Prince Mohammad bin Fahd University
College of Computer Engineering and Science (CCES)
Department: Computer Engineering and Science

Senior Project Report

BioAuth ATM System

Team Members:

Faie Albassam – 201900646 – Software Engineering (SE)

Dalal Almubarak – 201900514 – Software Engineering (SE)

Noura Alzuabi – 201901750 – Software Engineering (SE)

Hayat Batook – 202000267 – Software Engineering (SE)

Project Advisor:

Dr. Marius Nagy

Semester: Spring 2024

Submission Date: 30th April, 2024

Table of Contents

Table of Figures

1. Introduction

This report aims to present a detailed overview of the biometric ATM system project, which seeks to revolutionize the traditional ATM experience. By leveraging cutting-edge facial and fingerprint recognition technology, this innovative system will eliminate the need for physical cards and PIN numbers, providing users with a secure and convenient banking experience.

We will develop this biometric ATM system and will utilize industry-standard tools and methodologies to ensure the highest levels of security, performance, and usability.

1.1. Justification and Importance:

The justification for implementing biometric authentication lies in the vulnerabilities of the traditional ATM system, such as card theft, skimming, and unauthorized access. By eliminating the reliance on physical cards, the biometric ATM system will significantly enhance security and protect users' accounts.

Furthermore, this system will offer improved accessibility for individuals with disabilities or those who struggle with remembering or entering PINs. With its user-friendly interface and multi-language support, the biometric ATM system will cater to a diverse user base, ensuring a seamless banking experience for all.

In addition to its security and convenience benefits, the biometric ATM system will also contribute to a more sustainable future by reducing the need for physical cards and their associated environmental impact.

This report will provide a comprehensive overview of the entire project, covering the system requirements, design, implementation, testing, and deployment phases. It will serve as a valuable resource for understanding the development and potential impact of the biometric ATM system.

1.2. Background/Literature Survey

The proposed biometric ATM system seeks to improve security and convenience in banking by replacing traditional card-based authentication with advanced facial and fingerprint recognition technology. This innovative approach aims to address the risks related to card skimming, theft, and unauthorized account access.

Biometric authentication systems have become increasingly popular due to their ability to offer a high level of security and user convenience. Facial recognition technology has been widely used in various sectors such as law enforcement, security systems, and mobile device access control [1]. Similarly, fingerprint recognition has been a well-established biometric authentication method known for its reliability and user-friendliness [2].

Various researchers have explored integrating biometric authentication into ATM systems. For instance, Obed-Emeribe [3] proposed a multimodal biometric ATM system that combines face, fingerprint, and iris recognition to enhance security by requiring multiple biometric traits for authentication. However, their system still relied on traditional card-based initiation, which could pose vulnerabilities related to cards.

Similarly, Babatunde. [4] developed a fingerprint-based ATM authentication system that eliminated the need for cards or PINs. Their system utilized minutiae-based fingerprint matching and achieved an impressive accuracy rate of 98.67%. While this approach mitigates card-related risks, it solely relies on fingerprint recognition, which may not be suitable for all users or situations.

The proposed biometric ATM system aims to leverage the strengths of facial and fingerprint recognition, allowing users to choose their preferred authentication method while ensuring a high level of security. By eliminating the need for physical cards, the system reduces the risks associated with card skimming, loss, or theft, ultimately providing a more secure and convenient banking experience.

2. Requirements Analysis

2.1. Functional Requirements

FR -1 User Authentication

R-1.1: A four-digit PIN, a fingerprint, or a mix of both must be used by the system to authenticate users.

R-1.1: In order to authenticate, users must input their national ID.

FR-2: Biometric Authentication:

R-2.1: System shall be capable of supporting both facial recognition and fingerprint recognition as methods of biometric authentication.

R-2.2: Users shall be able to register his/her face and fingerprint when creating an account.

R-2.3: User shall be able to login to ATM using either facial recognition or fingerprint recognition.

FR-3 National ID Verification

R-3.1: The system shall prompt users to enter their national ID along with biometric or PIN authentication.

R-3.2: The user's entered national ID will be cross-referenced with previously stored national ID records.

R-3.3: Users will be prompted by the system to provide their national ID in addition to a PIN or biometric authentication.

FR-4 PIN Verification

R-4.1: The PIN entered by the user will be compared to the stored PIN linked to their account by the system.

R-4.2: For authentication, users will need to enter a 4-digit PIN.

FR-5: Account Management

R-5.1: Users shall be able to register an account into the ATM system.

R-5.2: Users shall be able to modify his/her account information.

R-5.3: Users shall be able to delete his/her account.

FR-6: Transaction Processing

R-6.1: User shall be able to withdraw funds from account.

R-6.2: Users shall be able to deposit funds in account.

R-6.3: Users shall be able to transfer funds for his/her account to another account.

R-6.4: Users shall be able to print account statements.

R-6.5: Users shall be able to view his/her account balance.

FR-7: Backup Authentication:

R-7.1: In case of biometric authentication failure, the system shall allow the user to use physical card and PIN as backup authentication method.

FR-8: Password Recovery:

R-8.1: System shall have forgot password option that will allow the user to reset his/her account password.

FR-9: User Interface:

R-9.1: The ATM's interface should be simple to use and straightforward, aiding users with the transaction and authentication procedures.

R-9.2: Users must be guided through the authentication process with the help of explicit instructions and prompts.

2.2. Non-Functional Requirements

NFR 1: Security:

The system shall guarantee the utmost level of data security and privacy by implementing stringent security measures to safeguard against potential threats and breaches.

NFR 2: Performance:

The system shall be designed to provide rapid and reliable biometric recognition within an acceptable timeframe. This shall be accomplished through the optimization of hardware components and software algorithms.

NFR 3: Scalability:

The system shall be created with scalability in mind to accommodate a growing user base and increasing transaction volume. This will enable seamless expansion without compromising performance, with the system architecture being

NFR 4: Reliability:

Emphasis shall be placed on reliability, with measures in place to minimize system downtime. The system shall be resilient against potential hardware and software failures to ensure uninterrupted service.

NFR 5: Compliance:

The system shall strictly adhere to data protection and privacy regulations, ensuring full compliance with legal requirements governing the handling and storage of biometric data.

NFR 6: Usability:

The system shall be user-friendly and intuitive, requiring minimal training for users to navigate the interface effectively.

NFR 7: Response Time:

The system shall respond promptly to user inputs and requests, ensuring a smooth and efficient user experience.

NFR 8: Data Backup and Recovery:

Regular data backups and a robust recovery plan shall be implemented to prevent data loss in case of system failures.

NFR 9: Regulatory Compliance:

The system shall comply with industry-specific regulations and standards related to banking, data protection, and biometric authentication.

NFR 10: Error Handling and Logging:

Comprehensive error-handling mechanisms shall be in place, with detailed logs maintained for troubleshooting and auditing purposes.

NFR 11: Network Security:

Encryption protocols and security measures shall be utilized to protect data during transmission.

2.3. Security Requirements

The biometric ATM system must incorporate stringent security measures to safeguard user data, thwart unauthorized access, and guarantee the integrity and non-repudiation of transactions. The specified security requirements include:

Biometric Data Security:

- Utilization of industry-standard encryption algorithms (e.g., AES-256) to securely store and transmit biometric data (facial and fingerprint information).
- Secure storage of biometric data in a tamper-proof database or storage system.
- Strict control and auditing of access to biometric data.

Authentication and Authorization:

- Implementation of robust authentication mechanisms, like multi-factor authentication, to ensure only authorized users can access the system.
- Support for role-based access control (RBAC) to limit access to sensitive functions and data based on predefined user roles (e.g., administrators, tellers, customers).
- Enforcement of strong password policies (e.g., minimum length, complexity, expiration) for user accounts, with passwords securely hashed and salted using industry-standard algorithms (e.g., bcrypt, Argon2) before storage.

Data Security:

- Encryption of all sensitive data (e.g., account information, transaction details) at rest and in transit using industry-standard encryption algorithms (e.g., AES-256, TLS 1.3).
- Implementation of measures to prevent common web application vulnerabilities, such as SQL injection, cross-site scripting (XSS), and cross-site request forgery (CSRF).

- Regular security audits and penetration testing to identify and address potential vulnerabilities.

Transaction Security:

- Incorporation of digital signatures and non-repudiation mechanisms to ensure the integrity and authenticity of transactions.
- Maintenance of tamper-proof transaction logs to prevent unauthorized modifications.
- Implementation of mechanisms to detect and prevent fraudulent activities, such as money laundering or unauthorized transactions.

Compliance and Regulations:

- The system must adhere to applicable industry regulations and standards, including the Payment Card Industry Data Security Standard (PCI DSS), the General Data Protection Regulation (GDPR), and local data protection laws.

Security Monitoring and Incident Response:

- The system must incorporate thorough logging and monitoring systems to promptly identify and address security incidents.
- There must be an established incident response plan to effectively manage security breaches or other security-related incidents.

2.4. Project Constraints

Constraint Number	Constraint Type	Constraint Description
C.1	Budget	The project needs to be completed within the allocated budget limits.
C.2	Timeline	The project must meet the specified timeline and deadlines.
C.3	Resource Availability	The project scope will be limited by the availability of skilled personnel, hardware resources, and software tools.
C.4	Regulatory Compliance	The system must adhere to the regulations, such as data protection laws, banking regulations, and biometric authentication standards.
C.5	Technology Constraints	The system's development will be limited by the capabilities of the chosen technologies, such as facial and fingerprint recognition algorithms, hardware performance, and integration with existing banking systems.
C.6	Security	The system must adhere to strict security requirements to safeguard user data, prevent unauthorized access, and ensure transaction integrity.
C.7	Scalability	The system should be designed to support future scalability needs in user base and transaction volumes without significant performance decline.
C.8	Usability	The user interface of the system must be user-friendly and shall provide a good user experience, catering to users with different levels of technical proficiency and accessibility needs.
C.9	Hardware	The system's capabilities will be constrained by the chosen ATM hardware components, including processing power, memory, and peripheral devices.
C.10	Integration	The system must seamlessly integrate with existing banking systems, and databases, following established protocols and interfaces.

2.5. Risk Assessment

It is essential to recognize and address the different risks associated with the implementation of the biometric ATM system, including technical, project management, and external risks.

Risk(s)	Potential Impact	Risk Mitigation
Unauthorized access to biometric data	User data and privacy breach, potential financial losses, and legal obligations	▪ Implement encryption protocols and establish secure storage methods for biometric information ▪ Enforce strict access restrictions and maintain detailed audit logs ▪ Perform routine security assessments and penetration tests to ensure data protection ▪ Comply with industry regulations and standards regarding the protection of sensitive data
Hardware malfunctions or compatibility issues	Interruption of system operations, service disruption, and potential data loss	▪ Choose high-quality hardware components ▪ Incorporate redundancy and failure mechanisms ▪ Ensure continuous maintenance and testing ▪ Ensure hardware and software components are compatible
Challenges in integrating with current banking systems	Delayed deployment, data discrepancies, and potential system breakdowns	▪ Perform comprehensive compatibility testing and properly integration planning ▪ Follow industry-standard protocols and interfaces ▪ Work closely with banking partners ▪ Establish data synchronization and reconciliation mechanisms.
Scalability challenges to accommodate more users and transactions	Decreased performance, system limitations, and potential service interruptions	▪ Develop a system architecture that is both modular and scalable. ▪ Deploy load balancing and horizontal scaling techniques. ▪ Monitor system performance regularly and make optimizations when necessary.

