Software Requirements Specification

for

Version 1.0 approved

Prepared by <author>

<organization>

<date created>

Table of Contents

Revision History

Name	Date	Reason For Changes	Version

1. Introduction

1.1 Purpose

This innovative digital banking and payment application are designed to address the evolving needs of users in the digital financial ecosystem. The primary purposes of the application are:

- **Redefined User Interaction:** The application aims to revolutionize the way users engage with their bank accounts and conduct financial transactions. It introduces a user-friendly interface and cutting-edge features to enhance the overall digital banking experience.
- **Enhanced Security Measures:** By incorporating facial authentication and biometric data, the application prioritizes security. These advanced security layers not only protect user accounts but also streamline the authentication process, ensuring a secure and frictionless login experience.
- **Streamlined Transactions:** The app provides users with the flexibility to choose their primary banks within the platform, streamlining transactions and consolidating financial relationships. Users can access account information, view transaction history, and initiate payments directly from their designated primary banks.

1.2 Document Conventions

This document follows standard conventions for documenting software requirements. Priorities for higher-level requirements are assumed to be inherited by detailed requirements. The document uses standard font styles and formatting for clarity.

1.3 Intended Audience and Reading Suggestions

This document is intended for various stakeholders involved in the development process, including developers, project managers, marketing staff, users, testers, and documentation writers. Developers should focus on the technical details, while project managers can derive project scope and timelines. Users will find information on the app's features and benefits. We recommend starting with the overview sections and proceeding to more detailed sections as needed.

1.4 Project Scope

The scope of this project encompasses various aspects of digital banking and secure payment transactions. Key elements include:

Mobile Number Integration:

Users can seamlessly link their mobile numbers to their bank accounts during registration, eliminating the need for traditional login credentials.

Facial Authentication:

In addition to mobile number authentication, the app empowers users with facial data for an added layer of security. This feature not only safeguards user accounts but also ensures a swift and frictionless login experience.

Primary Bank Designation:

Users have the freedom to designate their primary banks within the app. This consolidation of financial relationships adds convenience and efficiency to the user experience.

In-Store Purchases:

The application revolutionizes in-store purchases by allowing users to make payments effortlessly using their registered biometrics. This contactless and secure payment method enhances user convenience and promotes financial inclusivity by eliminating the need for physical payment instruments.

Transaction History:

The app facilitates a comprehensive transaction history feature, allowing users to track and review their financial activities over time. This includes details on completed transactions, pending transactions, and other relevant information.

This project's overall scope is to create a digital banking and payment application that not only meets the basic needs of users but also anticipates and addresses emerging trends in the digital financial landscape. It aims to provide a secure, user-friendly, and efficient platform for individuals to manage their finances seamlessly.

1.5 References

[1] D. Kumar and Y. Ryu, "A Brief Introduction of Biometrics and Fingerprint Payment Technology," 2008 Second International Conference on Future Generation Communication and Networking Symposia, Hinan, China, 2008, pp. 185-192, doi: 10.1109/FGCNS.2008.11.

[2] https://chantrapornchai.medium.com/face-analysis-using-ml-kit-and-tensorflow-lite-b1945d48094a

[3] https://docs.python.org/3/library/sqlite3.html

[4] https://wallet.polygon.technology

[5] N. ChitraKiran, B. Teja, S. Suresh, B. Krishna, S. M. Akarsh and J. Yomas, "A biometric based payment system by using payee and payer module," 2017 2nd IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT), Bangalore, India, 2017, pp. 2252-2256, doi: 10.1109/RTEICT.2017.8257001.

[6] https://medium.com/geekculture/crypto-wallet-app-using-flutter-and-solidity-9f67b0d0819f

[7] B. T. Dommaraju, D. S. Kondaveeti, S. Katta, V. N. Sai Akarsh Devanaboina and N. L. Sowjanya Cherukupalli, "Fingerprint Sensor based Biometric Payment Cards," 2023 7th International Conference on Computing Methodologies and Communication (ICCMC), Erode, India, 2023, pp. 388-392, doi: 10.1109/ICCMC56507.2023.10083680.

2. Overall Description

2.1 Product Perspective

The innovative digital banking and payment application exist as a standalone product designed to redefine user interactions with bank accounts and payments. It is not a replacement for existing systems but rather a new, self-contained solution. The application operates in the context of the evolving digital financial ecosystem, introducing groundbreaking features to enhance user experiences. While it is a standalone product, it may integrate with existing banking systems through secure interfaces for streamlined transactions.

