SouthWest Bank

Secure Banking System

Software Requirements Specification (SRS)

Group 15

Aneesh Shastry
Karthik Narayan
Mahathi Shakthidharan
Rajesh Surana
Sagar Sangani
Shankar Krishnamurthy
Tanvi Apte
Varun Burde

Revision History

Date	Revision	Description	Author
09/12/2015	1.0	Initial Version	Mahathi Shakthidharan
09/18/2015	2.0	Second Version	Shankar Krishnamurthy
09/24/2015	3.0	Third Version	Rajesh Surana
09/24/2015	4.0	Fourth Version	Mahathi Shakthidharan

Table of Contents

1. Purpose

Purpose of this document is to describe the specific as well as non-functional requirements of Secure Banking System (SBS) in detail. It also describes types of users who will be using SBS and their access controls, how they will be interacting with the system, etc. As this project focuses on implementing secure web services, we dedicate considerable portion of this document on explaining various security features that this system will implement. This document establishes contract between current requirements of the bank and to be developed Banking System.

Primary intended targets of this document are developers, testers, stake holders and higher level users of this system.

1.1. Scope

Scope of this document is to provide thorough insight into system architecture, various use cases for user interaction with system interface, security features, hardware and software tools specification and systems constraints.

1.2. Definitions, Acronyms, Abbreviations

The following is a list of commonly used definitions used throughout this document:

1.2.1. Definitions

1.2.1.1. Secure Banking System: It is a software system developed primarily to facilitate secure banking transactions and user account management through the Internet.

1.2.1.2. One Time Password: It is valid for only one login and for specific amount of time stated at the time of generation. In contrast to static password, it is impervious to replay attacks.

1.2.1.3. Personally Identifiable Information: In this software system it will be name, account number, email, residential address and phone number.

1.2.1.4. Internal User: User who is using SBS for providing services to external user. This could be bank manager or system administrator.

1.2.1.5.External User: User who is using SBS for own monetary transactions. This user has at least one account in the bank.

1.2.2. Acronyms

1.2.2.1. SBS: Secure Banking System

1.2.2.2. SRS: Software Requirement Specification

1.2.2.3. OTP: One Time Password

1.2.2.4. UML: Unified Modeling Language

1.2.2.5. PKI: Public Key Infrastructure

1.2.2.6. PII: Personally Identifiable Information

1.2.2.7. GUI: Graphical User Interface

1.2.2.8. SSL: Secure Socket Layer

1.2.2.9.TSL: Transport Layer Security

1.3. References

[1] https://www.digicert.com/ssl.htm
[2] https://en.wikipedia.org/wiki/One-time_password
[3] https://en.wikipedia.org/wiki/Public_key_infrastructure
[4] https://en.wikipedia.org/wiki/Personally_identifiable_information

1.4. Overview

This SRS document describes the system software for banking purpose in terms of its functionality, environment, users and security features. This system will endow external users with the ability to debit/credit, transfer and pay from their account securely. They can also access transaction history and bank statements using secure logic to their accounts.
Internal Users like bank employee can access transactions initiated by external users with proper authorization in order to approve or decline them. They will provide other services like account creation/deletion, system troubleshooting and money transfer. Some internal users will be maintaining other internal users' information.

To implement the security we use Public Key Infrastructure, Digital Certificates, Virtual Login Keyboard and OTP.

This system will be hosted on a virtual machine and will be available to users online through secure interface.

2. Overall Description

2.1. Product Perspective

The Secure Online Banking system has been designed to allow customers – internal and external users, of a banking organization to perform transactions and bank operations online in a secured manner. Security to such an application is of utmost importance and any defect in the software can lead to huge financial losses.
The internal users- who are the bank employees and the bank manager, of the application use the system to perform banking and manage critical transactions of all user accounts while external users – the individual customers and the merchants use the system to initiate transfers, payments etc. from their individual accounts. The functionalities and features are explained in detail in the below sections.

2.2. Product Architecture

The system has a three tier architecture with a database layer. It can be represented as follows