		▪ Prepare for capacity growth and consider hardware upgrades in the future.
Issues with user accessibility and experience	Low user acceptance, customer discontent, and potential legal obligations	▪ Carry out thorough user testing and integrate feedback ▪ Comply with accessibility standards and guidelines ▪ Offer in-depth user training and support ▪ Integrate localization and multi-language support.
Project schedule and budget overruns	Delivery delays, increased expenses, and potential project termination	▪ Create a project plan and schedule ▪ Utilize efficient project management techniques ▪ Consistently track advancements and make necessary resource adjustments ▪ Set up transparent communication channels
External threats such as natural disasters or pandemics.	Disruptions in project tasks, limited resources, and potential delays	▪ Create an extensive business continuity and disaster recovery plan ▪ Execute remote collaboration and telecommuting strategies ▪ Set up backup plans and alternative resource distribution strategies

2.6. Applicable Standards

To guarantee the security, data protection, and interoperability of the biometric ATM system, it is imperative to adhere to a variety of industry standards and regulations. The project will strictly follow the following standards and guidelines:

1. **Payment Card Industry Data Security Standard (PCI DSS):** The system will be in compliance with the PCI DSS, a universally recognized set of security standards aimed at ensuring the safe handling of payment card data and transactions.
2. **General Data Protection Regulation (GDPR):** Given that the system will be handling personal data, including biometric information, it must adhere to the GDPR, a comprehensive data protection regulation enforced by the European Union.
3. **ISO/IEC 19794 Biometric Data Interchange Formats:** The system will adhere to

the ISO/IEC 19794 standards, which outline data formats for the exchange of biometric data, such as facial and fingerprint data.

4. **ISO/IEC 24779 Biometric Sample Quality:** The system will follow the ISO/IEC 24779 standards, which offer guidelines and best practices for evaluating the quality of biometric samples, like facial images and fingerprint scans.
5. **ISO/IEC 27001 Information Security Management:** An information security management system (ISMS) will be implemented in accordance with the ISO/IEC 27001 standard to ensure the confidentiality, integrity, and availability of information assets.
6. **Accessibility Guidelines:** The system will adhere to accessibility guidelines and standards, including the Web Content Accessibility Guidelines (WCAG) and Section 508 of the Rehabilitation Act, to ensure usability for individuals with disabilities.
7. **Banking Industry Standards:** The system will comply with pertinent banking industry standards and regulations, as stipulated by regulatory bodies like the Financial Action Task Force (FATF) and the Office of Foreign Assets Control (OFAC).

By upholding these standards and regulations, the biometric ATM system will guarantee data security and privacy.

2.7. Requirement Specification

R -1 User Authentication

R-1.1: A four-digit PIN, a fingerprint, or a mix of both must be used by the system to authenticate users.

- Users have the option of authenticating with their fingerprint, a four-digit PIN, or a mix of the two.

R-1.1: In order to authenticate, users must input their national ID.

- Users must supply both their preferred login method and their national ID during the authentication process.
- This ensures that users provide an additional form of identification for extra security.

R-2: Biometric Authentication:

R-2.1: System shall be capable of supporting both facial recognition and fingerprint recognition as methods of biometric authentication.

- System shall have the capability of facial recognition as a method of authentication for ATMs.
- System shall have the capability of fingerprint recognition as a method of authentication for ATMs.

R-2.2: Users shall be able to register his/her face and fingerprint when creating an account.

- System shall allow the user to register his/her face and fingerprint when creating an account.

R-2.3: User shall be able to login to ATM using either facial recognition or fingerprint recognition.

- Login screen shall provide users with three options for login such as PIN, Face, or Fingerprint.
- Users shall be able to login to their account by presenting their registered face and providing their national ID for verification.

- Users shall also have the option to login using their registered fingerprint and national ID for verification.
- If biometric authentication fails, the system shall display an error on screen.

R-3 National ID Verification

R-3.1: The system shall prompt users to enter their national ID along with biometric or PIN authentication.

- Users will be required to enter their national ID during the authentication procedure in addition to their preferred PIN or biometric authentication option.
- This ensures that users provide an additional form of identification for extra security.

R-3.2: The user's entered national ID will be cross-referenced with previously stored national ID records.

- The inputted national ID will be compared to the national ID records kept in the database to confirm its legitimacy.
- By verifying that the national ID supplied matches the data kept in the system, this cross-referencing procedure helps to prevent unauthorized access.

R-3.3: Users will be prompted by the system to provide their national ID in addition to a PIN or biometric authentication.

- When users start the authentication process, the system will ask them to enter their PIN or preferred biometric authentication method in addition to their national ID.
- This provides an additional degree of security to the authentication process by guaranteeing that users submit their national ID for verification.

R-4 PIN Verification

R-4.1: The PIN entered by the user will be compared to the stored PIN linked to their account by the system.

- The system will confirm a user's PIN during authentication by comparing it to the PIN that is stored in relation to the user's account.
- This improves security by guaranteeing that only users possessing the correct PIN can access their accounts.

R-4.2: For authentication, users will need to enter a 4-digit PIN.

- In order to access their accounts, users must enter a 4-digit PIN during the authentication process.
- Users' authentication process is made simpler and more secure with this standard PIN format.

R-5: Account Management

R-5.1: Users shall be able to register an account into the ATM system.

- Users shall be able to register an account by providing required details such as First Name, Last Name, Email, and Password.
- In account registration, the system shall ask the user to register his/her face and fingerprint for biometric authentication purposes.

R-5.2: Users shall be able to modify his/her account information.

- Users shall be able to update his/her account information such as First Name, Last Name, Email, and Password.
- Users shall also be able to set transaction limit, account limit, and preferred language in account setting.

R-5.3: Users shall be able to delete his/her account.

- System shall allow the user to delete his/her account.
- Account deletion shall require authentication to confirm.

R-6: Transaction Processing

R-6.1: User shall be able to withdraw funds from his/her account through the ATM.

- System shall show some options a user can select from such as 50, 100, 200, 300, 500, 1000, 5000 SAR.
- System shall allow the user to enter an amount manually.

R-6.2: Users shall be able to deposit funds into his/her account.

- System shall allow the user to deposit money in his/her account through the ATM.
- System shall count the amount and shall ask the user to confirm if it is correct.
- If the user clicks “Not Correct”, the system shall recount the amount.
- System shall generate an invoice for deposit.

R-6.3: Users shall be able to transfer funds for his/her account to another account.

- Users shall be allowed to transfer funds from his/her account to another account.

R-6.4: Users shall be able to print an account statement.

- Users shall be allowed to print account statements that list the last 10 transactions.

R-6.5: Users shall be able to view his/her account balance.

- User shall be able to view his/her account balance.
- System shall print an invoice for account balance.

R-7: Backup Authentication:

R-7.1: In case of biometric authentication failure, the system shall allow the user to use physical card and PIN as backup authentication method.

- Users shall be allowed to login using his/her ATM card and PIN.

R-8: Password PIN:

R-8.1: System shall have forgot PIN option that will allow the user to reset his/her account password.

- To begin the PIN recovery process, users must input their First Name, Last Name, National ID and Email.
- The user's email address will receive a confirmation code for validation.
- Users will input the code into the system for validation after receiving it.
- Users will be asked to enter a new PIN to finish the PIN reset process after successful verification.

R-9: User Interface:

R-9.1: The ATM's interface should be simple to use and straightforward, aiding users with the transaction and authentication procedures.

- Ease of use should be given top priority in interface design, with clear visual cues and simple navigation to help users move through transactions.
- The layout of the menu and button positions on the user interface should be optimized for simplicity of use and accessibility.

R-9.2: Users must be guided through the authentication process with the help of explicit instructions and prompts.

- The interface should give users clear instructions on what to do during the authentication process.

- Where users are to enter their authentication credentials—such as PIN, fingerprint, face recognition, or national ID—should be indicated visually.
- If authentication fails, error messages that instruct users on how to fix the problem and try authentication again should be shown.

2.8. Project Plan

The project plan delineates the schedule and duties necessary to carry out the project from planning to monitoring and control.

Phase 1: Planning and Analysis

1. Define Project Scope and Objectives: Outline project goals, scope, and objectives.
2. Gather Requirements: Collect detailed functional and non-functional requirements.
3. Regulatory Compliance Assessment: Research legal and regulatory requirements for biometric data in banking.
4. Risk Assessment: Identify and mitigate potential project risks.

Phase 2: Design

5. System Architecture Design: Develop a detailed architecture plan for hardware and software.
6. Database Design: Design and implement a secure database schema.
7. User Interface Design: Create high-fidelity mockups, incorporating stakeholder feedback.
8. Hardware Procurement: Procure required hardware components.

Phase 3: Development

9. Biometric Authentication Module: Implement facial and fingerprint authentication.
10. Account Management Module: Develop user account functionalities.
11. Transaction Processing Module: Integrate transaction features with biometric

authentication.

12. Security Measures Implementation: Integrate multi-factor authentication and encryption.
13. User Interface Implementation: Code user interface based on design.

2.8.1. Sub-Team Responsibilities and Team Structure

Student	Responsibilities
Hayat Batook (202000267)	● Develop a detailed architecture plan for hardware and software. ● Procure the required hardware components (Fingerprint Scanner). ● Implement facial and fingerprint authentication. ● Develop user account functionalities.
Faie Albassam (201900646)	● Design and implement a secure database schema. ● Create mockups, incorporating user feedback. ● Integrate transaction features with biometric authentication. ● Integrate multi-factor authentication and encryption to ensure security
Dalal Almubarak (201900514)	● Outline project goals, scope, and objectives. ● Identify and mitigate potential project risks. ● Code the user interface based on design and mockups
Noura Alzuabi (201901750)	● Collect detailed functional and non-functional requirements. ● Research legal and regulatory requirements for biometric

	data in banking. ● Verify overall system functionality ● Ensure compliance with regulations and security standards.

2.8.2. Project Management

ASANA was used to properly manage the project's development.

Iteration 1: Planning and Analysis

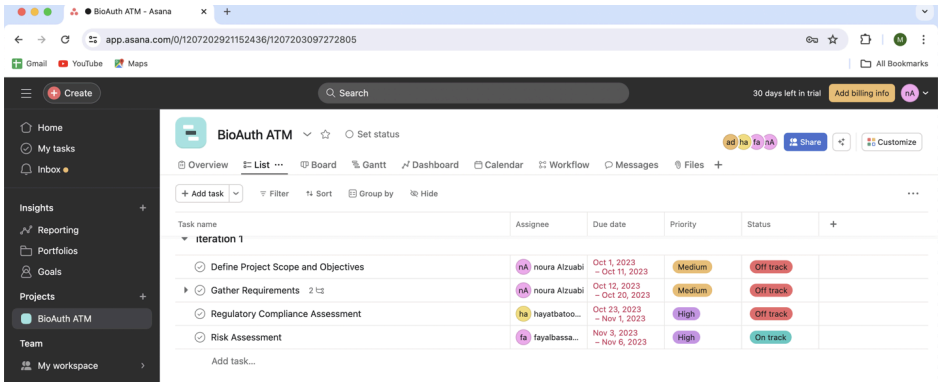

Figure 1 : *Planning and Analysis (Asana)*

Iteration 2: Design

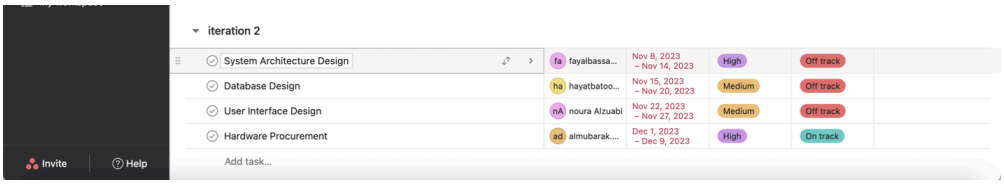

Figure 2 :*Design (Asana)*

Iteration 3: Development

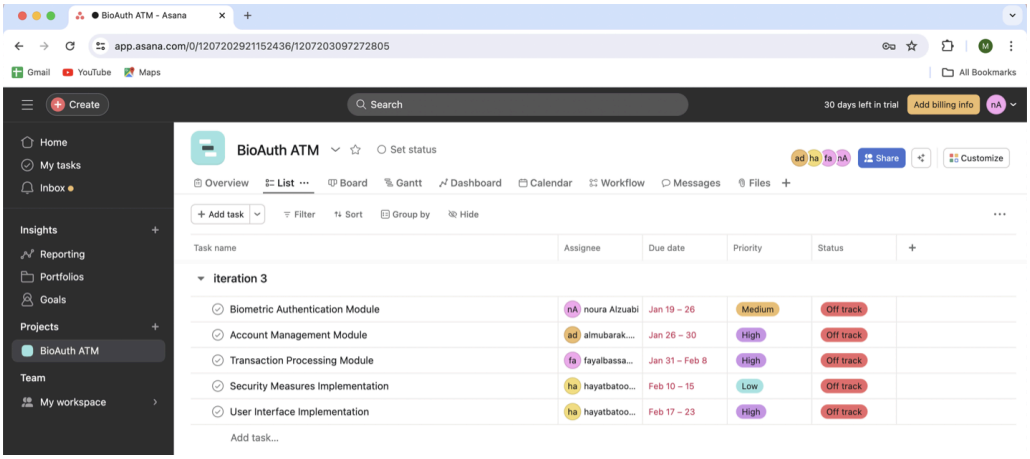

Figure 3 : *Development (Asana)*

Gantt Chart

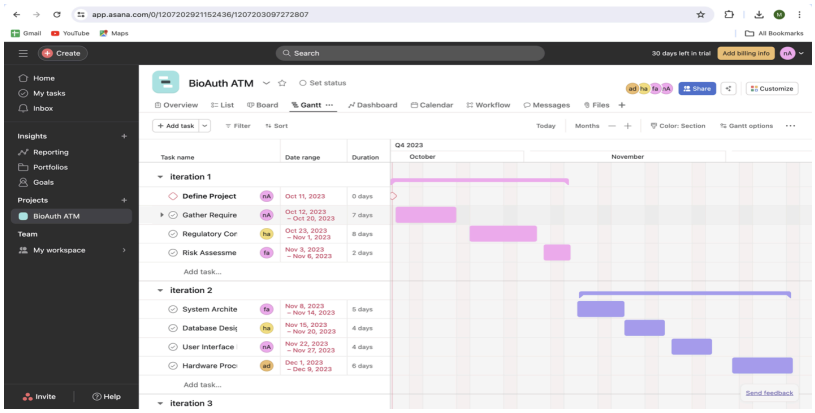

Figure 7 : *Gantt Chart*

(Asana)

