

**CS-2105**

**Software Engineering**

**Functional and Non-Functional Requirements**

#### **Department of Computer Science,**

**GC University Lahore**

**Submitted by: -**

**Iqra Khalique**

**Zarafshan Arjumand**

**Ayesha Yousaf**

**Section: CS-A2**

**Semester: 5th**

**Project’s Title:**

*Online Bank Management System*

**Project’s Proposal:**

This system would allow user to create an account and through that it can login. For security purposes, it requires your verified government documents. After all this, you can deposit and withdraw money. Moreover, you can send and receive money from other users as well. Further facilities include taking loan, funding any organization, donation, loan management and paying utility bills etc.

**Chosen Model:**

*XP Model*

**Functional and Non-Functional Requirements:**

**Functional Requirements:**

***User Registration:***

The account holders are able to register by setting a unique ID and password that meet the system-defined complexity (minimum 8 characters, including uppercase, lowercase, numbers and special characters). They will be required to provide official government-verified documents i.e. their CNIC and they will submit biometric data (fingerprints) via an integrated biometric device for authentication. If biometric fails 5 times in a row, then documents will be revalidated.

***User Login:***

The account holders can log in to their accounts using their ID and password. If login fails consecutively 5 times, the system will lock the account and notify the account holder via SMS and email. The account login can be unlocked after 4 hours or by answering specified security questions (i.e. What is the name of your mother) so the account holder can prove that they are the account owner. If the account holder for some reason can’t answer these questions then they will have to speak to customer support via email or phone call.

***User Profile***:

The account holders can view their profiles and may delete or alter its information provided after verification, the system will remove/alter it from its database. Information like CNIC, biometric details would be in a secure place (a separate page/interface) and would be shown after entering the 4-digit PIN. Pins as simple as 1111, 1234, etc. will not be valid pin options.

***Password/ID Recovery:***

If an account holder forgets their password or ID, the system will perform the following steps:

* The system will send an OTP (One-Time Password) to the account holder's registered contact i.e. via SMS. The OTP will be valid for 5 minutes.
* The application will auto-read with an option appearing to allow auto-reading the OTP from the account holder’s SMS. If the account holder does not allow auto-reading, and the account holder gets the OTP wrong consecutively 5 times, the account will be locked. The account unlocking process will be the same as mentioned in the *User Login* section.
* Upon successful OTP verification, the account holder can reset their password.

If they don’t have access to the phone number and email they referred to set up their account, they will have the option to speak to customer support using another phone number that isn’t connected to the account.

***User Authentication and Security:***

Account holder authentication and security can be managed by implementing two-factor authentication (2FA) for secure access on email or phone numbers. A password recovery mechanism can also be implemented by phone number verification. Account holders can turn off two-factor authentication but it is not recommended as it may weaken the security of the system. The system will use SMS for two-factor authentication.

***Account Management:***

The account holders will be able to create, view, update and delete their bank account information. Account holders that have pending loans and transactions cannot delete/alter their account.

***Transaction Management:***

The account holders can deposit and withdraw money from their accounts, transfer money to other account holders within the system, and receive money from other accounts. These features will be present on the main dashboard. To elaborate:

* **Deposit:** The option to deposit money into the account (with real-time updates to the balance). The maximum threshold for deposit is Rs. 900,000 per month.
* **Withdraw:** The option to withdraw money, ensuring the account balance does not drop below the minimum threshold. Minimum threshold is Rs. 500.
* **Money Transfer:** There will be an option for the account holders to send money to other registered account holders using their unique account IDs. They can receive money from other registered account holders, with instant balance updates.

Transactions will be instantaneous but on occasions of high traffic, transactions may take up to a minute.

***Loan Management:***

It is possible for account holders to apply for loans by submitting the required documents (i.e. salary slip or custodian’s salary slip). There will be a system for loan application approval or rejection. The Bank manager will accept or reject the loan application in 15 days and notify the account holder. All loan repayments will be tracked and interest (if any) will be calculated. There will be a proper process for loans which will include the steps:

* **Loan Application:** The account holders can apply for loans.
* **Eligibility Check**: Loans will only be granted to account holders who:
  + Provide proof of solid income (e.g., salary slips, tax records).
  + Meet the system-defined income threshold for loan eligibility.
* The system will automatically apply government policies on interest rates and repayment terms.