2.2 Product Features

High-Level Summary:

The major features of the application include:

Facial Authentication:
Users can access their bank accounts using facial authentication, ensuring security and a seamless login experience.

Mobile Number Integration:
Seamless linking of mobile numbers to bank accounts during registration, eliminating the need for traditional login credentials.

Primary Bank Designation:
Users have the flexibility to designate their primary banks within the app for streamlined transactions.

In-Store Purchases:
The app facilitates contactless payments using registered biometrics for in-store purchases.

Comprehensive Transaction History:
Users can track and review their financial activities, including completed and pending transactions

2.3 User Classes and Characteristics

2.3.1 Regular Users

2.3.1.1 Characteristics

Everyday Individuals:
Regular users are everyday consumers utilizing the application for routine personal banking needs.

Engagement in Basic Banking Activities:
Regular users engage in fundamental banking tasks, such as checking balances, transferring funds, and paying bills, through the application.

Value Convenience:
Convenience is paramount for regular users, emphasizing the need for a user-friendly interface and streamlined transactions.

2.3.1.2 Roles and Responsibilities

Basic User:
Responsibilities:
- Engage in day-to-day banking activities.
- Perform transactions such as fund transfers and bill payments.
- Regularly monitor account balances.

Access Level:
- Standard access with the ability to perform essential banking functions.

2.3.2 Merchants

2.3.2.1 Characteristics

Business Owners and Commercial Transactions:
Merchants, representing business owners and individuals involved in commercial activities, use the application for managing financial transactions related to their business operations.
In-Store Payments:
Merchants leverage the application for receiving secure in-store payments, facilitated through biometrics.
Appreciation for Security and Simplification:
Security is a top priority for merchants, who value features like biometric authentication. They appreciate functionalities that simplify financial processes.
Efficient Financial Transactions:
Merchants benefit from features streamlining financial transactions, ensuring efficiency in handling payments and managing business finances.

2.3.2.2 Roles and Responsibilities

Merchant User:
Responsibilities:
- Conduct commercial transactions related to business operations.

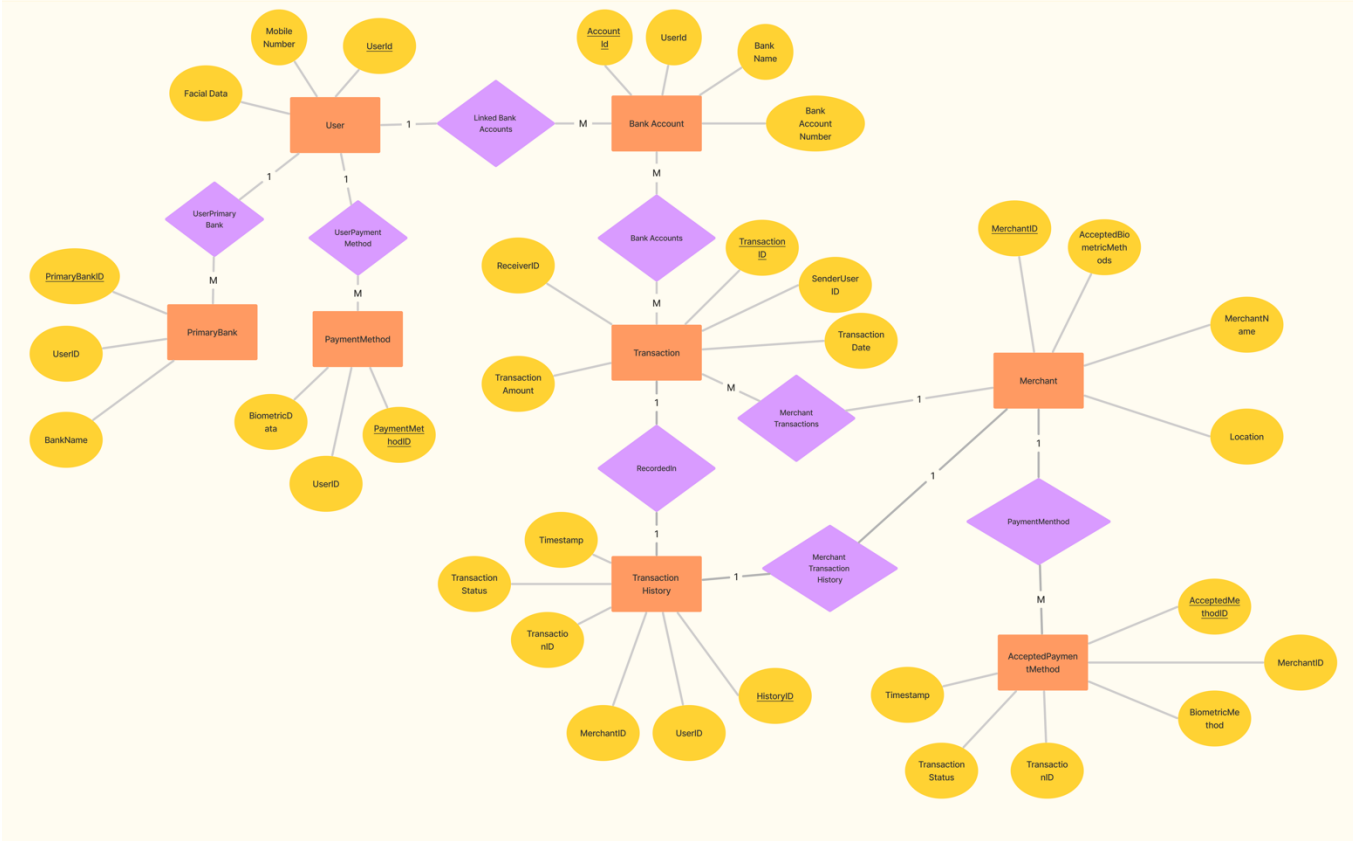
- Receive in-store payments securely through biometrics.
- Utilize features that simplify and secure financial transactions for their business.