Dashboard:

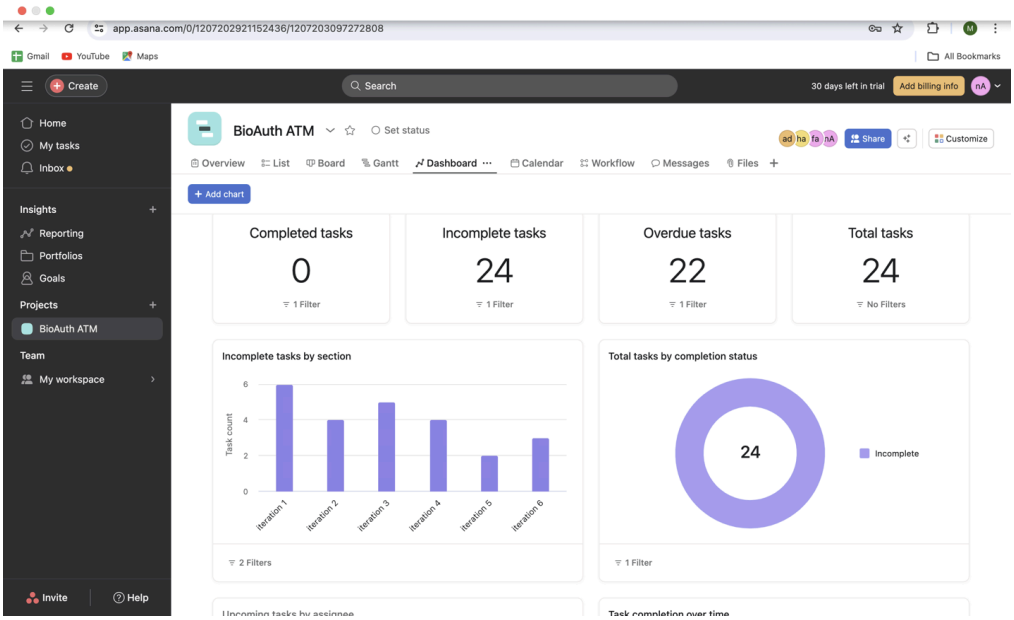

Figure 8 : *Dashboard*

(Asana)

Board:

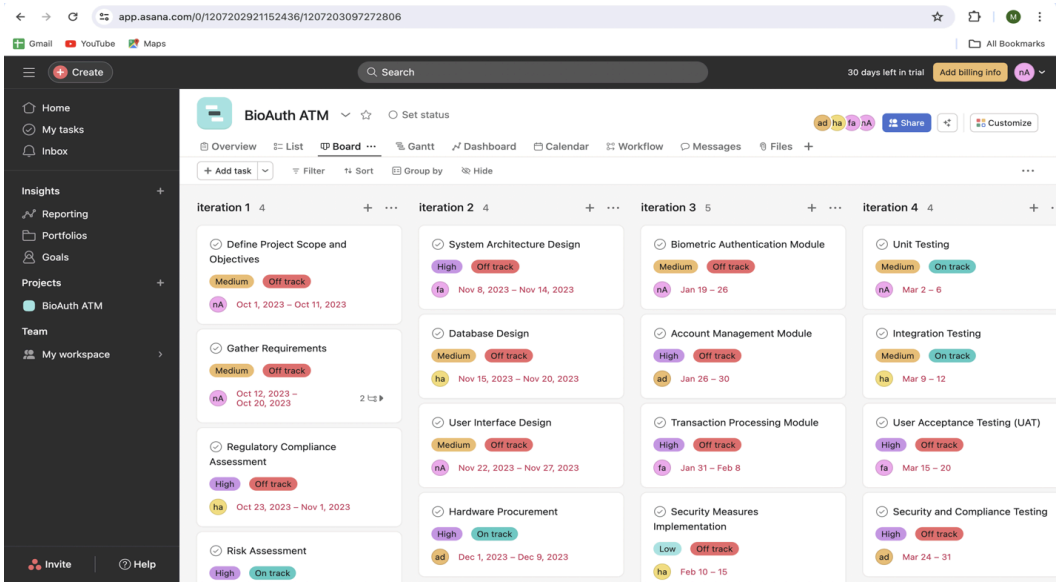

Figure 9: *Board (Asana)*

3. Project Design

3.1. Architecture Diagram

Facial Recognition: This component uses computer vision and machine learning techniques to detect and recognize a user's face for authentication purposes.

Fingerprint Recognition: This component captures and verifies a user's fingerprint for authentication by extracting and matching unique fingerprint patterns.

Authorization Module: This module controls access to the ATM system and its functionalities based on predefined rules and policies. It includes components for authentication (biometric or traditional), access control, policy management, and audit trailing.

Backend System: The backend system is the core component that manages the overall functionality of the ATM system. It includes the database, business logic, integration with external systems, and reporting capabilities.

