ONLINE BANKING SYSTEM

1. KNS SRI HARSHITH - 22BD1A6725

2. SURI SHASHANK - 22BD1A6756

3. ALAKANTI SURYA - 22BD1A6702

Problem Statement:

In today's fast-paced world, online banking has become a crucial service for individuals and businesses, offering convenience and accessibility to financial operations. Customers expect a seamless, secure, and efficient experience when managing their finances. However, many users are unsure of the exact services or products they need when they visit their bank’s website or app. Instead of navigating through specific sections, they often prefer using a search engine or the banking platform's search function to find what they need.

Suppose a customer wants to apply for a loan or set up an investment account. Their search should present various loan types, interest rates, investment options, eligibility criteria, and other related financial services. As the customer narrows down their preferences by selecting criteria such as loan amount, tenure, or investment duration, the system should dynamically filter options, providing them with the best-suited financial product.

The main problem is ensuring accurate categorization of banking services and products. Misrepresentation or omission of information can lead to incorrect or incomplete search results, leaving customers confused or unable to make a decision. Another challenge is delivering a personalized experience that displays relevant offers for savings accounts, loans, credit cards, and other services based on user preferences and previous interactions.

Additionally, online banking platforms must ensure real-time updates. For instance, if a customer’s transaction is processed, the changes should immediately reflect in their account

balance. Similarly, new services should be promptly indexed and displayed, while services no longer available should be removed from the options.

Security is paramount in online banking. The system must prioritize protecting sensitive user data from breaches, theft, or unauthorized access. Transactions and personal details should be safeguarded using advanced encryption and multi-factor authentication. The platform must also support integration with multiple database systems (SQL, NoSQL) to handle large volumes of customer data efficiently.

Finally, the user interface must be highly intuitive, responsive, and easy to navigate, ensuring that users can perform transactions, manage accounts, and access services without complications. The goal is to provide a secure, user-friendly, and personalized banking experience that empowers customers to manage their finances confidently.

Software Requirement Specification

For

Online Banking System

Version 2.0

Prepared by:

1. KNS SRI HARSHITH - 22BD1A6725
2. SURI SHASHANK - 22BD1A6756
3. ALAKANTI SURYA - 22BD1A6702

Keshav Memorial Institute of Technology

19/10/2024

Table of Contents

Revision History:

Name	Date	Reason for changes	Version
Week-1	26/09/2024	SRS creation (Introduction)	1.0
Week-2	19/10/2024	SRS updation (Class & Use Case Diagrams)	2.0

1. Introduction

This Software Requirements Specification (SRS) outlines the agreement between the customer and developer regarding the features and specifications of the **Online Banking System**. It provides a clear understanding of customer needs and serves as a reference for the system's development.

1.1 Purpose:

The **Online Banking System** facilitates banking services, allowing users to perform transactions without visiting a bank. Customers can easily withdraw, deposit, and manage their accounts, providing a seamless banking experience.

1.2 Document Conventions:

- **Heading:**
    - Font Size: 16, Bold, Times New Roman
- **Subheading:**
    - Font Size: 14, Bold, Times New Roman
- **Content:**
    - Font Size: 12, Times New Roman

1.3 Intended Audience:

This document serves multiple audiences:

- **Developers:** For designing and implementing the system.
- **Managers:** For tracking project costs and timelines.
- **Advertisers:** To promote the system’s unique features.
- **Users:** To assess whether the system meets expectations.

- **Testers:** For validating functionality and performance.

1.4 Product Scope:

The **Online Banking System** operates 24/7 with scheduled monthly maintenance. It allows users to perform remote transactions, reducing the need for physical bank visits. Financial institutions can offer services on demand without maintaining large physical infrastructures.

Key features include:

- **User Assistance:** An intuitive help system to guide users.
- **Security:** Advanced protection for user data.
- **Feedback:** Ongoing improvements based on user input.
- **Data Management:** A secure database for user and financial information.