Access Level:

- Enhanced access, allowing for business-specific functionalities and transaction management.

In this section, the document introduces roles and responsibilities associated with each user class, along with their corresponding access levels. These roles and access levels serve as a foundation for defining more detailed permissions, functionalities, and security measures in subsequent sections of the SRS documentation.

2.3.2 Entity Relation Diagram



2.4 Operating Environment

Environment Description:

Hardware Platform:
Compatible with mobile devices (iOS and Android).
Operating System:
Supports iOS version 15 and above, Android version 10 and above.
Software Components:
Interfaces with banking systems securely.

2.5 Design and Implementation Constraints

2.5.1 Technology and Tool Selection:

Description:
The project may be constrained by the use of specific technologies, tools, and databases dictated by organizational standards or existing infrastructure.
Impact:
Developers must align with predefined technologies, limiting flexibility in choosing alternative solutions.

2.5.2 Parallel Operations:

Description:
Parallel operations, such as simultaneous development and deployment, might be constrained by organizational policies or project timelines.
Impact:
Coordination and synchronization challenges may arise, affecting the efficiency of parallel processes.

2.5.3 Language Requirements:

Description:
The project may be bound by language requirements, necessitating multilingual support based on user demographics.
Impact:
Design and implementation must accommodate language-specific nuances, potentially influencing user interface and content.

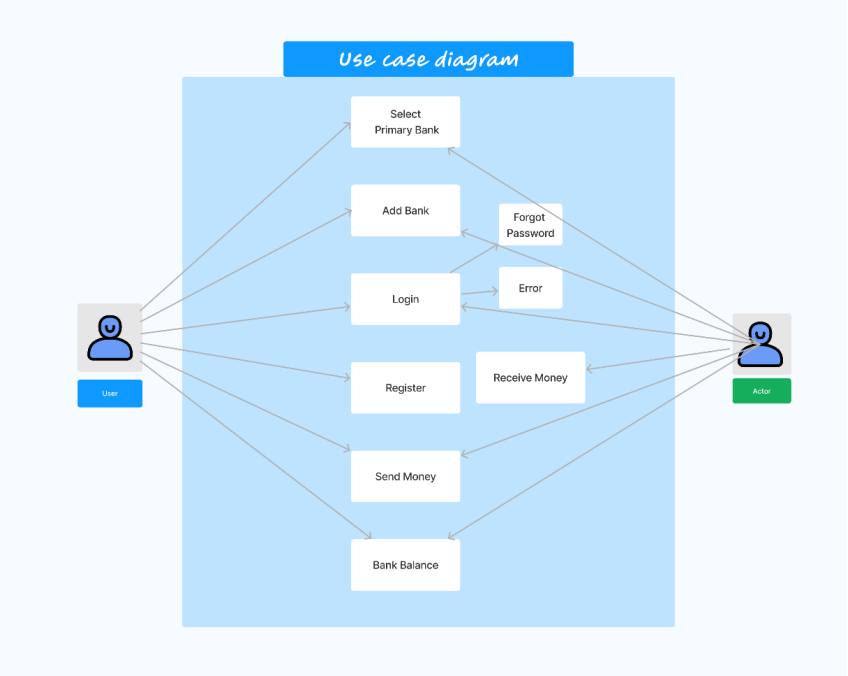
2.5.4 Development Environment:

Description:
Constraints related to the development environment, such as IDE versions or operating systems, may be in place.
Impact:
Developers must work within the specified environment, affecting tool compatibility and development workflows.