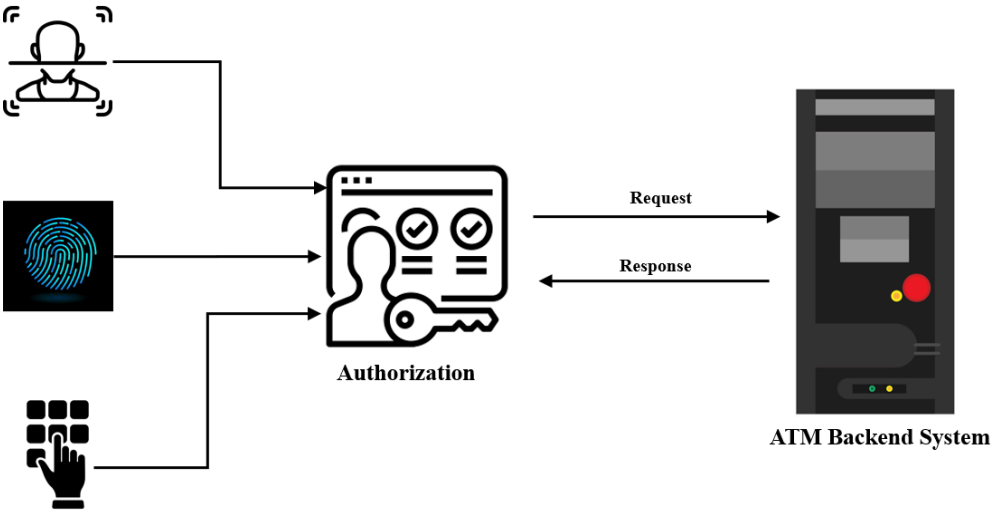

Figure 10: *System Architecture Diagram*

3.2. Conceptual Design

3.2.1. Use Case Diagram

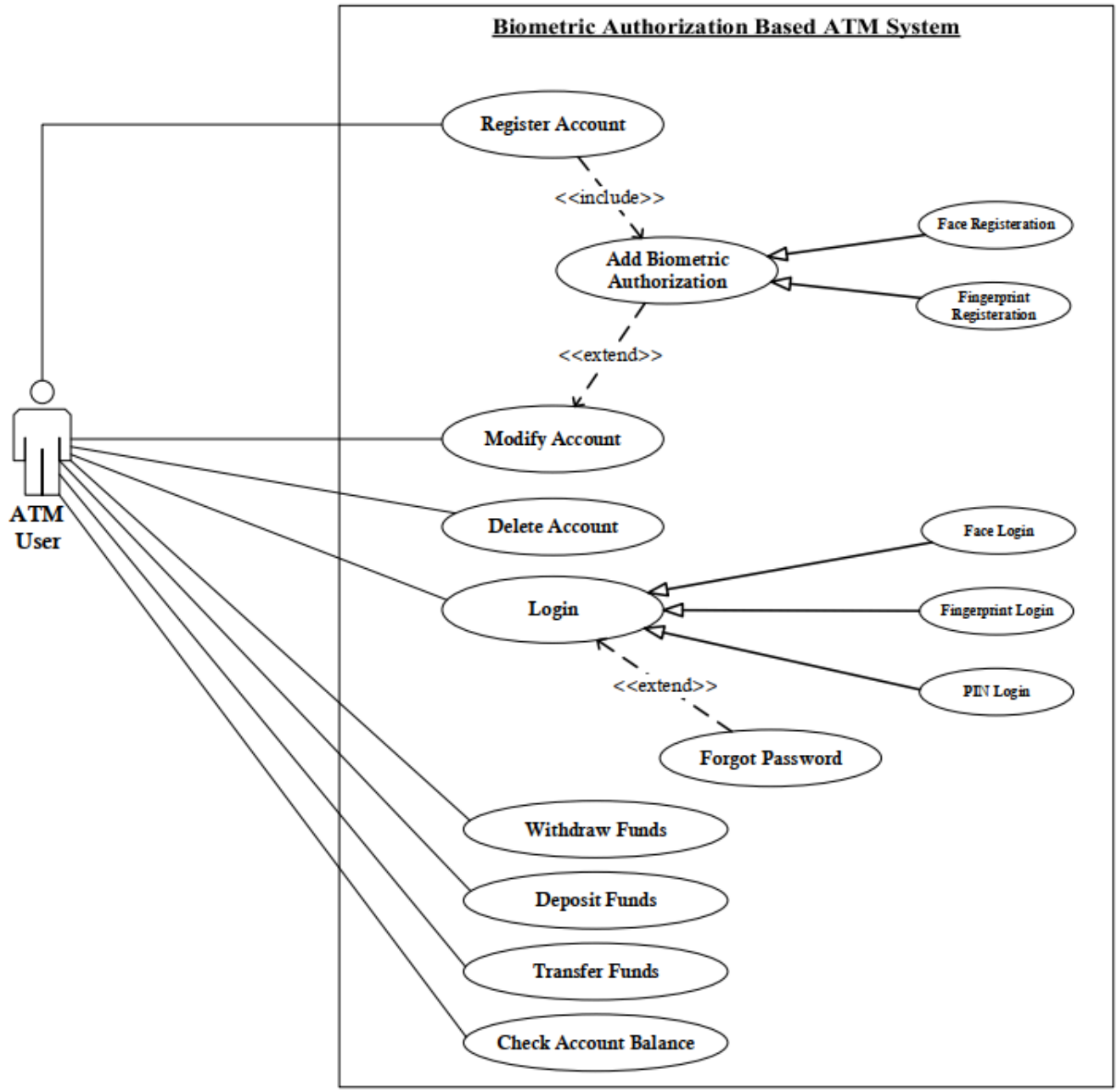

Figure 11: *Use Case Diagram*

3.2.2. *System Flowchart Diagram*

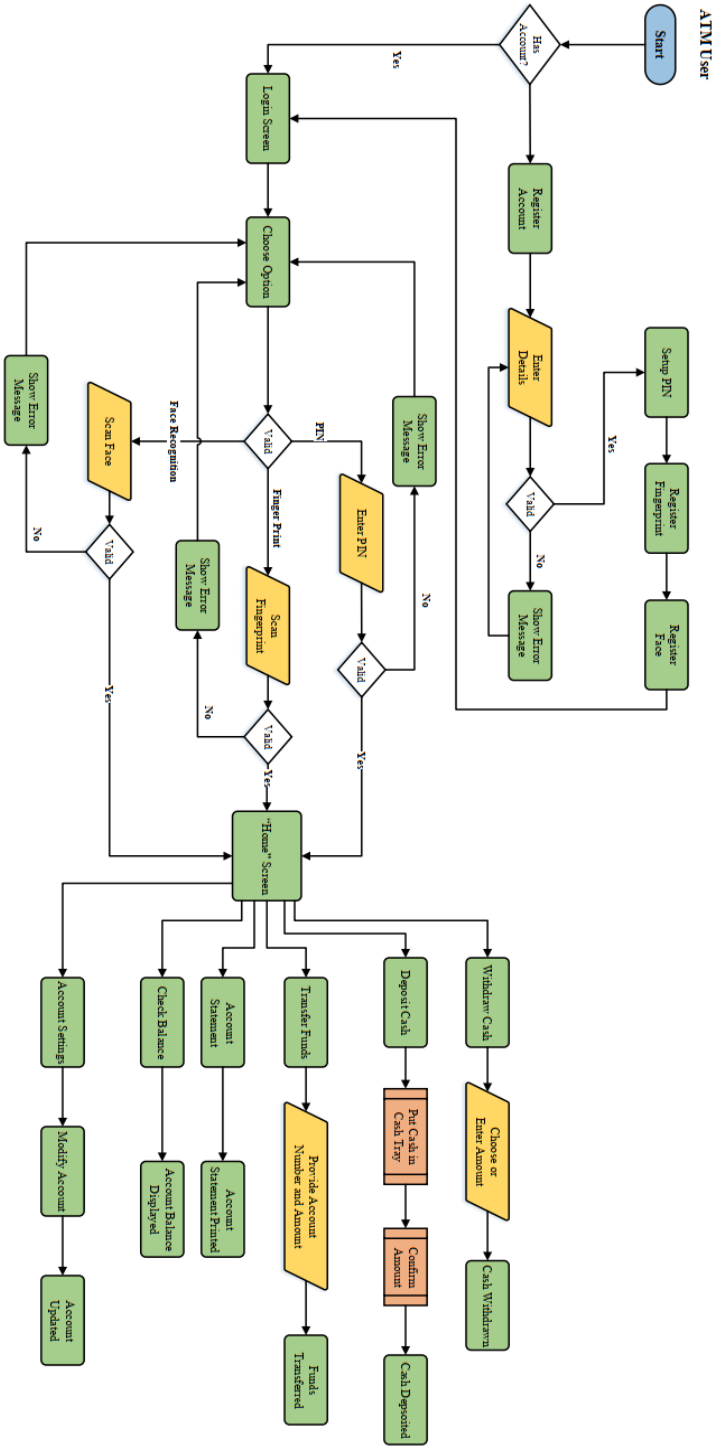

Figure 12: *Use Flowchart Diagram*

3.3. User Interface Design

3.3.1. Start Page

The initial page that will be shown on the ATM when a user approaches and starts the system.

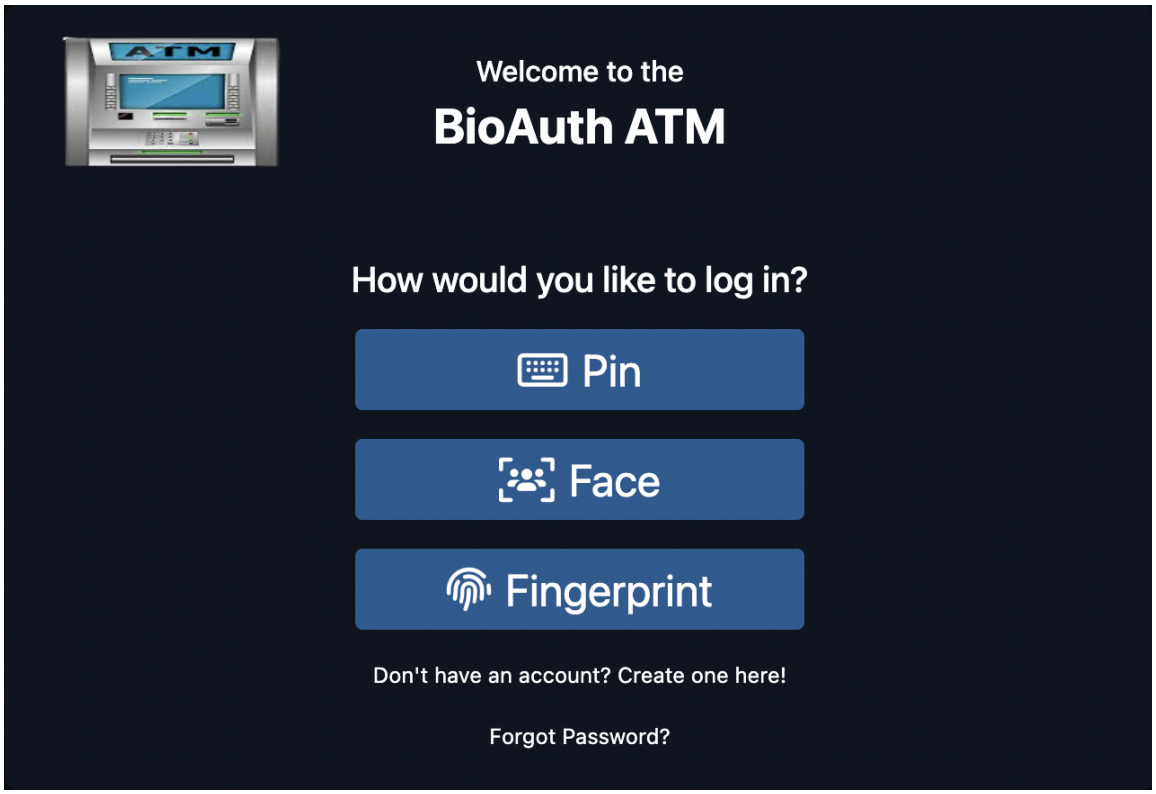

Figure 13: *Start Page*

This screen shows the option to login via

- Pin
- Facial Identification
- Fingerprint Identification

It also allows anyone to create an account directly on the software. Clicking this will direct the user to the Registration screens.In the case that a user is unable to login, they have the option to reset their password to allow them to log in to a website to reset their PIN.

3.3.2. Login Screens

After the user selects which method they would like to use to login, one of the following screens will be shown based on the selection option.

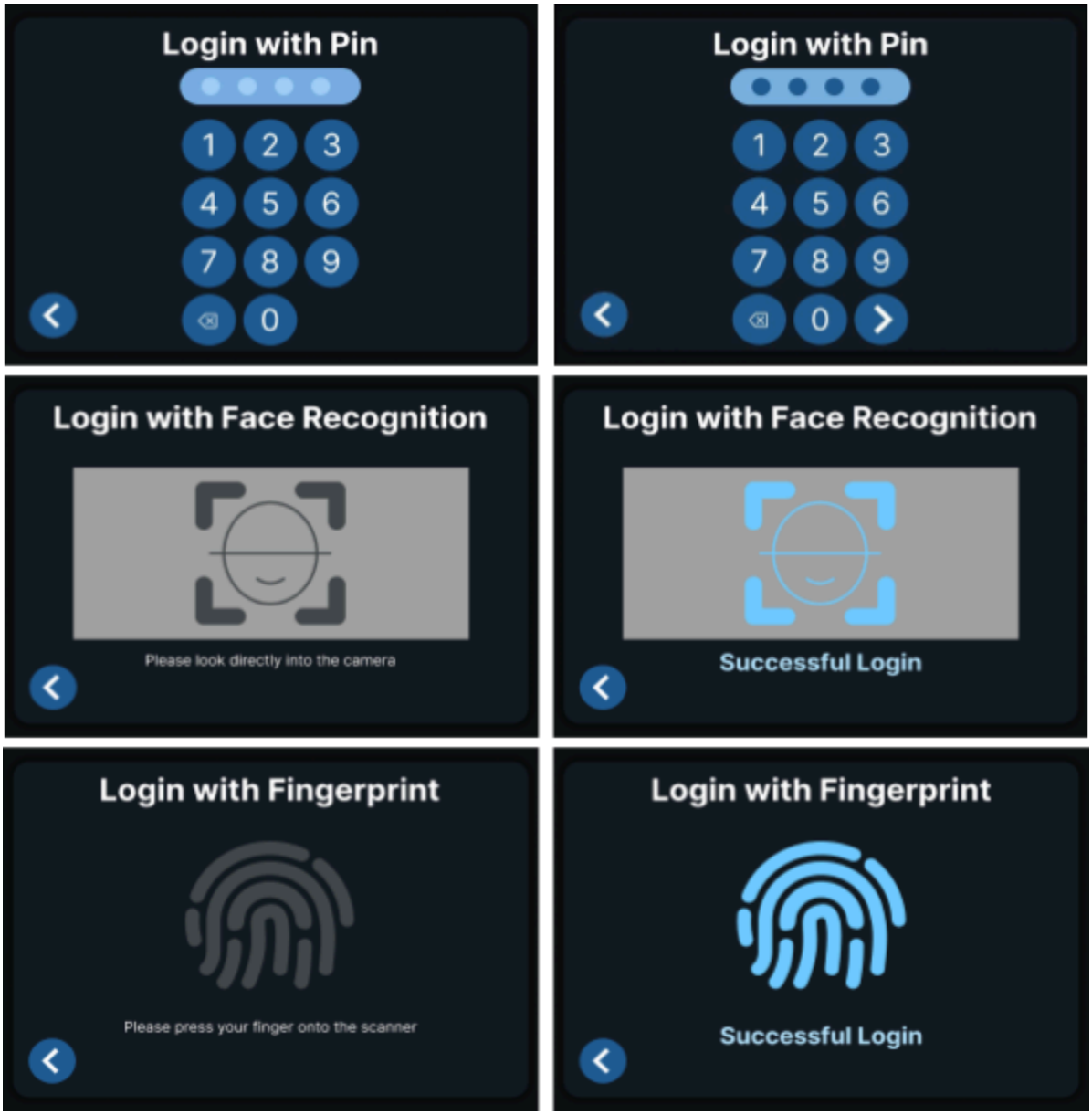

Figure 14: *Login Screens*

When using the PIN input method, the user can move forward by selecting the continue arrow button that appears after entering a 4-digit PIN. The user will be required to enter their national ID for verification in addition to the PIN. The user will successfully log in if the PIN entered is correct and the national ID is successfully verified; if not, an error message will let the user know that either the PIN or the national ID is wrong.

In order for the Face Recognition method to work, the user must face a camera directly for the system to scan their face. The user will be asked to provide their national ID for verification in addition to the facial scan. The user will log in successfully if the facial scan matches the registered face and the national ID is successfully verified; if not, an error message will let the user know that either the national ID or the facial scan is inaccurate.

In order to scan their fingerprint using the fingerprint method, users must place their finger on the system. The user will be asked to provide their national ID for verification in addition to the fingerprint scan. The user will log in successfully if the fingerprint matches the registered fingerprint and the national ID is successfully verified; if not, an error message will let the user know that either the fingerprint or the national ID is incorrect.

