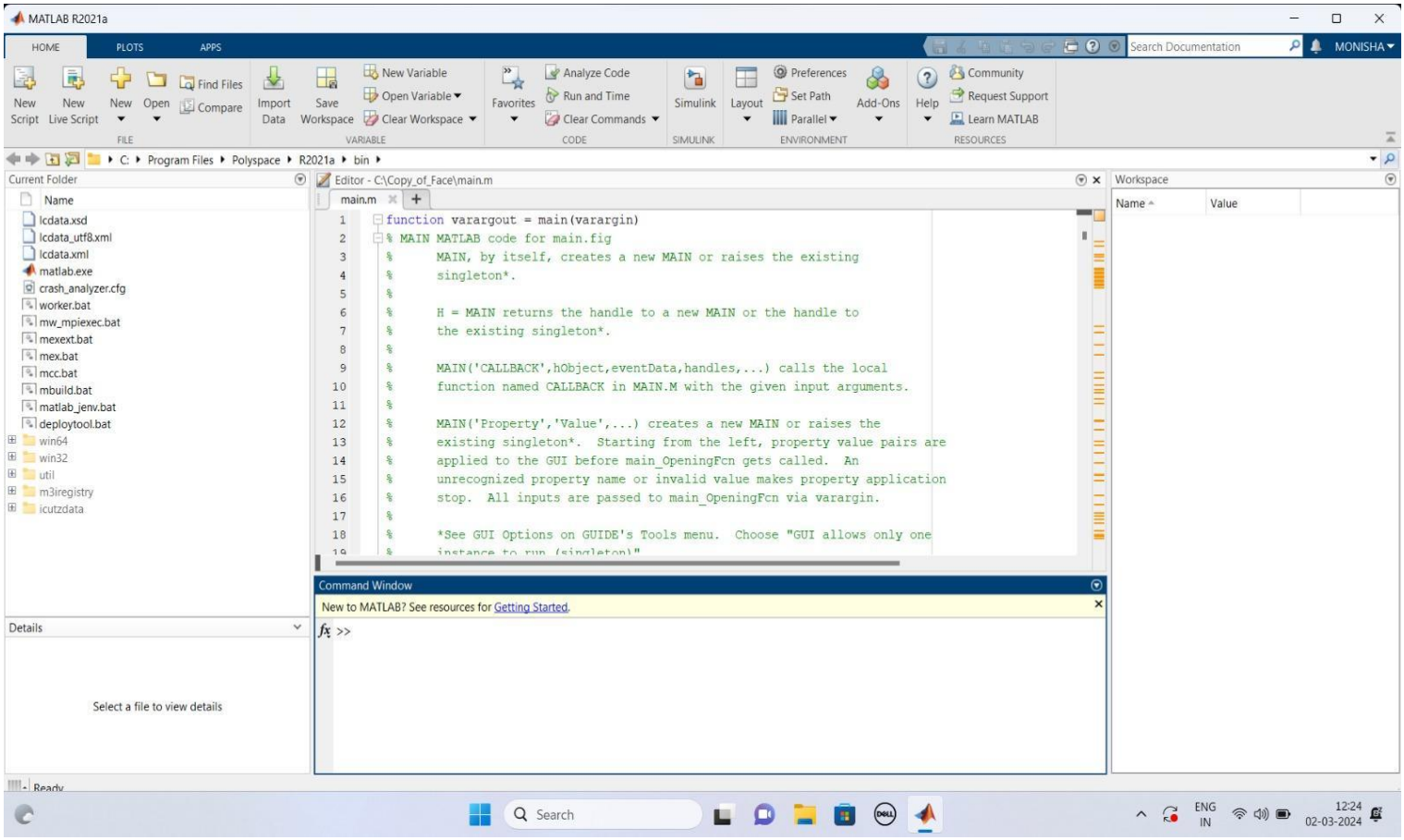
CARD INSERTION – Allows the user the show the card and gets authorized in the ATM transaction