2.5.5 Design Conventions and Programming Standards:

Description:
Adherence to established design conventions and programming standards set by the organization or industry may impose constraints.
Impact:
Developers must follow specified coding practices, ensuring consistency and maintainability of the codebase.

3. System Features



3.1 User Registration

- Description and Priority
- Facilitates a robust and secure account creation process through the integration of facial biometrics.
- Given the foundational role in establishing and verifying user identities, this feature is deemed of high priority.
- Stimulus/Response Sequences
  - User Accesses Registration Page:
    - The system responds by presenting an intuitively designed interface, guiding users through the entry of personal information and capturing facial biometrics.
  - Facial Biometrics Registration:
    - Users actively engage in capturing facial biometrics during the registration process, and the system ensures the secure storage of this sensitive data.
- Functional Requirements
  - Intuitive Registration Page:
    - The system is mandated to provide a user-friendly and intuitive registration interface to enhance the overall user experience.
  - Facial Biometrics Registration:

        - Users should have the capability to register facial biometrics seamlessly as part of the account creation process, emphasizing the importance of robust identity verification.
    - Error Handling:
        - The system should implement robust error handling mechanisms, providing clear feedback to users in case of data entry errors or biometric capture issues.

REQ-1: Provide an intuitive registration page.
REQ-2: Allow users to register facial biometrics during account creation.

3.2 User Authentication with Facial Recognition and PIN

- Description and Priority
    - Elevates the authentication process by combining facial recognition technology with an optional Personal Identification Number (PIN).
    - Given the critical role of authentication in securing user accounts, this feature is accorded a high priority.
- Stimulus/Response Sequences
    - Facial Recognition and PIN Login:
        - Users opting for facial recognition trigger the system to activate this feature and, optionally, prompt for a PIN entry for additional security.
    - PIN Verification:
        - Users entering their set PIN experience the system's verification process to ensure a multi-layered authentication mechanism.
- Functional Requirements
    - Utilize Facial Recognition for Login:
        - The system must effectively employ facial recognition technology as the primary means of user login for enhanced security.
    - Optional PIN Authentication:
        - Users should have the flexibility to set an optional PIN, offering an additional layer of authentication for those who prefer it.
    - Error Handling:
        - The system should gracefully handle errors, providing clear feedback in case of unsuccessful authentication attempts or PIN entry errors.

REQ-3: Utilize facial recognition for login.
REQ-4: Allow users to set an optional PIN for authentication.

3.3 Fund Transfer

- Description and Priority
    - Empowers users with a seamless and efficient fund transfer mechanism between linked accounts, addressing a crucial aspect of financial management.
    - Given its significance in facilitating financial transactions, this feature holds a high priority.
- Stimulus/Response Sequences
    - Initiating Fund Transfer:
        - Users initiating a fund transfer trigger the system to validate and process the transaction details promptly.
    - Notification of Fund Transfer:
        - Following a successful fund transfer, the system promptly sends confirmation notifications to both the user and, if applicable, the recipient.
- Functional Requirements
    - Maintain Comprehensive Transaction History:
        - The system must robustly maintain and organize a comprehensive transaction history, offering users insights into their financial activities.
    - Link Multiple Banks and Select Primary Bank:
        - Users should be able to link multiple banks to their account and designate a primary bank for transactions, ensuring flexibility in managing finances.
    - Error Handling:
        - The system should handle errors gracefully, providing clear feedback in case of fund transfer failures or transaction processing issues.

REQ-5: Maintain comprehensive transaction history.
REQ-6: Allow users to link multiple banks.
REQ-7: Enable users to select a primary bank.

3.4 Bank Balance Inquiry

- Description and Priority
  - Facilitates users in promptly checking the balances of their linked bank accounts, offering real-time financial information.
  - Given the constant need for users to stay informed about their financial status, this feature is accorded a high priority.
- Stimulus/Response Sequences
  - Accessing Bank Balance:
    - Users selecting the "Check Balance" option trigger the system to swiftly retrieve and display the current balances of their linked bank accounts.
- Functional Requirements
  - Fetch and Display Current Balances:
    - The system is mandated to efficiently fetch and display the most up-to-date balances of linked bank accounts, ensuring users have immediate access to their financial information.
  - Error Handling:
    - The system should handle errors effectively, providing clear feedback in case of balance inquiry failures or data retrieval issues.