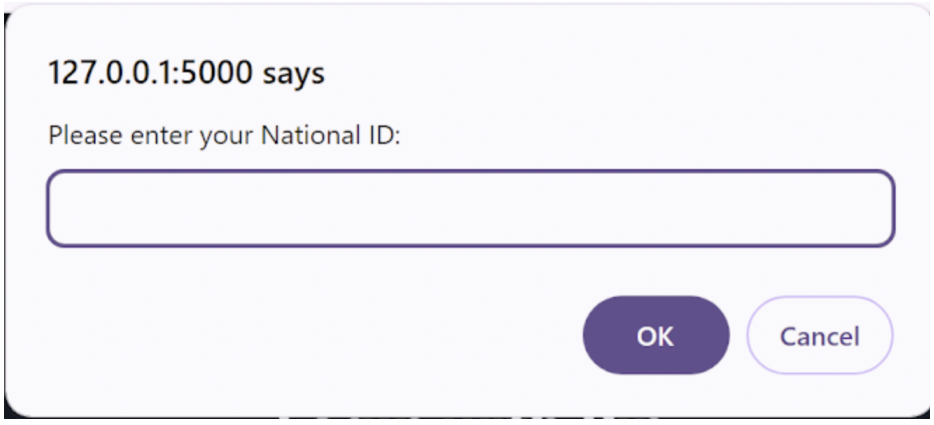

Figure 15: *National ID Input*

3.3.3. Registration Screens

if the user does not have an account, and have clicked to register, they will be asked to fill in the following form:

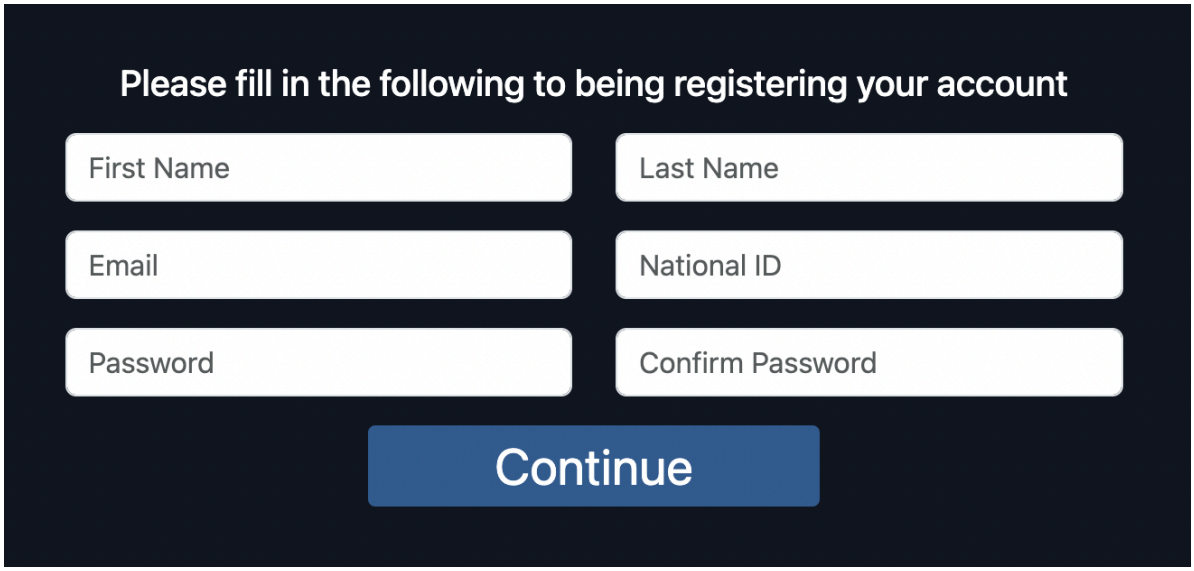

Figure 16: *Registration Screens*

The system will ask the user to fill in their first name, last name, National ID, email, and password.

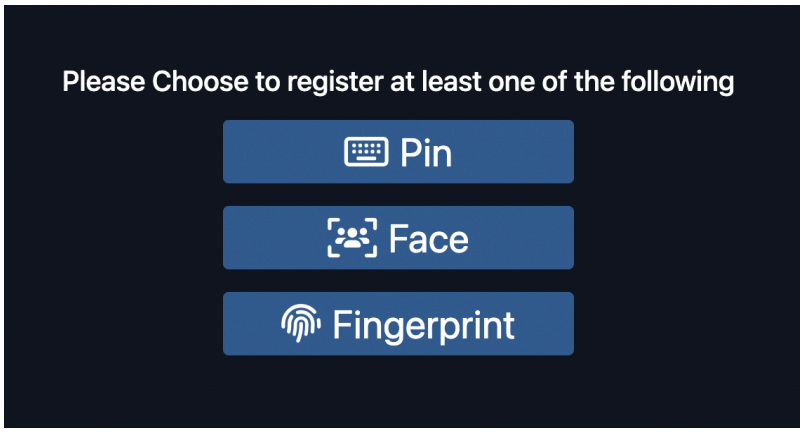

Figure 17.1 : *Add Authentication Methods*

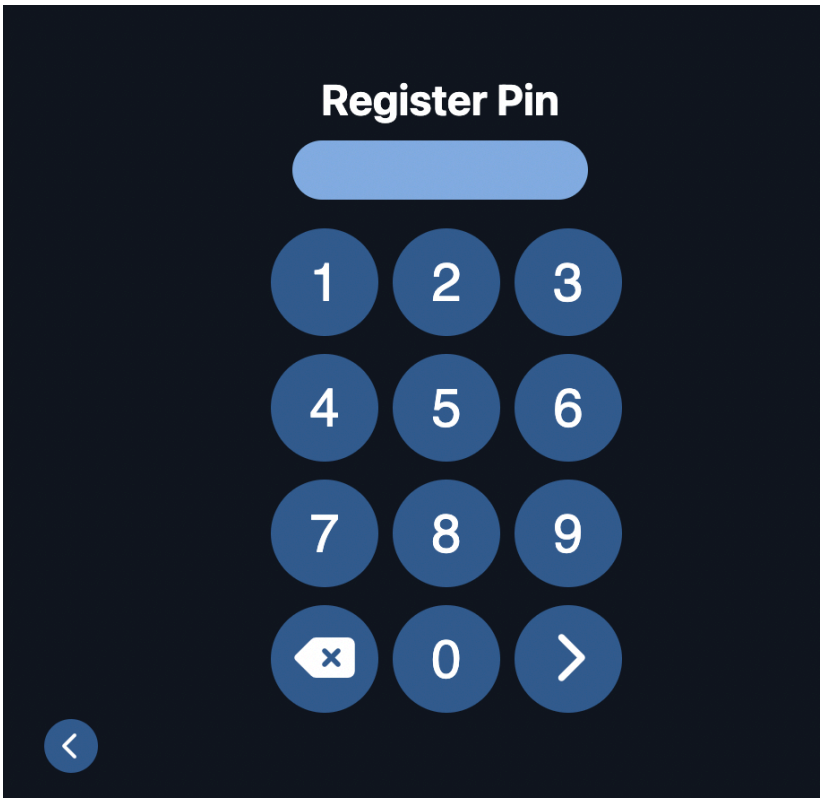

Figure 17.2: *Add Authentication Methods*

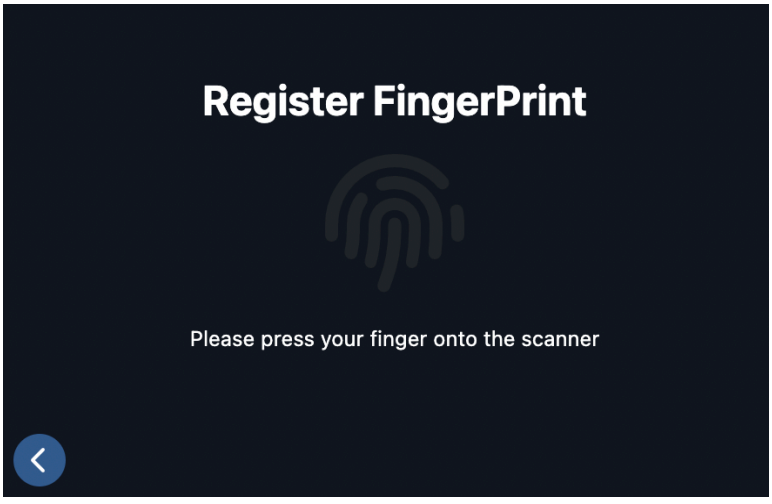

Figure 17.2: *Add Authentication Methods*

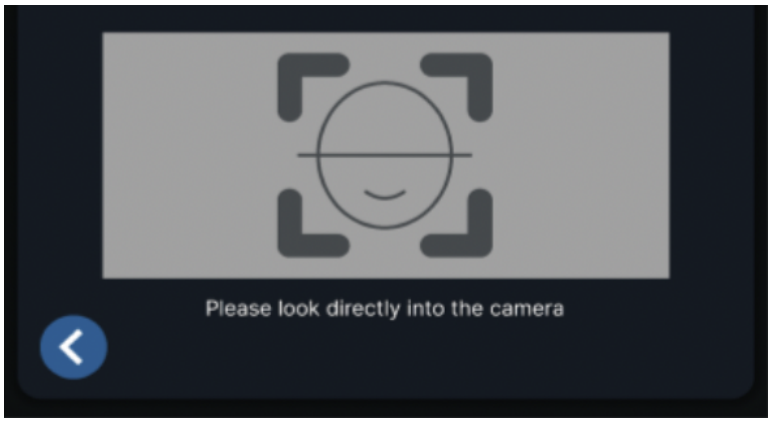

Figure 17.3: *Add Authentication Methods*

The user will be asked to register at least one of the biometric authentication methods.

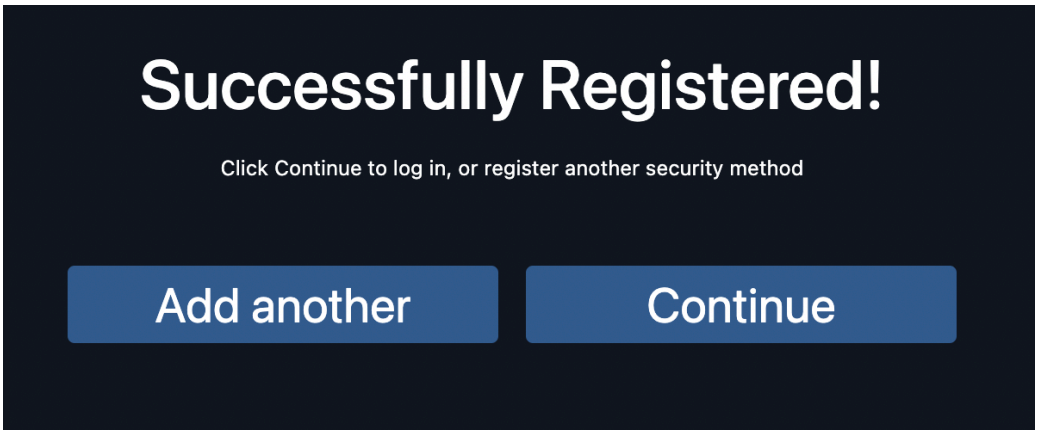

Figure 18: *Registration Screens - Success*

After the user has registered a biometric authentication method, they will have the option to register another method or proceed with logging in.

3.3.4. Forgot Passwords

if user has forgotten their password, they need to input their First and Last name, along with their Email. If these details exist in the system, an email with a reset code will be sent to the user, allowing them to change their password. After this, the user will be logged in to the system.