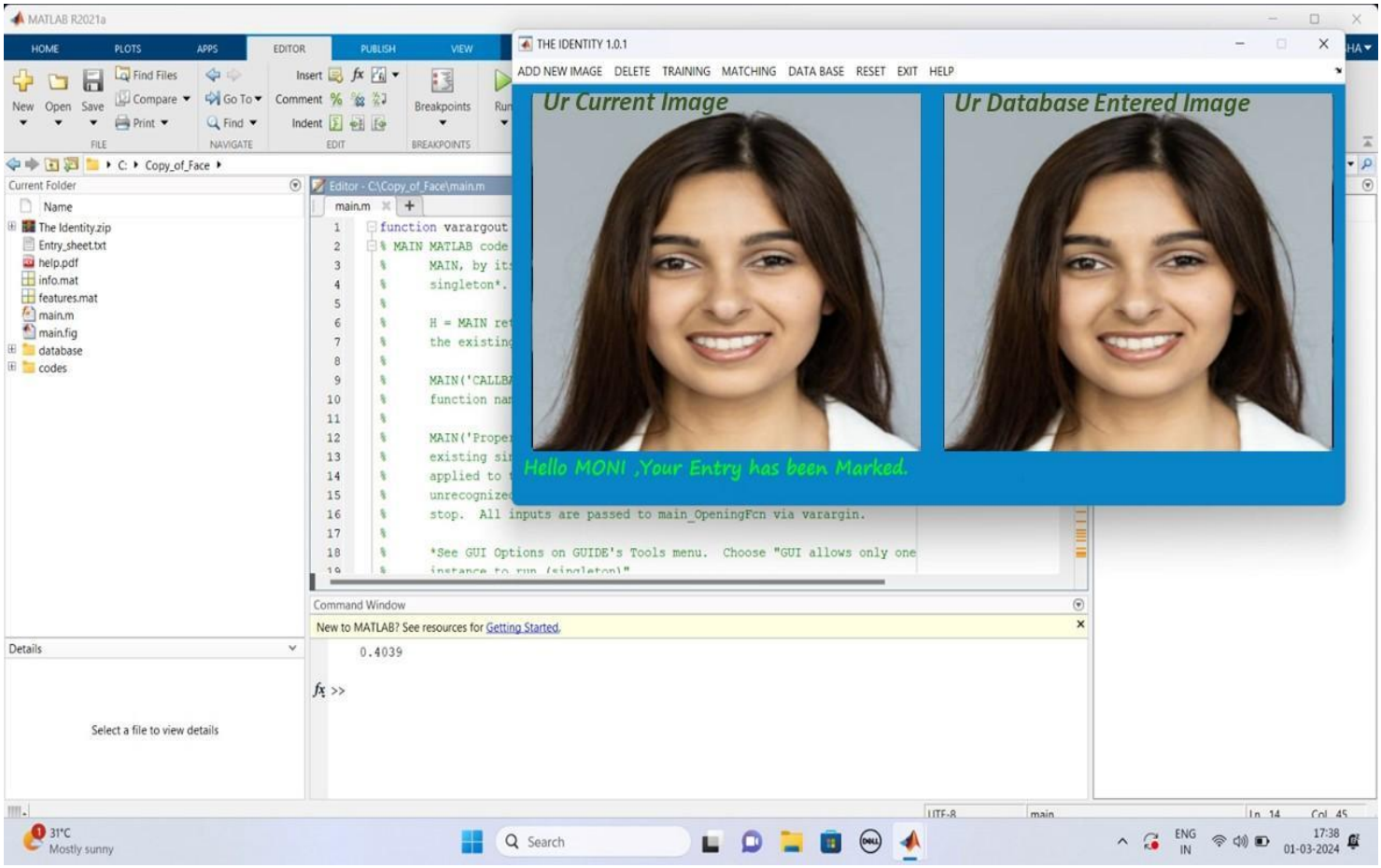
ENTER THE PIN – It asks the user to enter the pin to authenticate the user