REQ-8: Fetch and display current balances of linked bank accounts.

3.5 In-Store Payments

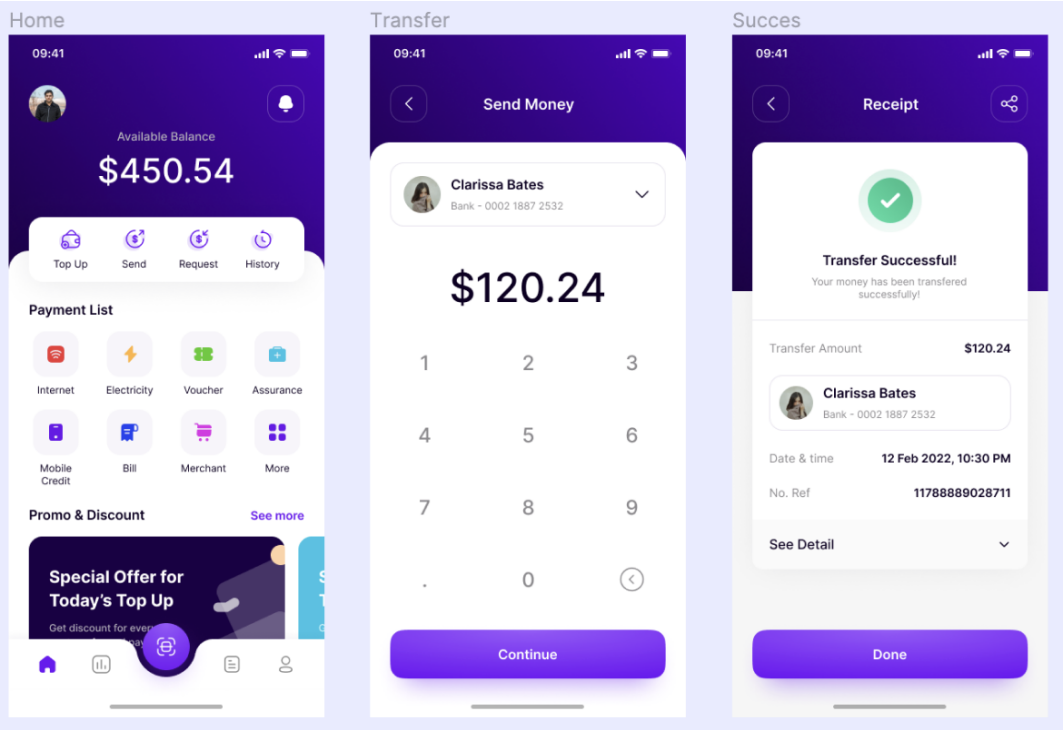
- Description and Priority
  - Revolutionizes traditional in-store purchases by enabling users to make secure and contactless payments using their registered facial biometrics, eliminating the need for physical payment instruments.
  - High priority is attributed to the transformative nature of the contactless payment experience, enhancing convenience and security.
- Stimulus/Response Sequences
  - Initiating In-Store Payment:
    - Users, upon approaching the payment counter at a physical store, trigger the system to prompt them for authentication through registered facial biometrics.
  - Confirmation of Payment:
    - Following successful authentication, the system processes the payment and promptly sends a payment confirmation to the user's

device. Simultaneously, the store receives confirmation of the completed payment.

- Functional Requirements
  - Facial Biometric Authentication:
    - The system is required to utilize advanced facial recognition technology for robust user authentication during in-store payments, ensuring a secure transaction process.
  - Contactless Payment Processing:
    - The system must process payments seamlessly without the need for physical cash or external devices, redefining the in-store payment experience for users.
  - Error Handling:
    - The system should incorporate robust error handling mechanisms, providing clear feedback in case of authentication failures or payment processing errors.

4. External Interface Requirements

4.1 User Interfaces



4.1.1 User Registration Interface:
Logical Characteristics:
- Intuitive Design: The interface guides users through the account creation process seamlessly.
- Facial Biometrics Capture: Allows users to capture facial biometrics securely during registration.
- Error Feedback: Provides clear feedback in case of data entry errors or biometric capture issues.

