Project Setup and Requirements Gathering

This document outlines the initial project setup and requirements gathering phase for the development of a robust backend system for a bank. It defines the project scope, goals, and key features and functionalities required to meet the needs of a typical banking system.

A. Define Project Scope and Goals:

- **Scope:** The scope of the project will involve developing a robust backend system for a bank. It will include user management, account management, transaction processing, services, and security features.
- **Goals:** The goals of the project are create a secure, scalable, and reliable bank backend that meets the needs of a typical banking system. The system should handle user authentication, account management, transaction processing, and enforce security measures to protect sensitive data.

B. Identify Key Features and Functionalities:

1. ***User Management:***
    - User registration and login with authentication.
    - Role-based access control to manage user permissions.
    - Password management (reset, change, and hashing).
2. ***Account Management:***
    - Account creation and management for customers.
    - Support for various account types (e.g., savings, checking).
    - Account balance inquiry, transaction history, and statement generation.
3. ***Transaction Processing:***
    - Fund transfers between accounts (internal and external).
    - Validation and processing of transactions.
    - Categorization and tagging of transactions.
4. ***Services:***
    - Bill payment functionality for various services like mobile phone bills, utility bills, and internet bills.
    - Features to view and manage upcoming bills, payment history, and billing details.
    - Integration with service providers' APIs or payment gateways to facilitate seamless and secure bill payments.
    - Notifications and reminders to users regarding upcoming bills or payment due dates.
    - Transaction history tracking and display for each service bill, providing users with a comprehensive overview of their transactions.

5. ***Security and Compliance:***
   - Encryption of sensitive data (e.g., passwords, account details).
   - Secure communication protocols (TLS/SSL) for data transmission.
   - Compliance with regulations such as GDPR and PCI-DSS.
   - Logging and auditing of user activities for security and compliance.
6. ***Concurrency and Error Handling:***
   - Concurrent request handling to ensure system responsiveness.
   - Robust error handling and retry mechanisms for transient failures.
   - Graceful handling of exceptions and error scenarios.
7. ***Caching and Performance Optimization:***
   - Caching frequently accessed data to improve performance.
   - Database query optimization, indexing, and performance tuning.
   - Load balancing strategies to handle increased traffic.
8. ***Monitoring and Logging:***
   - Logging of application events for debugging and auditing purposes.
   - Real-time monitoring of system performance, health, and security.
   - Alerting and notifications for critical events.
9. ***Reporting and Analytics:***
   - Generation of various reports, such as account statements and transaction summaries.
   - Statistical analysis and insights on banking data.