This is the software Requirement Specification for our Online Banking System. Our project is all about Net banking. It will facilitate the user to make transactions with visiting a bank. We will give the facility to customers to withdraw, deposit money from their accounts. We make the entire exchange between the customers very easy.

1.5 References:

We took references from different websites like HDFC, SBI and icici

HDFC Bank – Personal Banking & Netbanking Services

State Bank of India (onlinesbi.sbi)

ICICI Bank - Personal, Business, Corporate and NRI Banking Online

2. Business Objectives:

2.1 Product Overview

The project aims to develop an online banking platform that offers essential banking services to customers while enabling bank staff to manage accounts and financial products. The system will streamline day-to-day operations, allowing customers to perform transactions, view account details, and apply for services like loans. It will also offer secure data handling and a user-friendly experience accessible via both desktop and mobile devices.

2.2 Product Features

2.2.1 Bank Manager

- **Staff Management:** Bank Manager will be able to manage the Bank staff based on their performance, current status, leave records, etc
- **Branch Operations:** Manage and update details related to specific bank branches and ensure seamless customer service across multiple branches.
- **Customer Oversight:** View a list of customers within their branch, access customer profiles, and resolve account-related queries.

2.2.2 Bank Staff

- **Account Management:** Bank staff will be able to open, update, or close customer accounts, manage account details, and monitor transaction histories.
- **Loan Approval:** Staff can review loan applications, approve or reject them based on pre-set criteria, and manage loan-related inquiries.
- **Branch Operations:** Manage and update details related to specific bank branches and ensure seamless customer service across multiple branches.

- **Customer Oversight:** View a list of customers within their branch, access customer profiles, and resolve account-related queries.

2.2.3 Customers

- **Account Access:** Customers will be able to check their balance, review past transactions, and update personal details such as address or password.
- **Transactions:** Customers can conduct essential banking tasks such as transferring funds, making deposits or withdrawals, and repaying loans.
- **Loan Services:** Customers can apply for personal, home, or business loans, track the status of their loan applications, and manage repayments through the platform.
- **Alerts and Notifications:** Customers will receive real-time notifications for important activities, such as successful transactions, loan approvals, and account updates.
- **Card Services:** Customers can apply for credit card and debit card for ease of use and can manage credit repayment on the platform

2.3 Operational Environment

The online banking system will be cross-platform and support modern browsers such as Google Chrome, Mozilla Firefox, and Microsoft Edge. Additionally, it will provide a mobile-optimized version compatible with iOS and Android.

The system will be developed to run smoothly on operating systems such as Windows, macOS, and Linux with minimal hardware requirements.

2.4 User Types

The primary users of the system are:

- **Customers:** Individuals who access the system to manage their personal accounts, perform financial transactions, and apply for loans.

- **Bank Staff:** Employees of the bank responsible for handling customer accounts, processing loan applications, and managing branch services.
- **Bank Manager:** Head of the bank responsible for handling bank staff on top of other responsibilities like managing customer accounts, processing loan applications, and managing branch services.

The platform assumes that both customers and bank staff are familiar with basic web and mobile applications.

2.5 Design and Implementation Considerations

- **Security:** The system will employ robust security measures, including encrypted communication and secure authentication (multi-factor authentication if needed), to safeguard customer and transaction data.
- **24/7 Availability:** The online banking system must be available around the clock, allowing customers to access their accounts and perform transactions at any time.
- **Responsiveness:** The platform will be responsive, ensuring an optimized experience on both desktop and mobile devices, regardless of screen size or resolution.

2.6 Assumptions and Dependencies

The platform assumes that users will have access to a stable internet connection and compatible devices to access the banking services.

The backend of the system will rely on a database that securely stores sensitive information such as account balances, transaction histories, and loan data.

The success of the system depends on the availability of online banking support to customers, and the platform's ability to handle peak load times during busy banking hours.

4. Functional Requirements:

These requirements include the development of search tools, sorting, filtering, navigation, as well as the visual components of the site, which can be maintained by the bank staff or administrators.