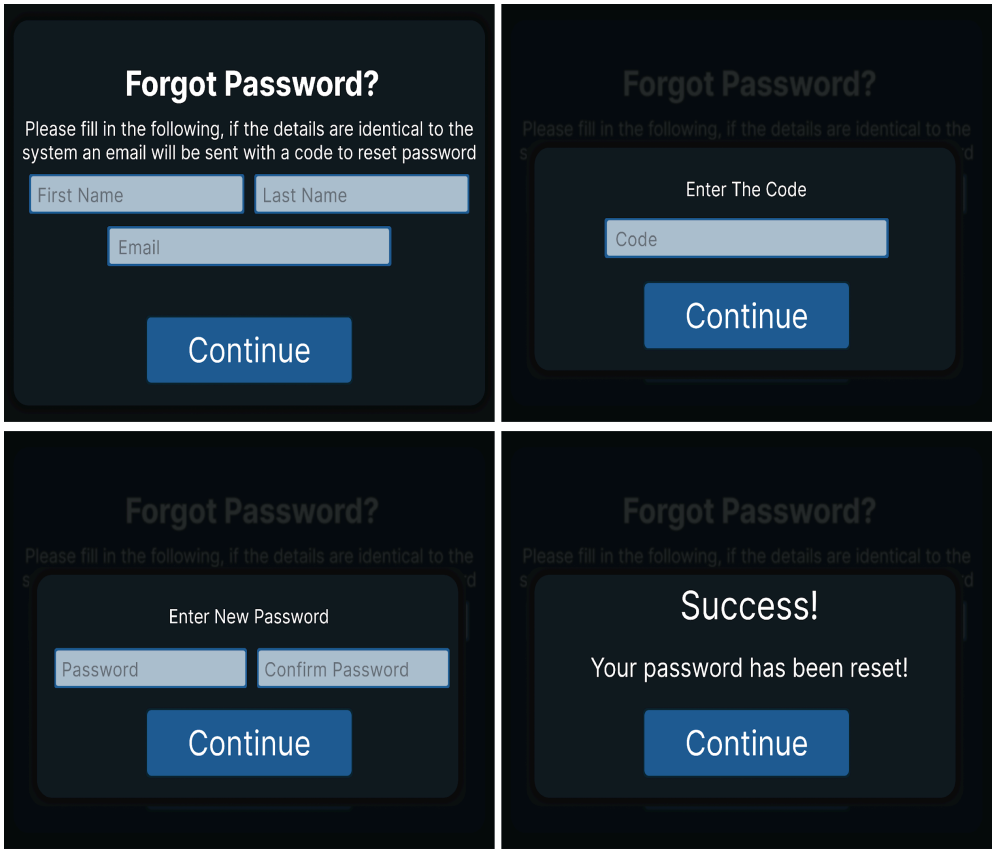

Figure 19: *Forgot Password Screen*

3.3.5. Home Screen

After a successful login, users will be directed to the home page, allowing them to choose what they would like to do whilst in the system.

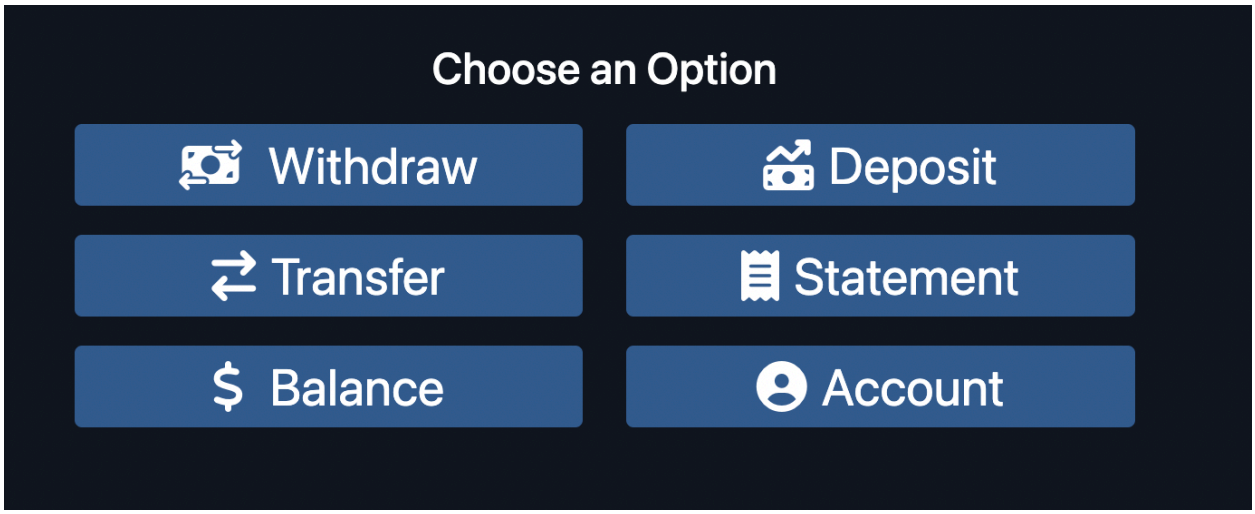

Figure 20: *Home Screen*

The following are the options the user as their selections:

- **Withdraw:** Allows the user to take out money.
- **Deposit:** Allows the user to add money to their account.
- **Transfer:** Allows the user to transfer to another account.
- **Statement:** Prints a Mini Statement the user can read.
- **Balance:** Shows the total balance the user has in their account, along with the last few transactions.
- **Account:** Allows the user to see their account details as well as edit. Also contains system settings.
- **Logout:** Allows the user to log out from the system.

3.3.6. Withdraw Screens

user clicks on the Withdraw option, the following screen will show:

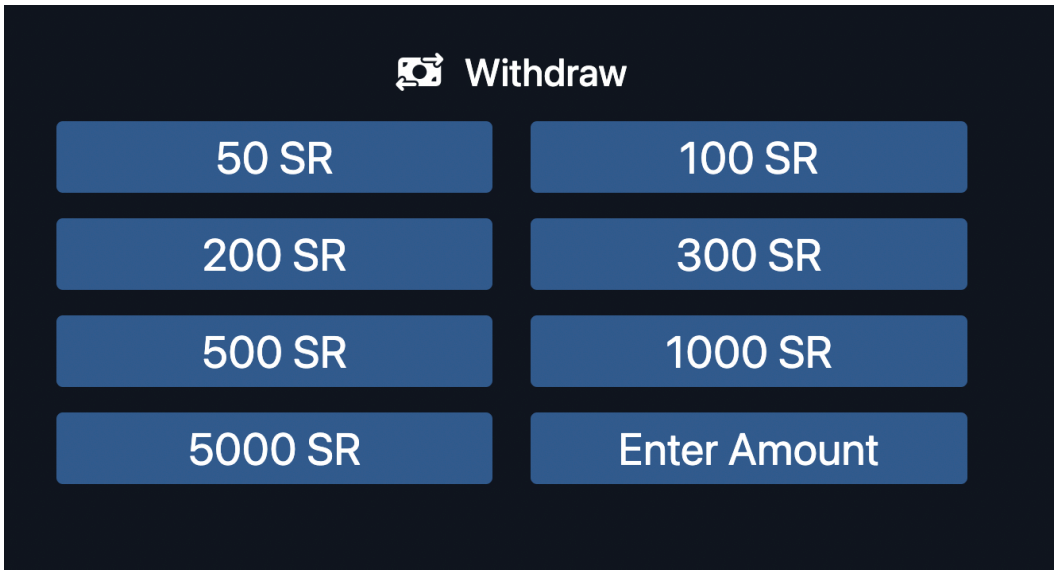

Figure 21.1: *Withdraw Screens*

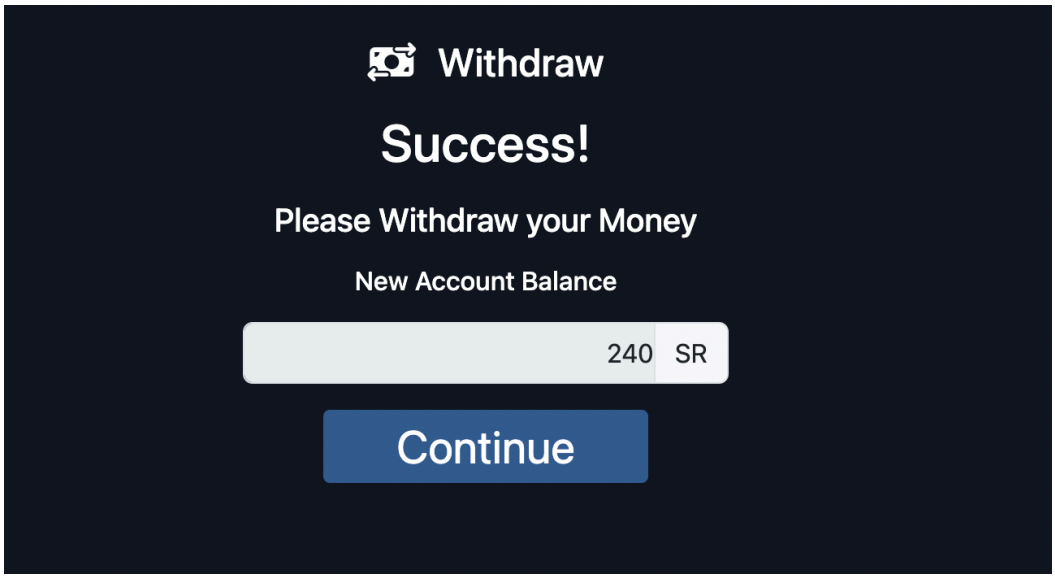

Figure 21.2: *Withdraw Screens*

Here the user is allowed to withdraw however much money they would like to. There are seven preset amounts, as well as a custom amount, which takes them to the top-right screen:

- 50 SR
- 100 SR
- 200 SR
- 300 SR
- 500 SR
- 1000 SR
- 5000 SR

After the user has selected the amount to withdraw, the system will show a loading screen while the transaction commences. After a successful transaction, the money will be dispensed for the user to pick up, and the system will show the user's new balance.

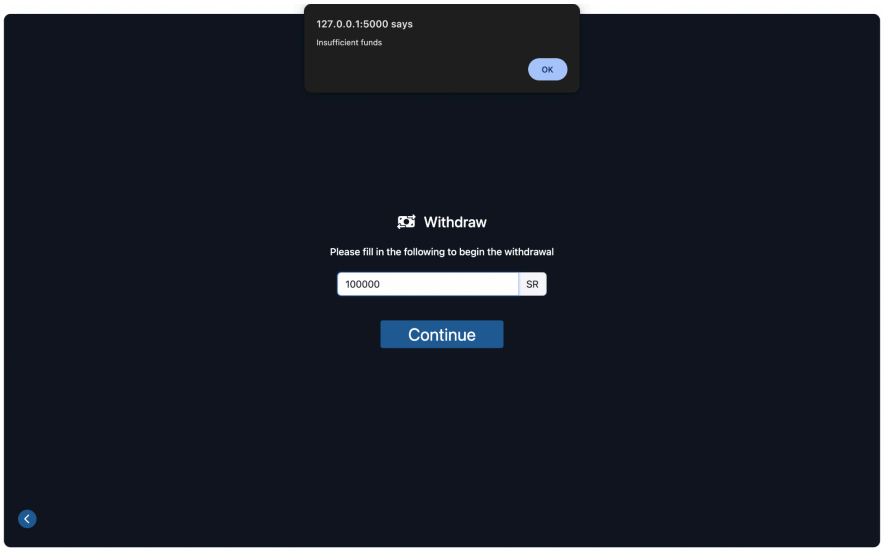

Figure 21.3: *Withdraw Screens - Insufficient Funds Error*

3.3.7. Deposit Screens

if the user clicks on the Deposit option; the following screen will show:

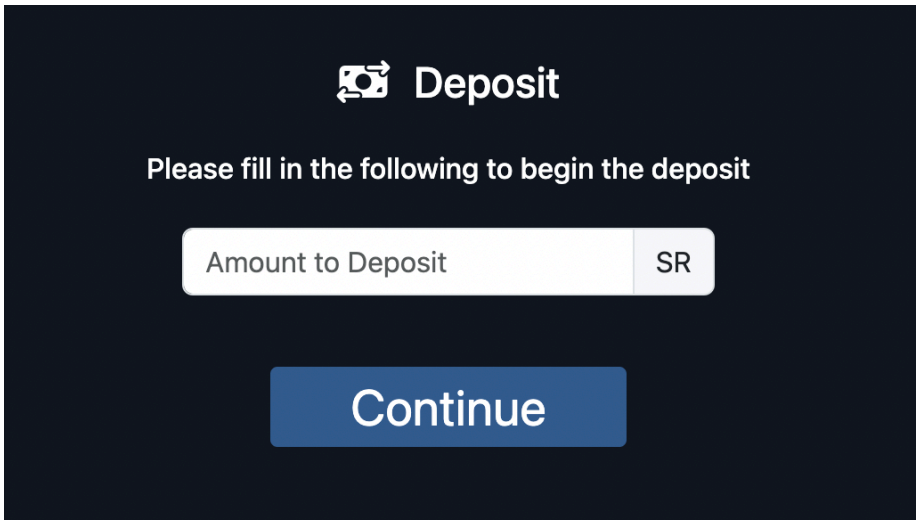

Figure 22.1: *Deposit Screens*

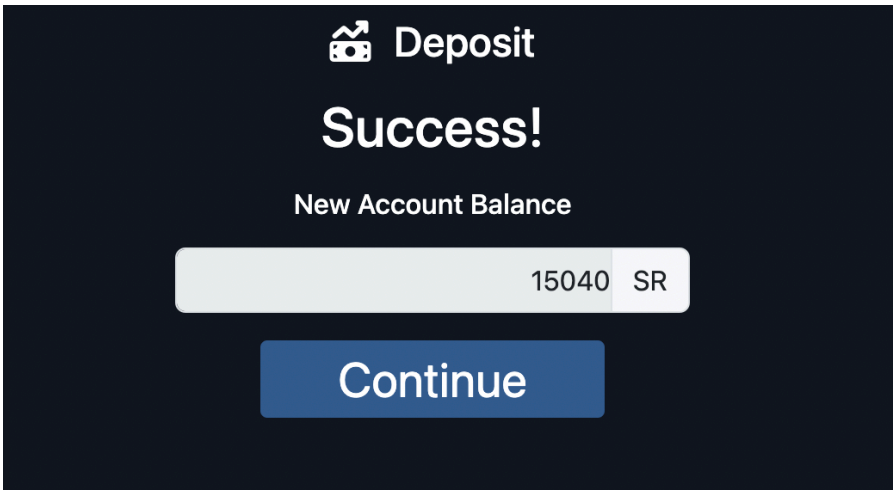

Figure 22.2: *Deposit Screens*

The user will directly slot in the amount of money they would like to deposit into the slot area, after the system recognizes this, the money will be deposited into their account, and their new

balance will reflect this change.