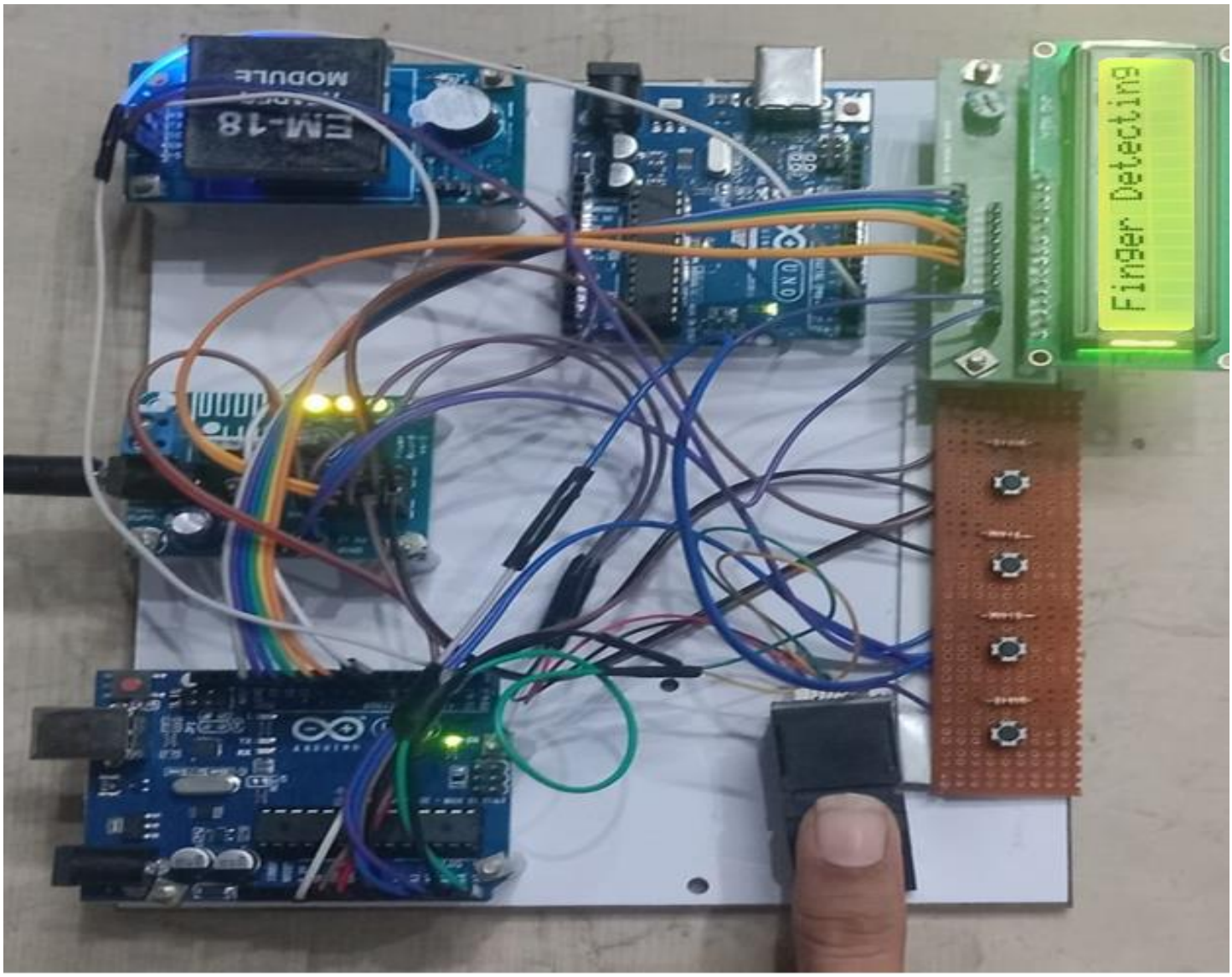
ATM PIN GETS VERIFIED HERE