4.1 Bank Manager

Requirement ID: RM.01.01

Title: Database Management

Description: The bank manager should have oversight of the entire database to ensure accurate tracking of all records related to customers, accounts, and loans. Any database access or update issues should be resolved promptly to minimize service disruption.

Priority: 2

Requirement ID: RM.01.02

Title: Loan Policy Review and Management

Description: The bank manager must periodically review and update loan policies to ensure they are aligned with industry standards and regulations. The manager should also oversee loan application processes to ensure compliance with bank policies.

Priority: 2

Requirement ID: RM.01.03

Title: Reporting and Analytics

Description: The bank manager should have access to analytical reports that provide insights into customer behavior, transaction volumes, and loan performance, enabling data-driven decision-making.

Priority: 3

Requirement ID: RM.01.04

Title: Staff Management

Description: The bank manager should have access to staff details, performance across different areas, areas of expertise, etc. for better staff management and allocation.

Priority: 3

4.2 Bank Staff

Requirement ID: RS.02.01

Title: Database Management Access

Description: Bank staff should have access to the database to track all records of customers, accounts, and loan details. They should be trained to resolve any issues with database access or updates efficiently.

Priority: 2

Requirement ID: RS.02.02

Title: Loan Management and Approval

Description: Bank staff should review loan applications submitted by customers and have the authority to approve or reject applications based on the bank's policies. All decisions must be logged for future reference.

Priority: 2

Requirement ID: RS.02.03

Title: Customer Account Management

Description: Bank staff should be able to view all customer details, transaction histories, loan applications, and account statuses to assist customers effectively.

Priority: 3

4.3 Customers:

Requirement ID: R1.02.01

Title: Customer Registration

Description: New customers should sign up by creating an account with their personal details (email or mobile number). Registration is mandatory for accessing banking services such as fund transfers and loan applications.

Priority: 1

Requirement ID: R1.02.02

Title: Customer Login

Description: Customers must use valid credentials (created at the time of registration) to log into the banking system securely.

Priority: 1

Requirement ID: R1.02.03

Title: View and Edit Personal Details

Description: Customers should be able to view and edit their personal information (e.g., address, phone number), payment methods, and account preferences.

Priority: 2

Requirement ID: R1.02.04

Title: View Account Balance and Transaction History

Description: Customers should be able to view their account balances and transaction histories, allowing them to track their financial activity.

Priority: 2

Requirement ID: R1.02.05

Title: Perform Fund Transfers

Description: Customers should be able to transfer funds between their own accounts or to other accounts, using valid online banking credentials.

Priority: 2

Requirement ID: R1.02.06

Title: Provide Feedback on Bank Services

Description: Customers should be asked to provide feedback on the quality of banking services they received, including transaction processes and customer support.

Priority: 3

Requirement ID: R1.02.07

Title: Loan Application and Tracking

Description: Customers should be able to apply for loans (personal, home, etc.), track the status

of their loan applications, and view repayment schedules.
Priority: 3

4.4 Bank Vendors:

Requirement ID: R1.03.01
Title: Vendor Collaboration with Bank Administrator
Description: External vendors (for services like insurance or financial products) must collaborate with the Bank Administrator to receive approval for offering their products under the banking platform. Initial product quality or service checks must be conducted, and vendors must maintain ongoing service quality.
Priority: 1

Requirement ID: R1.03.02
Title: Advertising Financial Products
Description: Vendors are responsible for promoting their financial products on the platform. The bank will not be held responsible for any claims or advertisements made by the vendors.
Priority: 2

Requirement ID: R1.03.03
Title: Receiving Customer Feedback on Financial Products
Description: Vendors should be responsible for receiving customer feedback and addressing queries related to the financial products or services they offer via the platform.
Priority: 3

Requirement ID: R1.03.04
Title: Providing Solutions for Customer Issues
Description: Vendors must provide quick and efficient solutions to customer complaints or inquiries regarding their financial products, ensuring minimal disruption to customer service.
Priority: 2

5. Other Nonfunctional Requirements for Online Banking System

5.1 Performance Requirements

- **Response Time**: Transactions such as balance inquiry, money transfers, and loan requests must complete within 2-5 seconds. Account details and balance history should load within 1 second under normal load conditions.
- **Concurrent Users**: The system must handle up to 5000 concurrent users without significant degradation in performance. The system should scale to accommodate peak traffic, especially during working hours and end-of-month transactions.
- **Database Transactions**: Each financial transaction should commit to the database within 1 second, ensuring data consistency and atomicity (ACID compliance) to avoid transactional errors.
- **Backup Speed**: Automated backups of sensitive data should occur within off-peak hours and must not impact system availability. The system must recover within 15 minutes in the event of failure.