The loan application will be processed in 1-2 working days. The account holders can view and manage loan repayment schedules through their account. Eligibility criteria will be updated every 2 months and interest rates will be updated every month.

***Utility Bill Payment:***

The account holders can pay utility bills (electricity, water, internet, etc.) through their bank accounts. Electronic receipts can be sent or generated for successful payments. Bill payment will have the following steps in which the system will:

* Fetch bill details in real time from government APIs like Fetch API based on the account holder's account information and then notify the government API to update its database.
* Notify the account holder upon successful payment.
* Automatically mark the bill as paid and clear dues in both the system and government records.

Discrepancies between system and government records will be informed through the app and through email, the account holder will provide copies of the government records and updates will be made by the system or manually by an admin. In case the government APIs fail to fetch or update bill details, the system will notify the account holder and retry every 30 minutes for up to 24 hours before escalating the issue to manual resolution by an admin.

***Funding and Donation:***

The account holders can donate to approved registered organizations that are also government-verified. The account holders can fund specific projects or organizations that are listed within the system and approved by the system. The process will include:

* Verification details will be fetched from government APIs to ensure the organization’s legitimacy.
* The system’s admins will have a proper vetting process for the organization which will include proof of funding going to the place they have promised, reviews on online sites like Google or Yelp, speaking with partners of the organization.

Account holders can request particular organizations to be added to the system, if number of requests reach 25, the organization’s vetting process will begin and if it passes the vetting process, the organization will be added to the system.

***Notification:***

The account holders receive notifications for successful transactions (deposits, withdrawals, transfers, etc.), loan approvals or rejection, upcoming loan repayment dates, utility bill due dates and general account updates. Critical notifications, such as transaction failures and loan approvals, will be sent immediately, while general updates will be consolidated and sent once daily to reduce notification overload.

***Customer Support:***

A chat will be implemented within the customer support system that will either be an AI chatbot or an actual person. This is for account holder queries and complaints. The chat is available 24/7. If the AI chatbot cannot resolve the issue within 5 minutes or after 3 unsuccessful attempts, the query will be automatically escalated to human support, with a response time target of 30 minutes during peak hours.

***Monthly Statements:***

The account holders can view and download detailed monthly statements, which include:

* Deposits, withdrawals, and transfers.
* Loan details (approved loans, repayments, and outstanding balances).
* Utility bill payments and donations.
* Statements can be sent automatically via email or downloaded manually from the account holder dashboard.

The account holders will have the option to opt out of receiving monthly statement emails though this is not encouraged.

***Transaction History:***

The account holders can access a detailed history of all transactions, with filters for specific time periods or transaction types. The system will provide history between the selected period by the account holder.

***Transaction Limits and Alerts:***

The system will set custom daily or monthly transaction limits for deposits, withdrawals, and transfers for the account holder. Account holders will be notified when a transaction exceeds these limits (that transaction would be cancelled by the system) or nears the maximum balance threshold. The account holders will be able to set up a custom transaction limit for deposit and withdrawal, otherwise the monthly deposit limit will be Rs. 900,000. The withdrawal limit is equal to the amount of money in the account.

.

***Feedback:***

The account holders can submit feedback on app features, rate functionality, and provide comments. Feedback is stored for system improvement, and account holders are notified of any responses or actions. A dedicated section highlights common issues and their resolutions to enhance transparency.

**Non-Functional Requirements:**

***Performance:***

The system should be able to handle at least 10k concurrent account holders at once without any significant performance issues, this is essential for a smooth account holder experience even during peak times. The transaction processing should be completed within 3-10 seconds, it could be tighter based on the system’s complexity. The system will be stress-tested using tools like JMeter, to ensure it can handle 10,000 concurrent account holders. The system will have some specific target metrics:

* **Response time:** ≤ 3-10 seconds for critical operations like deposits, withdrawals, and transfers.
* **Throughput:** The system should process at least 1,000 transactions per minute without degradation.
* **Latency:** Ensure minimal latency (below 100ms) for database queries and API calls.

Transaction delays exceeding the specified limit of 10 seconds will trigger a fallback mechanism to reroute requests to a secondary server or queue system.

***Scalability:***

The system should be scalable to support increasing numbers of account holders and transactions as the banking system gains more account holders. We will need to plan for load balancing and cloud infrastructure to handle such a growth. Scalability will be managed by using cloud infrastructure, there will be proper load balancing and future scalability will also be considered (this includes database scalability). The system will initially be deployed on AWS cloud infrastructure with a capacity to scale up to 100,000 concurrent users, using auto-scaling and load-balancing mechanisms.