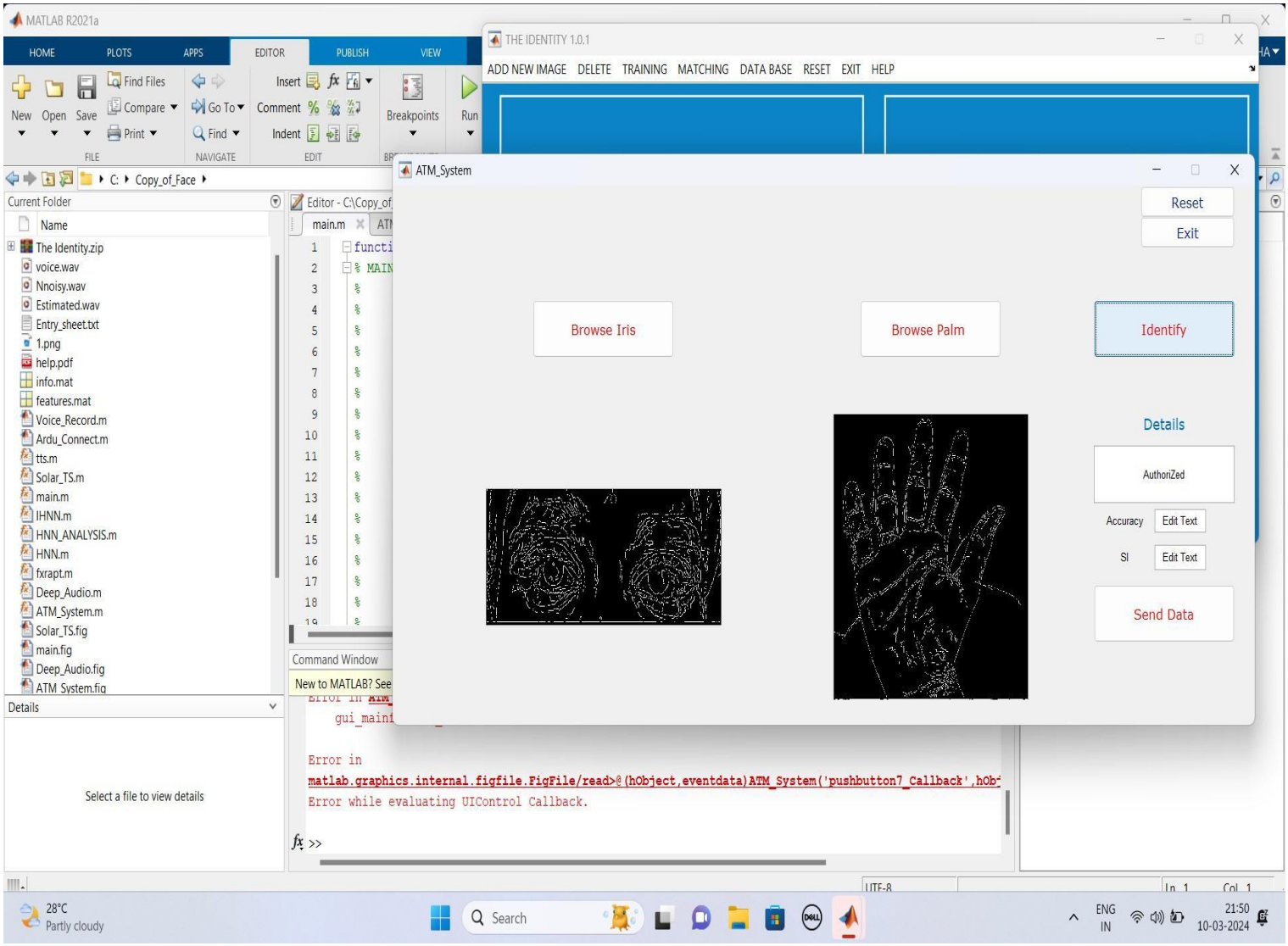
MATLAB SOFTWARE FOR BIO-METRIC AUTHENTICATION