5.2 Safety Requirements

- **Data Loss Prevention**: In case of a system crash or unexpected shutdown, all pending transactions must be either rolled back or stored securely to prevent any loss. The system must log any discrepancies and alert the administrators immediately.
- **Physical Safety**: The system must ensure that physical access to critical server components is restricted to authorized personnel only. No sensitive operations should be allowed unless the user has the correct level of access.
- **Transaction Safety**: To prevent incorrect transactions, the system must perform thorough checks, including available balance verification and approval workflows for high-value transactions. Any failed transactions should trigger automated rollback mechanisms and alert the customer.
- **Fraud Detection**: The system should have a built-in fraud detection mechanism to alert and block suspicious or unauthorized activities based on user behavior analysis and transaction patterns.

5.3 Security Requirements

- **User Authentication**: All users, whether customers, bank staff, or admins, must authenticate via a secure two-factor authentication (2FA) system before accessing the platform. Passwords should adhere to the latest encryption standards and be stored using cryptographic hashing (e.g., SHA-256).
- **Data Encryption**: Sensitive data like passwords, transaction details, and personal information must be encrypted in transit and at rest using at least 256-bit AES encryption.
- **Access Control**: Different levels of access should be enforced:
    - **Customer**: Can only access personal details, accounts, and perform transactions.
    - **Bank Staff**: Can access customer records and perform administrative tasks as defined by their role.
    - **Admin**: Can modify bank-wide configurations, grant permissions, and access logs.
- **Transaction Validation**: All transactions above a threshold amount (e.g., $10,000) must require secondary approval or multi-factor authentication.
- **Audit Logs**: All system activities must be logged for security audits, including login attempts, failed transactions, and unauthorized access attempts. Logs must be tamper-proof and stored securely.
- **Compliance**: The system must comply with financial data security regulations such as PCI-DSS (Payment Card Industry Data Security Standard) and GDPR (General Data Protection Regulation).

5.4 Software Quality Attributes

- **Availability**: The system must be available 99.99% of the time, ensuring minimal downtime, particularly during critical financial operations like payroll processing.
- **Reliability**: Transactions must be processed reliably, without any duplication or data loss. Fail-safe mechanisms should prevent incomplete transactions.
- **Scalability**: The system must be able to scale horizontally, supporting additional users and accounts without performance degradation as the number of customers grows.

- **Maintainability**: The codebase should be modular and easy to maintain, allowing for quick fixes and updates. Routine maintenance must be conducted without affecting system availability.
- **Portability**: The system should support deployment across various platforms and cloud services to allow for distributed operations and disaster recovery.
- **Interoperability**: The system must be able to integrate with third-party services like payment gateways (UPI, credit cards, internet banking) and notification services (SMS, email).
- **Usability**: The user interface must be intuitive and easy to use, ensuring a smooth banking experience for all customer demographics.
- **Testability**: All features must be easily testable with automated scripts, especially for security vulnerabilities, performance benchmarks, and functional testing.

5.5 Business Rules

- **Customer Permissions**: Customers can only access their own account details, manage payments, and request services such as loans or card replacements. No customer can access another customer’s account details.
- **Bank Staff Permissions**: Bank staff can approve or reject loan requests, update customer records, and oversee customer transactions. Permissions are role-specific.
- **Administrator Permissions**: Admins can override any system settings, including enabling or disabling bank services, modifying interest rates, and managing staff permissions.
- **Approval Process for Loans**: Any loan request must pass through a multi-step approval process that includes automatic credit checks, staff review, and, for high-value loans, management approval.
- **Refunds & Dispute Resolution**: Any dispute or refund process must be completed within 14 days. The system should allow automatic refunds if the service failure is detected on the platform's side.