4.1.2 User Authentication Interface:
Logical Characteristics:
- Facial Recognition Activation: Activates facial recognition for users opting for this login method.
- Optional PIN Entry: Prompts users with an optional PIN to enhance authentication.
- Error Handling: Gracefully handles authentication errors, providing feedback to users.

4.1.3 Fund Transfer Interface:
Logical Characteristics:
- Transaction Validation: Validates transaction details before processing fund transfers.
- Notification: Sends prompt notifications to the user and recipient confirming successful fund transfers.
- Error Handling: Provides clear feedback in case of fund transfer failures or transaction processing issues.

4.1.4 Bank Balance Inquiry Interface:
Logical Characteristics:
- Real-Time Balance Display: Efficiently fetches and displays up-to-date balances of linked bank accounts.
- Error Handling: Handles errors effectively, providing clear feedback in case of balance inquiry issues.

4.1.5 In-Store Payments Interface:
Logical Characteristics:
- Facial Biometric Authentication: Utilizes advanced facial recognition for user authentication during in-store payments.
- Contactless Payment Processing: Processes payments seamlessly without the need for physical payment instruments.
- Error Handling: Incorporates robust error handling mechanisms, providing clear feedback in case of authentication or payment processing errors.

4.2 Hardware Interfaces

Logical and Physical Characteristics:

Hardware Platform: Compatible with mobile devices (iOS and Android).

Operating System: Supports iOS version 15 and above, Android version 10 and above.

Software Components: Interfaces securely with banking systems.

4.3 Software Interfaces

Connections and Data Exchange:

Database Interface: Interacts with SQLite database (referenced in [3]) for secure data storage.
Biometric Technology: Utilizes facial recognition technology (referenced in [2]) for user authentication.
Payment Platform Integration: Interfaces with the Polygon wallet platform ([4]) for secure and efficient payment processing.
Programming Language Interface: Developed using Python (referenced in [3]) for implementation.

4.4 Communications Interfaces

Communication Functions:

Protocols: Utilizes standard communication protocols for interactions with banking systems, possibly HTTPS or other secure protocols.
Notification Protocol: Sends notifications to users and recipients using standard messaging protocols.
External Data Sharing: Shares data securely with external platforms such as the Polygon wallet ([4]).
This outlines the logical and physical characteristics of the interfaces between the software product and various components, ensuring a comprehensive understanding of how the application interacts with users, hardware, software components, and external platforms.

5. Other Nonfunctional Requirements

5.1 Performance Requirements

Response Time:
The application should respond to user interactions within 2 seconds to ensure a seamless and responsive user experience.

Transaction Processing Time:
Fund transfers and in-store payments should be processed in real-time, completing within 5 seconds of initiation.

Scalability:
The system should be scalable to accommodate a user base growth of at least 20% per month without significant degradation in performance.

5.2 Safety Requirements

User Data Protection:
All user data, especially biometric information, must be securely stored and encrypted to prevent unauthorised access or data breaches.

Error Handling:

The system should provide clear error messages to users, avoiding confusing or misleading information that could lead to unintentional actions.

5.3 Security Requirements

User Authentication:
Facial recognition and optional PIN authentication must be robust to prevent unauthorised access to user accounts.

Data Encryption:
All communication between the application and external systems, especially banking systems, must be encrypted to ensure data security.

Compliance:
The application must comply with relevant data protection regulations and standards to safeguard user privacy.

5.4 Software Quality Attributes

Usability:
The application should be designed with a user-friendly interface, promoting ease of use for individuals with varying levels of technical expertise.

Reliability:
The system should be highly reliable, with minimal downtime and robust error recovery mechanisms.

Maintainability:
The codebase should be well-documented, and any updates or maintenance tasks should be easily manageable to ensure long-term sustainability.

6. Other Requirements

Database Requirements:
The application should utilize SQLite (referenced in [3]) for data storage, with regular backups to prevent data loss.

Internationalisation Requirements:
The application should support multiple languages to cater to a diverse user base.

Legal Compliance:
The development and operation of the application must comply with all relevant local and international laws and regulations, especially those related to financial transactions and data protection.

Appendix A: Glossary

Biometric Data:
Unique physiological or behavioral characteristics used for user authentication, such as facial features.

Encryption:
The process of converting data into a secure code to prevent unauthorized access.

Scalability:
The ability of a system to handle a growing amount of work, users, or transactions.

Appendix B: Analysis Models

- *(No specific analysis models provided in this section)*

Appendix C: Issues List

- *(No specific analysis models provided in this section)*