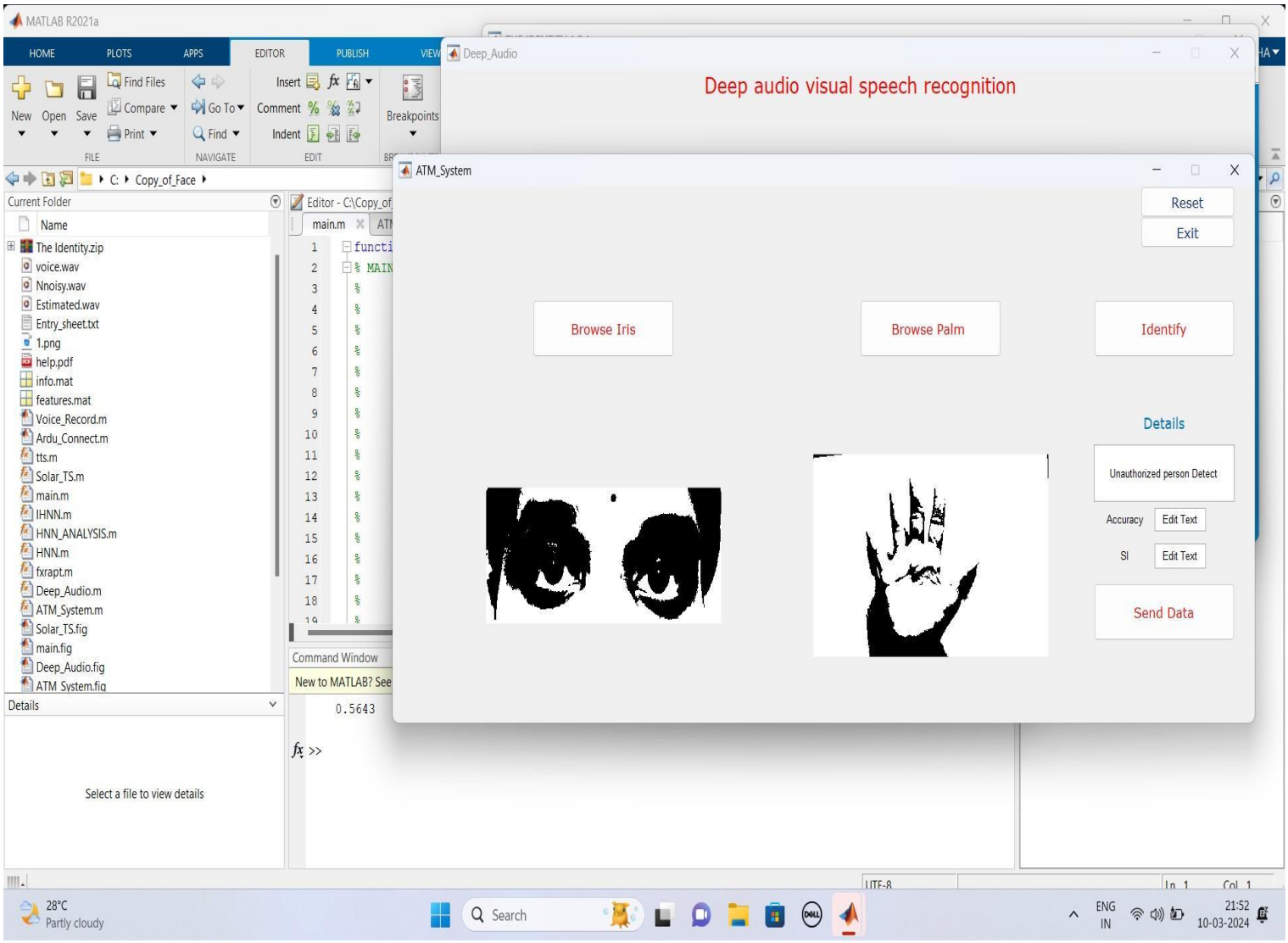
FACE RECOGNITION – Detects face and Authenticates the Person