Appendix A: Glossary

Account Balance:

The amount of money currently available in a customer's bank account, including all transactions that have been processed.

Categorization of Banking Services:

The process of organizing and classifying various banking services (such as loans, accounts, credit cards) into easily identifiable categories for user navigation and search.

Credit Card:

A payment card issued by a bank, allowing the cardholder to borrow funds to pay for goods and services, which must be repaid later.

Database System:

A structured system for storing, managing, and retrieving data efficiently. In this context, SQL (Structured Query Language) and NoSQL databases are mentioned, which are two different types of database systems used to handle customer data.

Encryption:

The process of converting data into a secure format that can only be accessed by authorized parties. Advanced encryption methods are used to protect sensitive information such as personal details and transactions.

Eligibility Criteria:

The set of conditions or qualifications that a customer must meet to access a specific financial product, such as a loan or investment account.

Investment Account:

A type of account used by customers to hold and manage investments, such as stocks, bonds, or mutual funds, often through the bank's platform.

Interest Rate:

The percentage charged by a bank on a loan or paid to a customer on savings accounts or investments, typically expressed on an annual basis.

Loan:
A financial product that allows customers to borrow money from the bank, with the obligation to repay the principal amount along with interest over a predetermined period.

Misrepresentation:
The act of providing incorrect or misleading information, which in the context of online banking, can lead to customer confusion or incorrect decision-making.

Multi-Factor Authentication (MFA):
A security process where users are required to provide two or more verification factors (e.g., password, OTP) before accessing their account, making the system more secure against unauthorized access.

NoSQL:
A non-relational database system that allows for more flexible data storage, typically used for handling large volumes of unstructured or semi-structured data.

Personalization:
The practice of customizing the banking platform's content and services based on a customer's preferences, behavior, and previous interactions, ensuring a tailored experience.

Real-Time Updates:
A system feature that ensures that any changes made to the account or system (such as processed transactions or new services) are reflected immediately and accurately without delay.

Responsive User Interface (UI):
A design approach where the interface automatically adjusts to various device screen sizes, ensuring that the platform is easy to use on both desktop and mobile devices.

Search Engine:
A feature within the banking platform that allows customers to search for specific products, services, or information by entering keywords, making navigation more efficient.

SQL:
A relational database management system used for structured data storage, which allows for querying, updating, and managing data using a standard language.

Tenure:
The length of time over which a customer agrees to repay a loan, or the duration of an investment, typically expressed in months or years.

Transaction:
An action performed by a customer within the banking platform, such as transferring funds, withdrawing money, or making a payment.

User Interface (UI):
The visual part of the banking platform that allows users to interact with the system, including menus, buttons, and forms.

Account Management:
The process where bank staff open, close, or update customer accounts, monitor transaction histories, and manage account-related information.

Alerts and Notifications:
Real-time messages sent to customers, informing them about activities such as completed transactions, loan approvals, or changes in account status.

Availability:
The system's ability to remain operational and accessible 24/7, ensuring customers can perform transactions or access account information at any time.

Balance Inquiry:
The act of checking the available balance in a customer’s account, typically performed through the online banking system.

Branch Operations:
Administrative tasks carried out by bank staff to manage and update the details and services provided at specific bank branches.

Cross-Platform:
A software feature that ensures the system works seamlessly across multiple operating systems and devices, such as desktops, tablets, and smartphones.

Customer Oversight:
The process by which bank staff manage customer profiles, monitor their account activity, and resolve any issues related to their accounts.

Deposit:
The process of adding funds to a bank account, either by the customer or an authorized third party.

Encryption:
The method used to protect sensitive data (like account details or personal information) by converting it into an unreadable format, which can only be accessed by authorized individuals.

Loan Approval:
The process where bank staff review and approve or reject loan applications based on predetermined criteria.