***Security:***

Implementing secure data encryption for sensitive account holder data and transactions which is important for a banking system. There will be regular security audits to identify and remove certain vulnerabilities. We will ensure compliance with data protection laws and financial regulations. We will use AES-256 for encrypting sensitive data (e.g. passwords, CNIC, biometric data), TLS 1.3 will be implemented for secure data transmission between the client and server. Encryption keys will be stored securely and managed. The system will adhere to PCI-DSS (for payment security), GDPR (for account holder data protection), and ISO 27001 (for information security management). Encryption keys will be rotated every 90 days, stored in a secure hardware security module (HSM), and subjected to quarterly internal security audits.

***Availability:***

The system should be available, up and running 24/7 with a very high uptime. There will also be scheduled maintenance during off-peak hours (like 2:00-4:00 a.m.) and notify account holders 24 hours in advance to minimize disruptions. High uptime is critical for trust in the banking system. Target uptime is 99.9% which allows for a maximum of 8.76 hours of annual downtime. A failover mechanism will be implemented to switch to a backup server in case of server failure. In the event of unscheduled downtime, account holders will be notified via SMS and email within 15 minutes, and updates will be provided every hour until the system is restored.

***Usability:***

The system will have an intuitive and account holder-friendly interface for mobile that is easy to use even for less tech savvy account holders. We will not be implementing a web app due to additional complications and considering that most account holders prefer mobile banking. The need for a web app could change based upon account holder demographics. Material Design (for Android) and Human Interface Guidelines (for iOS) will be followed to ensure a consistent and intuitive account holder experience. Account holders with disabilities will also be accommodated by implementing screen reader support, high contrast mode for account holders with visual impairments and large touch targets for account holders with motor impairments. In-app surveys will be implemented to improve usability and for usability testing.

***Maintainability:***

The codebase should be made in such a way that it will allow easy updates and maintenance. There should be detailed documentation for developers. There should also be module integration. This helps both in-house developers and external partners to integrate with the system easily. Modular code structure will be implemented to make the code easier to maintain. Version control will be done using Git-based control system (e.g. GitHub, GitLab) with well-defined branching strategies to manage code changes. API documentation tools will be used, internal code documentation using comments will be practiced and account holder manuals and developer guides will be in place for onboarding new developers.

***Backup and Recovery:***

There will be regular and automated backups of account holder data and transaction log, though the account holder can turn it off at will. This is to provide account holders with the freedom to decide whether they want to allow their phone’s storage to be filled up with the backup files of the banking app. A disaster recovery plan will be planned and implemented to restore the system within a reasonable amount of time in case of failure. Daily incremental backups and weekly full backups of account holder data and transaction logs will be performed. Backups will be stored in the cloud using cloud services like Azure Blob Storage, backups will be retained for a minimum of 30 days and older backups will be deleted automatically and the account holders can also manually delete the backup data. In case of system failure, data loss will be limited to 15 minutes before the failure.

***Compliance:***

The system will be made in compliance to the banking industry standards and in compliance with the government regulations for handling financial transactions and account holder data. Compliance with the following will be ensured:

* PCI-DSS for secure payment processing.
* GDPR for account holder data protection (if targeting EU account holders).
* ISO 27001 for information security management.
* National data protection laws (e.g., Pakistan's Personal Data Protection Bill, if applicable).

The system will prioritize compliance with Pakistan's Personal Data Protection Bill, and ensure compatibility with GDPR and PCI-DSS for future international expansion.

***Interoperability:***

The system will have to integrate with external services such as government ID verification systems, third-party payments gateways, utility companies, etc. as it is a standard requirement for modern banking systems. The system will be integrated with NADRA APIs or equivalent services for real-time id verification. Popular payment gateways like Paypal, JazzCash and local banks’ APIs will be supported. Standardized REST APIs will be provided for bill payment companies

***Reliability:***

The system should ensure data integrity and consistency. Transaction failures should be handled gracefully and provide clear feedback to account holders. This ensures that transactions are reliable and failures are handled properly. This is a good way to ensure a seamless account holder experience and maintain trust with the account holder base. This all includes data consistency, error handling, and transaction rollback.