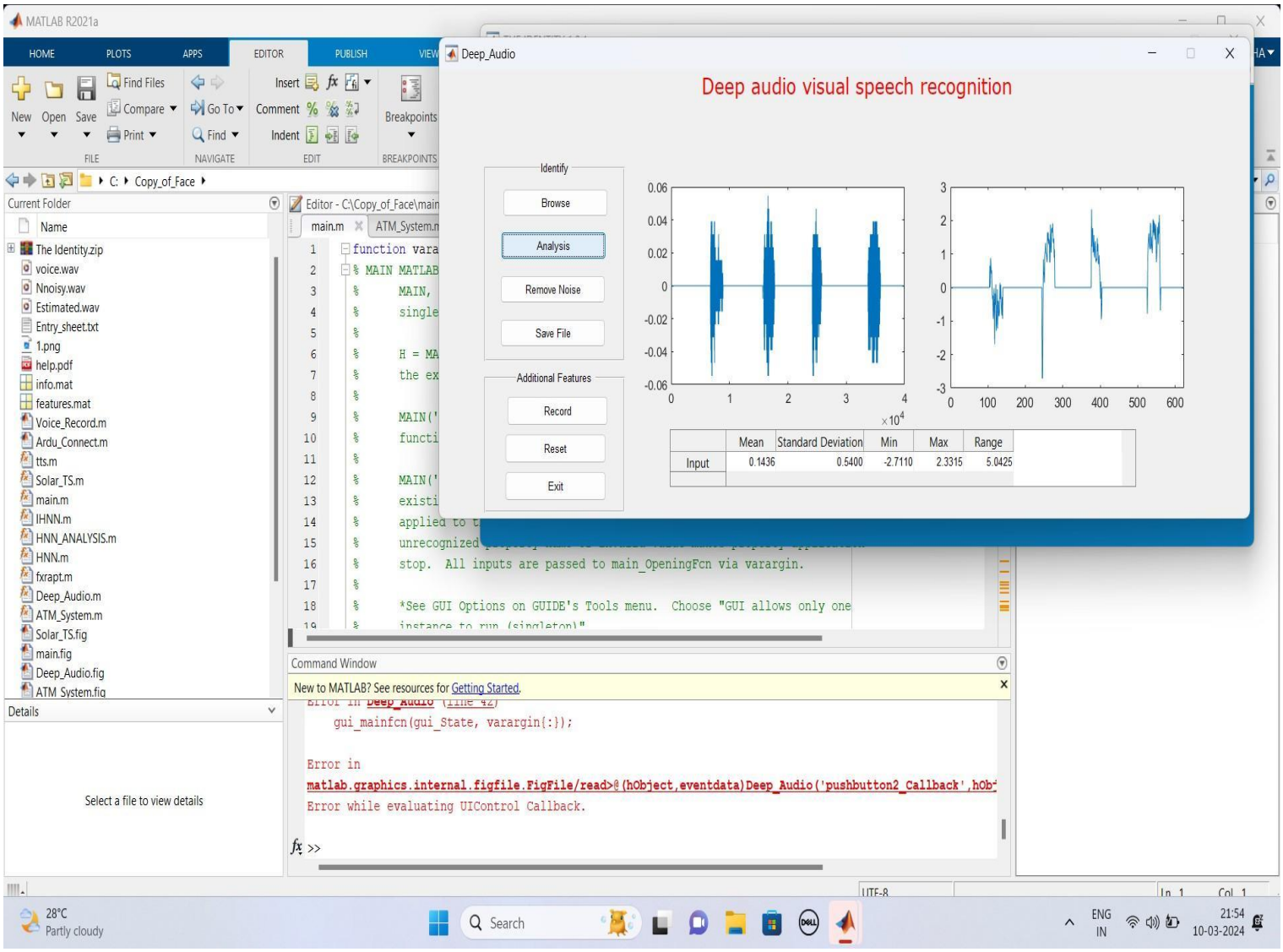
FINGERPRINT RECOGNITION – Detects finger and Authenticates the Person