Mobile-Optimized:
A feature of the banking platform that ensures a smooth and responsive user experience on mobile devices, adjusting the interface to fit smaller screens.

Multi-Factor Authentication (MFA):
A security measure that requires users to verify their identity using two or more methods (e.g., password and SMS OTP) before accessing their account.

Operational Environment:
The technical ecosystem in which the online banking system operates, including the supported browsers (e.g., Chrome, Firefox) and operating systems (e.g., Windows, macOS).

Real-Time Notifications:
Immediate alerts provided to users about updates, transactions, or actions on their account without delay.

Responsiveness:
The system's ability to adjust its layout and performance based on the user's device (desktop or mobile), providing an optimized user experience regardless of screen size.

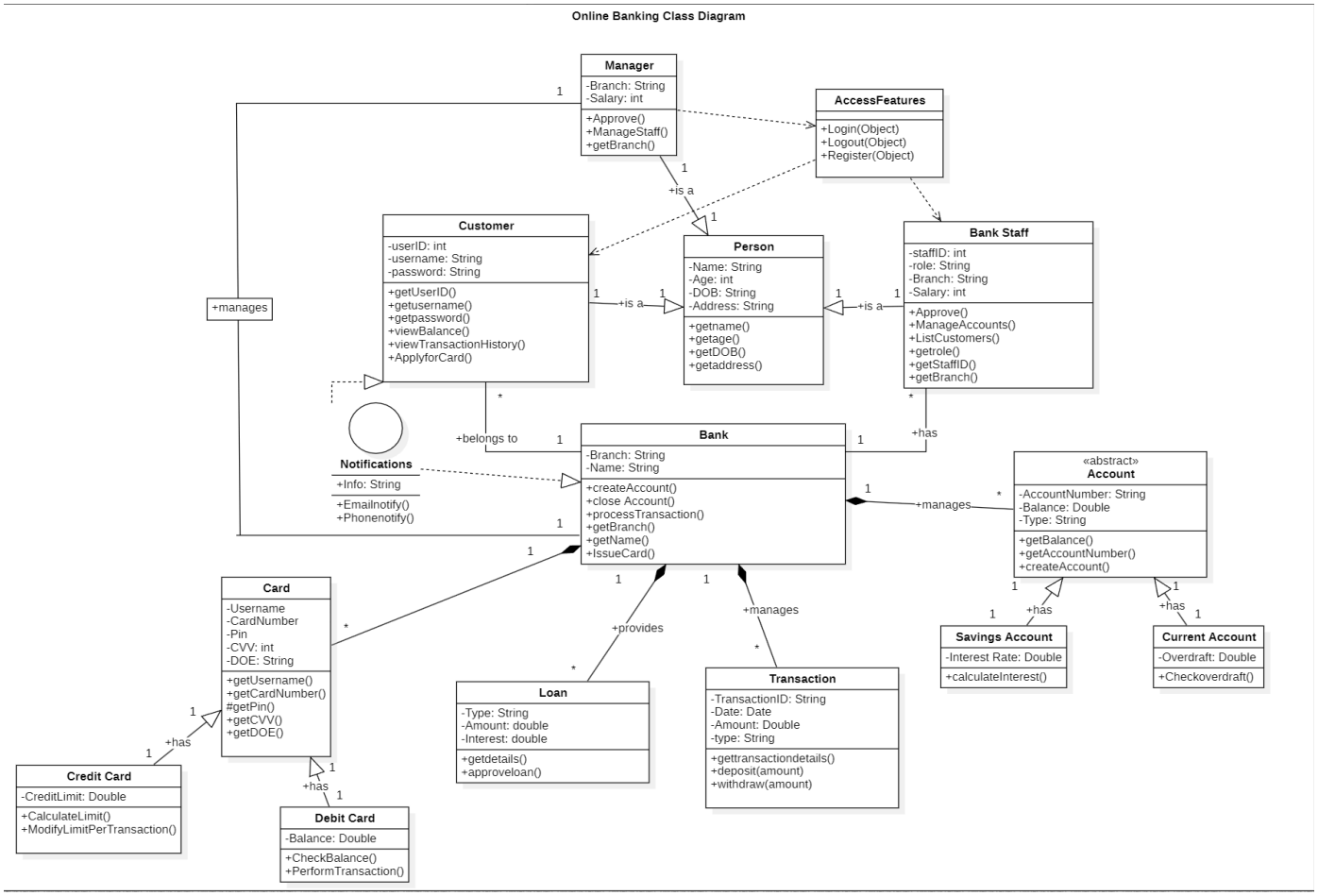
Scheduled Maintenance:
Regularly planned downtime where system updates or improvements are implemented, ensuring system performance and security are maintained.