3.3.8. Transfer Screens

If the user clicks on the Transfer option, the following screen will show:

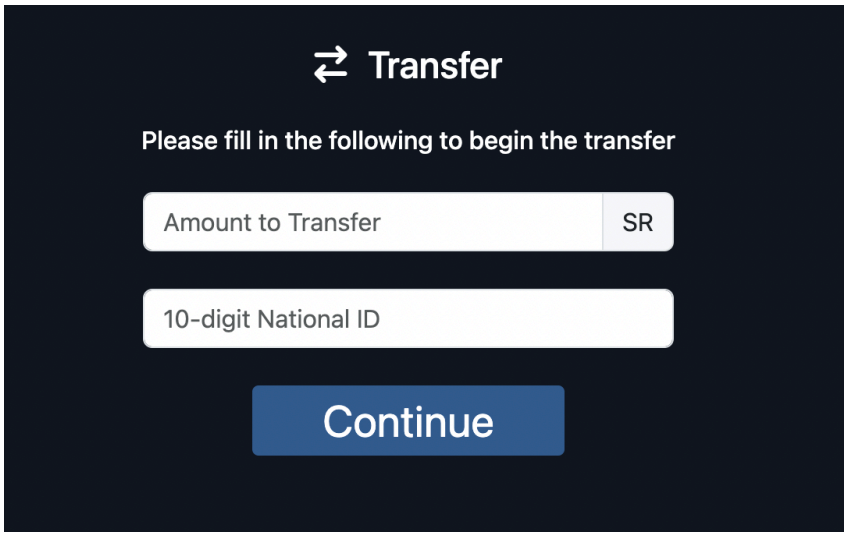

Figure 22.1: *Transfer Screens*

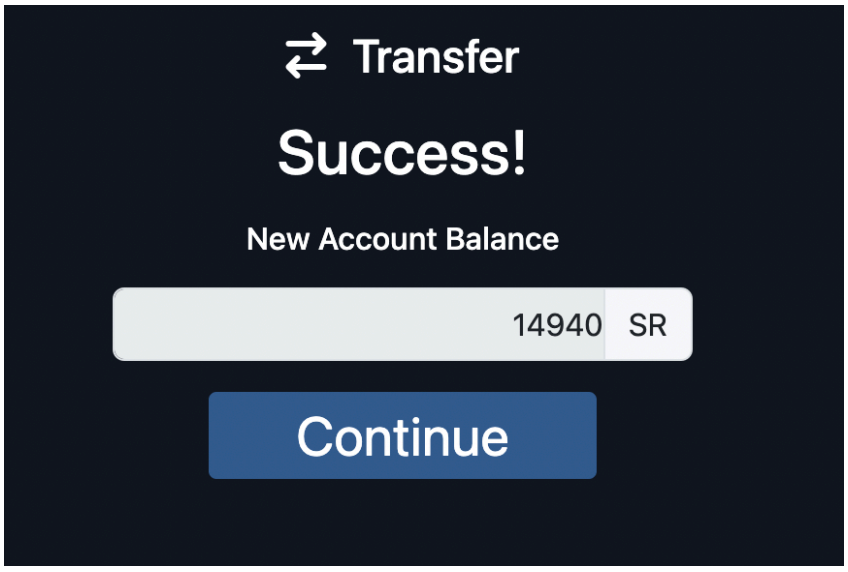

Figure 22.2: *Transfer Screens*

The user will be prompted to input the amount of money to transfer, as well as the 15-digit account number of the transferee.

3.3.9. Statement Screens

if the user clicks on the Statement option; the following screen will show:

Figure 23.1: *Statement Screens*

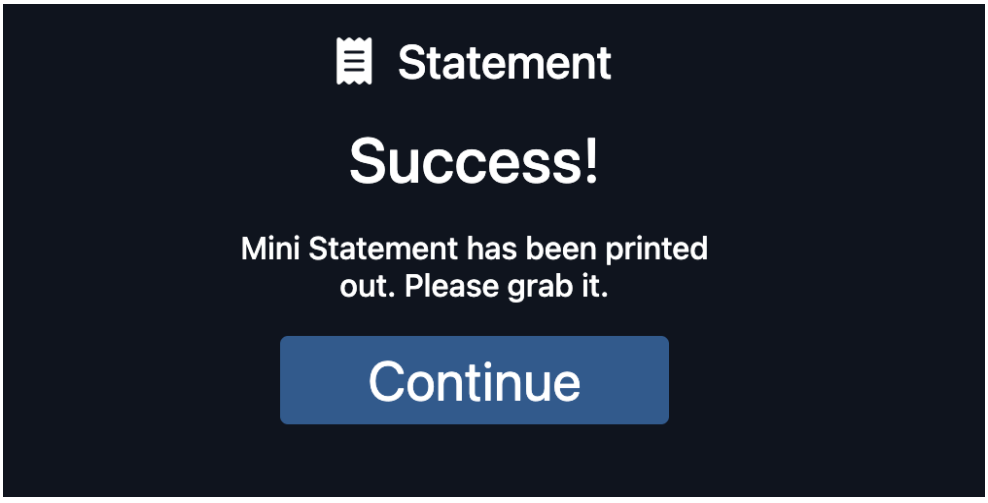

Figure 23.2: *Statement Screens*

Users will download a Mini Statement with their transactions from the previous 30 days after

selecting the "Continue" button.

3.3.10. Balance

If the user clicks on the Balance option, the following screen will show:

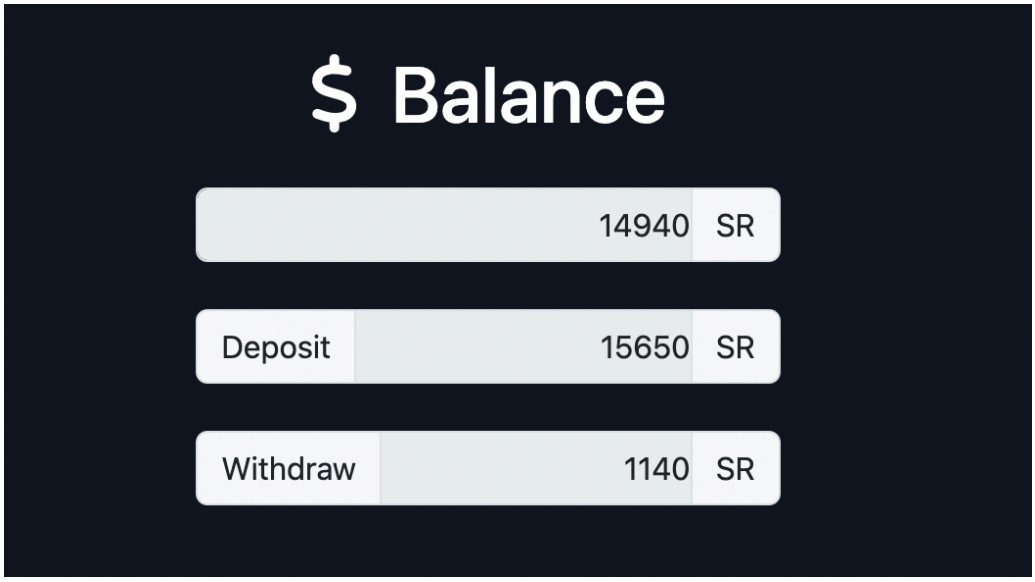

Figure 24: *Balance Screens*

Here the user can see the balance they have in their account, as well as the last 2 transactions that lead to this balance.

3.3.11. Account

user clicks on the Statement option; the following screen will show:

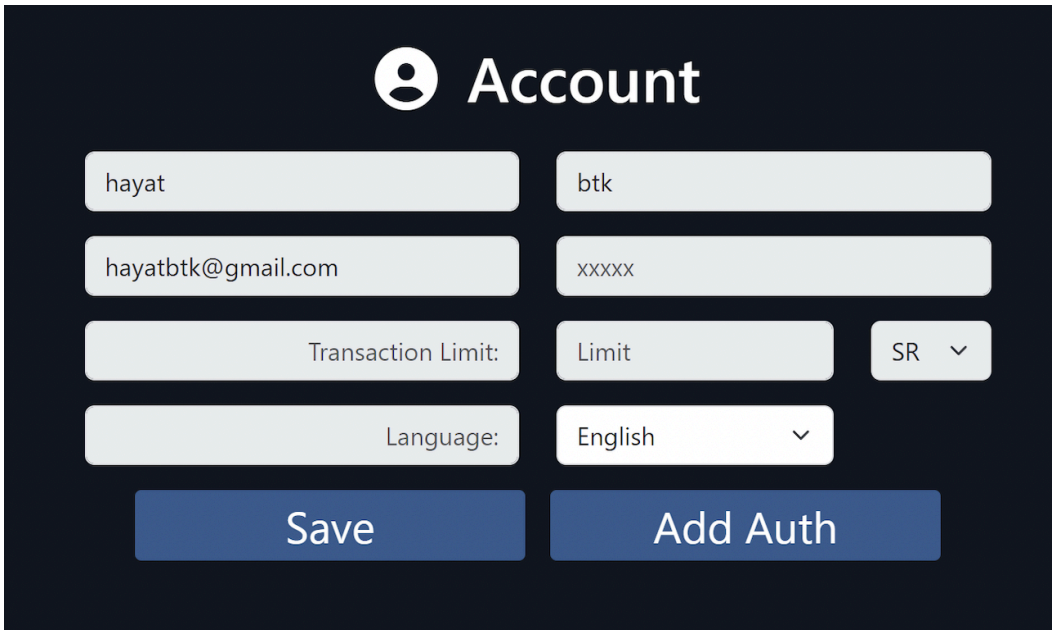

Figure 25: *Account Screens*

in this page the user can view their first name, last name, email address, and transaction limit. The Language is also changeable using a drop-down menu.