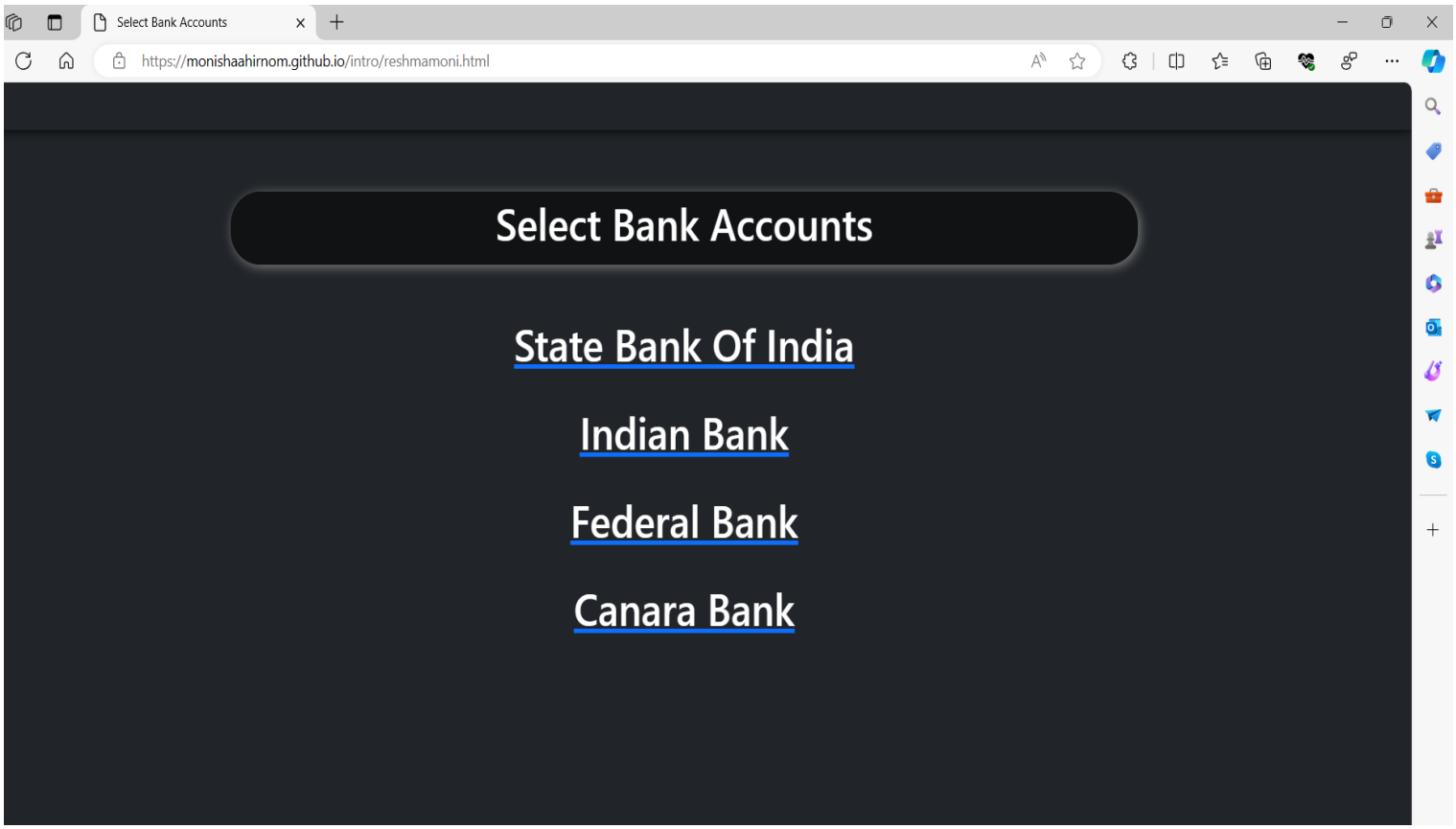
IRIS AND PALM RECOGNITION



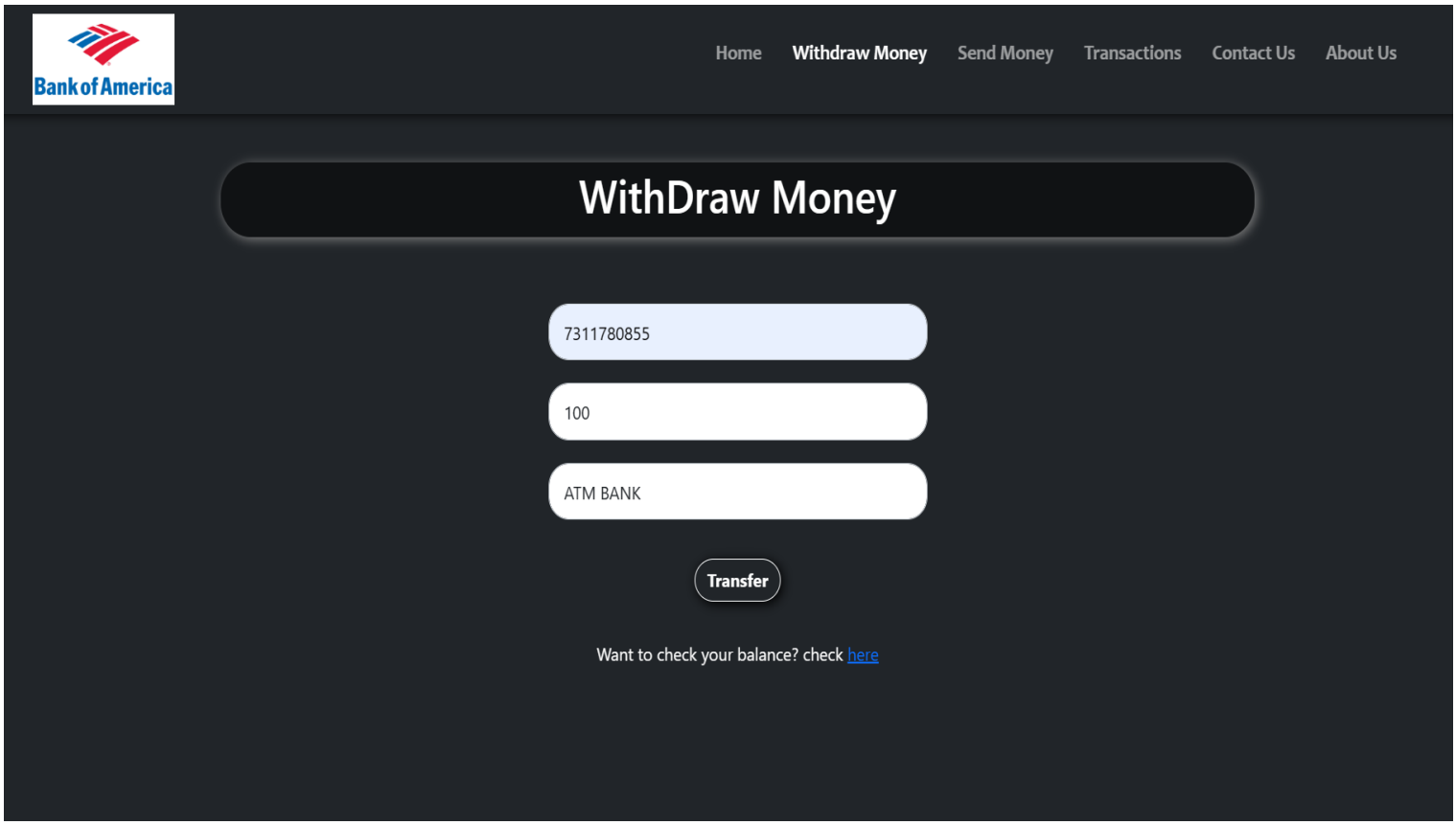
IRIS AND PALM DETECTION



VOICE AND SPEECH RECOGNITION



SELECT BANK ACCOUNT – It allows you to select the bank account to do the transactions



WITH DRAW MONEY - It helps us to withdraw money from the ATM Machine.

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.

[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.

[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.

[4] 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.

[5] 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.

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

[7] 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.

[8] 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.

[9] Malinka, O. Hujnak, P. Hanacek and L. Hellebrandt, "E-Banking Security Study—10 Years Later," in IEEE Access, vol. 10, pp. 16681-16699, 2022.

[10] 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.

[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.

[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

[16] A. Aboalhsan and M. N. Alatawi, "Deep Learning Technique for Fingerprint Recognition," 2022 2nd International Conference on Computing and Information Technology (ICCIT), Tabuk, Saudi Arabia, 2022, pp. 340-343

[17] F. Wang, J. Cheng, W. Liu and H. Liu, "Additive Margin Softmax for Face Verification," in IEEE Signal Processing Letters, vol. 25, no. 7, pp. 926-930, July 2018