Transactions:
Any financial operation initiated by a customer, such as transferring funds, depositing money, withdrawing cash, or paying off loans.

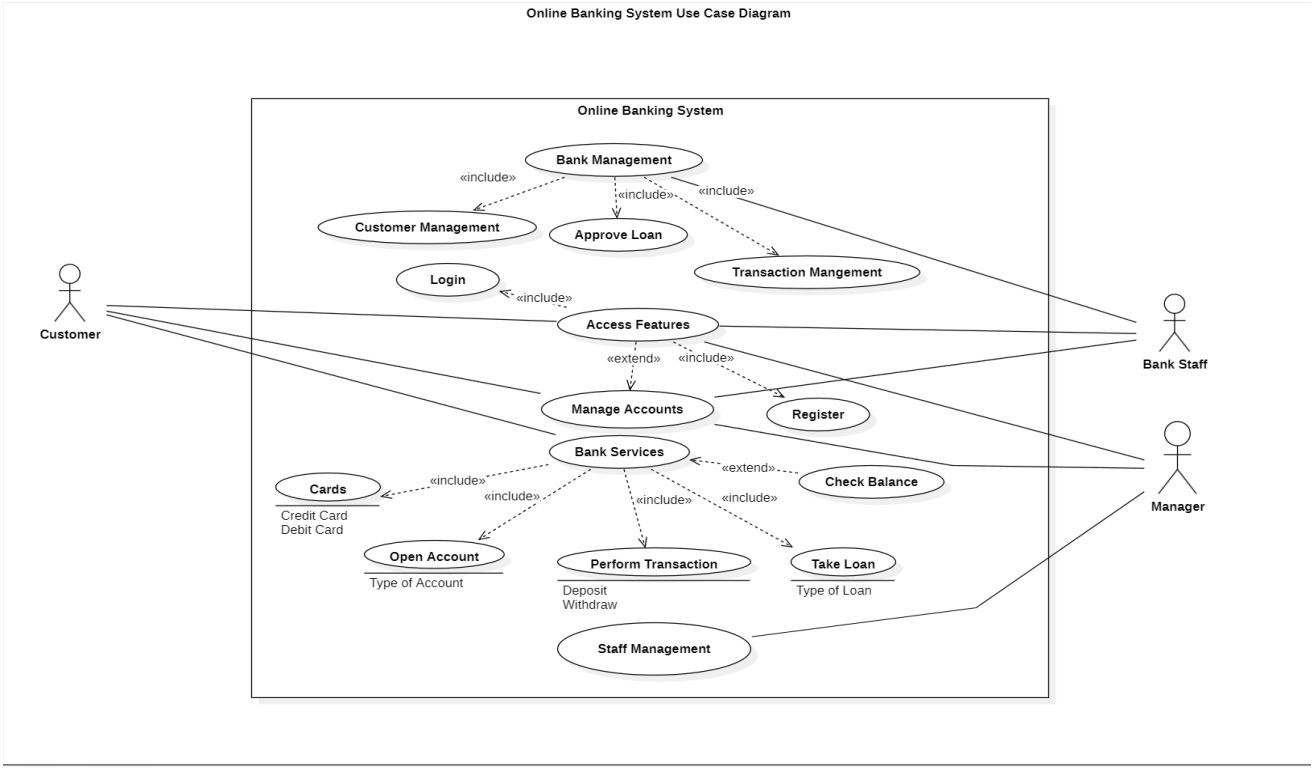
User Assistance:
An intuitive help or support system integrated into the platform to guide customers through the banking process, ensuring ease of use.