3.4. Database Design

AuthenticationMethod Table

- id (primary Key)
- type
- user_id
- hashed_data

ResetPasswordCode Table

- id (primary Key)
- user_id
- code

Transaction Table

- id (primary Key)
- type
- amount
- date
- user_id
- recipient_id
- recipient

User Table

- id (primary Key)
- first_name
- last_name
- email
- national_id
- password_hash
- balance
- auth_methods
- transactions

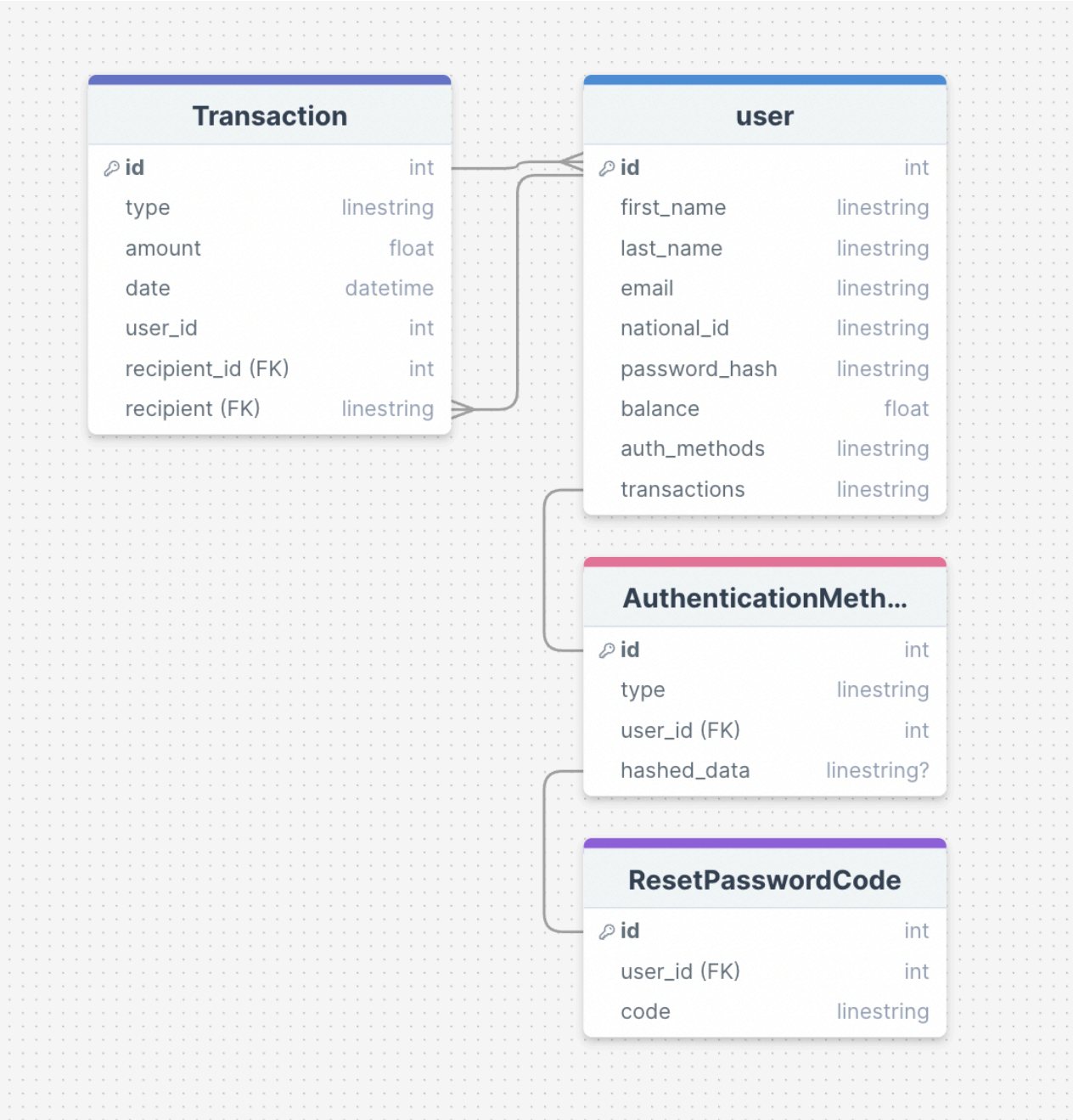

Figure 26: *Database Model*

4. Implementation

4.1. Face ID Registration

```
<script>
            // reference to the current media stream
            var mediaStream = null;

            // Prefer camera resolution nearest to 1280x720.
            var constraints = {
                audio: false,
                video: {
                    width: { ideal: 640 },
                    height: { ideal: 480 },
                    facingMode: "environment"
                }
            };

            async function getMediaStream(constraints) {
                try {
                    mediaStream = await
navigator.mediaDevices.getUserMedia(constraints);
                    let video = document.getElementById('cam');
                    video.srcObject = mediaStream;
                    video.onloadedmetadata = (event) => {
                        video.play();
                    };
                } catch (err) {
                    console.error(err.message);
                }
            };

            async function switchCamera(cameraMode) {
                try {
                    // stop the current video stream
                    if (mediaStream != null && mediaStream.active) {
                        var tracks = mediaStream.getVideoTracks();
                        tracks.forEach(track => {
                            track.stop();
                        })
                    }
                    // set the video source to null
                    document.getElementById('cam').srcObject = null;

                    // change "facingMode"
                    constraints.video.facingMode = cameraMode;

                    // get new media stream
                    await getMediaStream(constraints);
                } catch (err) {
                    console.error(err.message);
                    alert(err.message);
                }
            }
```

```
            function takePicture() {
                let canvas = document.getElementById('canvas');
                let video = document.getElementById('cam');
                let photo = document.getElementById('photo');
                let context = canvas.getContext('2d');

                const height = video.videoHeight;
                const width = video.videoWidth;

                if (width && height) {
                    canvas.width = width;
                    canvas.height = height;
                    context.drawImage(video, 0, 0, width, height);
                    var data = canvas.toDataURL('image/png');
                    photo.setAttribute('src', data);

                    document.getElementById("loadingOverlay").style.display =
"flex";
                    $.ajax({
                        url: "{{ url_for('auth.register_face') }}",
                        type: 'POST',
                        data: JSON.stringify({ email: registeredEmail, imgData:
data }),
                        contentType: "application/json",
                        success: function (response) {
                            console.log(response);

                            const nextStepId = "SuccessfulRegister";
                            const steps = document.querySelectorAll(".step");

                            steps.forEach(function (step) {
                                step.classList.remove("active");
                            });

document.getElementById(nextStepId).classList.add("active");

document.getElementById("loadingOverlay").style.display = "none";

                        },
                        error: function (jqXHR, textStatus, errorThrown) {
                            console.error("Error:", textStatus, errorThrown);

document.getElementById("loadingOverlay").style.display = "none";
                        }
                    });

                } else {
                    clearphoto();
                }
            }
```

```
        function clearPhoto() {
            let canvas = document.getElementById('canvas');
            let photo = document.getElementById('photo');
            let context = canvas.getContext('2d');

            context.fillStyle = "#AAA";
            context.fillRect(0, 0, canvas.width, canvas.height);

            var data = canvas.toDataURL('image/png');
            photo.setAttribute('src', data);
        }

        document.getElementById('loginFaceBtn').onclick = (event) => {
            switchCamera("user");
        }

        document.getElementById('snapBtn').onclick = (event) => {
            takePicture();
            event.preventDefault();
        }

        clearPhoto();
    </script>
```

4.2. Fingerprint Registration

We used the Digital Persona 4500 fingerprint reader.

```
 <script>
        var registeredEmail = null;
        let resultImg = document.getElementById('resultImg');

        function fromBase64Url(s) {
            return ((s.length % 4 === 2) ? s + "==" :
                (s.length % 4 === 3) ? s + "=" : s)
                .replace(/-/g, "+")
                .replace(/_/g, "/");
        }
        window.addEventListener('DOMContentLoaded', function () {
            // Check if the device has been connected
            let reader = new fpController({
                debug: true,
                version: 1
            });

            let trigger = document.getElementById('startReading');
            let result = document.getElementById('result');

            if (trigger)
                trigger.addEventListener('click', (e) => {
                    reader.startReading();
                });
```

```
            // Adding event listener to capture onAcquisitionStarted
    event

            reader.reader.on("SamplesAcquired", (event) => {
                console.log('Fingerprint sample acquired');

                console.log(event);
                var samples = event.samples[0];
                console.log(samples);

                sendSamplesToServer(samples);
            });


        });
        function sendSamplesToServer(samples) {
      var base64Str = "" + fromBase64Url(samples);
          let resultImg = document.getElementById('resultImg');
              console.log(base64Str);

            resultImg.src = base64Str;

            console.log(registeredEmail);
           document.getElementById("loadingOverlay").style.display =
    "flex";

            $.ajax({
                type: "POST",
                url: "{{ url_for('auth.register_finger') }}",
                data: JSON.stringify({ email: registeredEmail, img:
    base64Str }),
                contentType: "application/json",
                success: function (response) {
                    console.log("Success", response);

           const nextStepId = "SuccessfulRegister";
        const steps = document.querySelectorAll(".step");

                steps.forEach(function (step) {
                        step.classList.remove("active");
                    });
      document.getElementById(nextStepId).classList.add("active");

    document.getElementById("loadingOverlay").style.display = "none";
                },
      error: function (xhr, status, error) {
            console.error("failed", xhr, status, error);
              alert("Fingerprint registeration failed");

    document.getElementById("loadingOverlay").style.display = "none";
                }
            });
        }
</script>
```

4.3. PIN Registration

```
<script>
        $(document).ready(function () {
            $('.tick-btn').click(async function () {
                var pin = $('#pinInput').val();
                var userId = 1;
                try {
                 document.getElementById("loadingOverlay").style.display =
"flex";
                    await new Promise((resolve, reject) => {
                        $.ajax({
                            type: "POST",
                            url: "{{ url_for('auth.register_pin') }}",
                            contentType: "application/json",
                            data: JSON.stringify({ pin: pin, user_id: userId,
email : registeredEmail }),
                            success: function (response) {
                                console.log(response.message);
                                resolve(response);
                            },
                 error: function (xhr, status, error) {
      console.error("Registration failed", xhr.responseText);
                                alert(JSON.parse(xhr.responseText).error);
                                window.location.reload();
                                reject(new Error("Registration failed"));
                            }
                        });
                    });
                  document.getElementById("loadingOverlay").style.display =
"none";
                    console.log("This code runs after a successful AJAX
call.");
                } catch (error) {
                    console.error("An error occurred:", error.message);
                }
            });

        });
    </script>
```

5. Conclusions and Future Work

To sum up, the creation of our biometric automated teller machine (ATM) represents a noteworthy advancement in banking technology, providing users with improved security, convenience, and accessibility. We have successfully addressed important issues with traditional ATM systems, like PIN-based authentication vulnerabilities and limited account management capabilities, by implementing facial and fingerprint recognition for authentication along with strong account management and transaction processing functionalities.

5.1. Future Work

- Improved Biometric Recognition: Iris recognition. Research advanced methods for improved precision and speed.
-
- Enhanced Transaction Security: To further improve transaction security, put in place extra safeguards including digital signatures and real-time fraud detection.
- Expanded Accessibility Features: Add more accessibility features, like voice-activated commands and haptic feedback, to support users with a range of needs.

References

Babatunde, I.G. (2013). A Fingerprint-based Authentication Framework for ATM Machines. *Journal of Computer Engineering & Information Technology*, 02(03). doi:https://doi.org/10.4172/2324-9307.1000112.

GDPR (2013). *General Data Protection Regulation (GDPR)* . [online] General Data Protection Regulation (GDPR). Available at: https://gdpr-info.eu.

ISO (2016). *ISO/IEC 24779-1:2016*. [online] ISO. Available at: https://www.iso.org/standard/57379.html [Accessed 30 Apr. 2024].

ISO (2017). *ISO/IEC 19794-15:2017*. [online] ISO. Available at: https://www.iso.org/standard/63865.html [Accessed 30 Apr. 2024].

Lourde, R.Mary. and Khosla, D. (2010). Fingerprint Identification in Biometric SecuritySystems. *International Journal of Computer and Electrical Engineering*, pp.852–855. doi:https://doi.org/10.7763/ijcee.2010.v2.239.

Obed-Emeribe, C. (2013). Multimodal Biometric Technology System Framework and E-Commerce in Emerging Markets. *International Journal of Advanced Computer Science and Applications*, 4(7). doi:https://doi.org/10.14569/ijacsa.2013.040727.

Security Standard Council (2019). *Official PCI Security Standards Council Site - Verify PCI Compliance, Download Data Security and Credit Card Security Standards*. [online] Pcisecuritystandards.org. Available at: https://www.pcisecuritystandards.org.

Sun, Y., Ren, Z. and Zheng, W. (2022). Research on Face Recognition Algorithm Based on Image Processing. *Computational Intelligence and Neuroscience*, [online] 2022, pp.1–11. doi:https://doi.org/10.1155/2022/9224203.

W3C (2018). *Web Content Accessibility Guidelines (WCAG) Overview*. [online] Web Accessibility Initiative (WAI). Available at: https://www.w3.org/WAI/standards-guidelines/wcag/.