[18] C. Y. Lo, C. -W. Sham and L. Ma, "A Novel Iris Verification Framework Using Machine Learning algorithm on Embedded Systems," 2020 IEEE 9th Global Conference on Consumer Electronics (GCCE), Kobe, Japan, 2020, pp. 173-175

SIMATS ENGINEERING

ENGINEER TO EXCEL

Approved By AICTE | IET-UK Accreditation

NATIONAL CONFERENCE ON RECENT TRENDS IN ANALYTICS AND COMPUTING TECHNOLOGIES (RTACT 2024)

CERTIFICATE

This is to certify that Mr / Ms **MONISHA T** has presented a paper titled **"ENHANCING BANKING SECURITY THROUGH MULTIMODAL BIOMETRIC AUTHENTICATION SYSTEM"** from **Prince Dr K Vasudevan College Of Engineering And Technology** in the **"National Conference On Recent Trends In Analytics And Computing Technologies (RTACT 2024) held on 15th March 2024"** Organized by Department of AR and VR, Institute of CSE, SIMATS Engineering, SIMATS, Chennai - 602105.

Convenor
Dr. M. Gunasekaran

Principal
Dr. B. Ramesh

SIMATS ENGINEERING

ENGINEER TO EXCEL

Approved By AICTE | IET-UK Accreditation

NATIONAL CONFERENCE ON RECENT TRENDS IN ANALYTICS AND COMPUTING TECHNOLOGIES (RTACT 2024)

CERTIFICATE

This is to certify that Mr / Ms **RESHMA J** has presented a paper titled **"ENHANCING BANKING SECURITY THROUGH MULTIMODAL BIOMETRIC AUTHENTICATION SYSTEM"** from **Prince Dr K Vasudevan College Of Engineering And Technology** in the **"National Conference On Recent Trends In Analytics And Computing Technologies (RTACT 2024) held on 15th March 2024"** Organized by Department of AR and VR, Institute of CSE, SIMATS Engineering, SIMATS, Chennai - 602105.

Convenor
Dr. M. Gunasekaran

Principal
Dr. B. Ramesh