Appendix B: Analysis Models

Class Diagram:



Use Case Diagram:



Use Case Template:

Use Case ID:		1	
Use Case Name:		Online Banking System	
End Objective:		Facilitate Banking services to customers	
Created By:	1. Suri Shashank	**On** (date):	October 18,2024
	2. Alakanti Surya		
	3. K N S Sri Harshith		
User/Actor:		Customer and Bank Staff	
Trigger:		Customer utilizing Banking transactions in the site	
Basic/Normal Flows:			

User Actions	**System Actions**
The user logs into the banking portal by entering valid credentials.	The login page prompts the user for a valid username and password.
The user views account information, transaction history, and loan details.	The system retrieves and displays the user's account balance, transaction history, and any active loan details.
The user initiates a fund transfer or applies for a loan.	The system provides options to transfer funds to another account or apply for a loan. It validates the transfer/loan request.
The user views and edits their personal details, such as address and payment preferences.	The system allows the user to view and update personal information. Any changes made are updated in the database.
The user completes the banking transaction (e.g., fund transfer or loan application).	The system processes the request, updates the balance/loan status, and provides a confirmation message
Exception Flows	
User Actions	**System Actions**
The user attempts to log in but doesn’t have an account.	The system prompts the user to register for an account through the registration page.
The user enters incorrect login credentials	The system displays an error message: "Please check the username or password entered" and prompts the user to re-enter the correct details.
The user tries to transfer funds, but the account balance is insufficient.	The system displays a message: "Insufficient balance for this transaction" and does not proceed with the transfer.
The user applies for a loan, but the loan request exceeds their credit limit or the application is incomplete.	The system displays an error message: "Loan request denied due to insufficient credit limit" or requests the user to complete missing details.

Appendix C: To Be Determined (TBD) List

The following items have been identified as "To Be Determined" (TBD) in the Software Requirements Specification (SRS) for the Online Banking System. These elements need to be finalized or further elaborated during the system design and development phase:

- **Sequence Diagrams**
    - A detailed sequence diagram is required to illustrate the interactions between system components, users (customers, staff, manager), and external systems (e.g., payment gateways, external vendors) during key operations such as login, fund transfer, loan application, and transaction processing.
    - Status: TBD
    - Target Closure Date: 25/10/2024
- **Component Diagram**
    - A component diagram is necessary to show the high-level architecture of the banking system, depicting the system's key components, such as the user interface, database, authentication service, notification system, etc.
    - Status: TBD
    - Target Closure Date: 25/10/2024
- **System Integration Plan**
    - A comprehensive plan detailing how various system components will integrate, particularly how third-party services (e.g., external financial product vendors, insurance providers) will be connected to the core banking system.
    - Status: TBD
- **Load and Performance Testing Requirements**
    - Precise performance benchmarks for load handling, including maximum concurrent users, transaction speed under different load conditions, and system response time.
    - Status: TBD
- **Error Handling and Recovery Mechanisms**
    - Specifications on how the system will handle errors and unexpected failures, including rollback mechanisms, logging, and recovery processes.

    - Status: TBD
- **Detailed User Roles and Permissions Matrix**
    - A detailed matrix of user roles (e.g., customer, bank staff, bank manager, admin) and their corresponding permissions within the system.
    - Status: TBD
- **Security Protocols and Encryption Standards**
    - Specifications regarding the exact encryption standards and protocols to be used for securing sensitive data (e.g., customer personal details, transaction data) both in transit and at rest.
    - Status: TBD
- **Data Backup and Recovery Plan**
    - A detailed plan specifying how customer and system data will be backed up, including frequency, storage location, and recovery procedures in the event of a system failure or data loss.
    - Status: TBD
- **Mobile Platform Integration Details**
    - Further details on how the system will integrate and function on mobile platforms, including responsiveness and feature parity with the web version.
    - Status: TBD