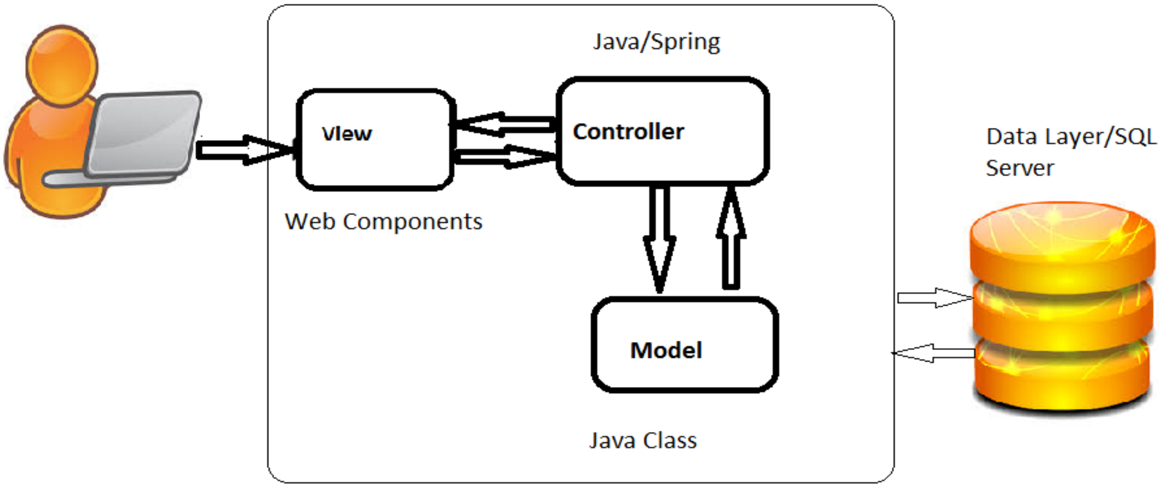


Fig. 1. - Product Architecture

2.3. Product Functionality/Features

User Login

- Here, the users are allowed to access the system features through a secure login mechanism.
- Authentication to first time login through a device is provided through OTP.
- The users are also provided with password recovery link.

External User Account Functionalities/Features

- Users can initiate a change in the account critical information through an approval mechanism wherein any change has to be approved by the bank employees before it is updated in the system.
- External Customers of the system can initiate transfers to other customers through the unique external customer identification ID.
- The customers can set preferences for alerts in various transactions in their accounts.
- The customers will also be provided with option to restrict the bank employees to view their information.
- External customers are also provided with option to initiate transfers to a list of registered merchants in the system.
- The External customers of the system are also provided with options to download statements.
- A special set of external users called the merchants will be able to accept the initiated payments by the individual customers and forward it to the bank to receive payments.

Bank User (Internal User) Functionalities/Features

- The internal users of the system are classified into two groups – Bank employees and system admins.
- The regular employee will be creating the set of external user accounts and the manager will approve the creation of the accounts.
- The bank employee sub group are further categorized as regular bank employees and bank managers.
- The regular employees are provided permissions to review critical transactions by the manager and upon approval they can review the pending critical transaction pool and approve them to proceed.
- Upon approval from the individual users, the regular employees will be able to view, update and modify the individual user account information.
- The bank managers in addition to access the features and functionalities of the regular employees will have access to management of individual user accounts.
- The system admins have access to the various system resources and their functionality is to manage the internal (Bank employee) accounts. The management of the internal user accounts include creation, modification and deletion of the internal user accounts.
- The system admins can also access the encrypted PII information of the employees and forward it to the government employees on request.

Security Features

Security is important part of banking application. Such an application deals with customer's critical personal information and financial information. To ensure the security of the application the following security features have been implemented

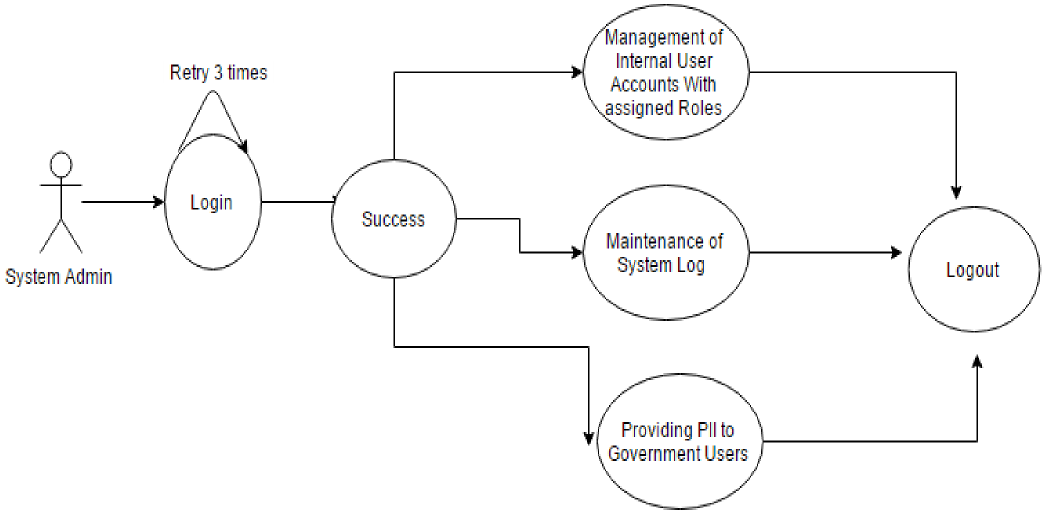
- Secure Sockets Layer (SSL): This technology is used in our application to establish a secure connection between the server and the client. This connection is used by both the server and the client for all communication during the session. When a client requests a secure SSL connection, the host replies back with a valid SSL certificate and this certificate is used for the communication. At the end of each session, the connection is automatically terminated.
- Public Key Infrastructure (PKI): In addition to the SSL, the PKI will also be implemented for the security of the application. A public key infrastructure (PKI) supports the distribution and identification of public encryption keys, enabling users and computers to both securely exchange data over networks such as the Internet and verify the identity of the other party.
- One Time Password (OTP): This feature sends a temporary password to the user to a pre-registered e-mail address. This password is then verified by the system when a user has to make a critical transaction and for merchant payments.
- In addition, all system logs are accessible only to the system admin to maintain confidentiality and security of the system.

2.4. User Characteristics

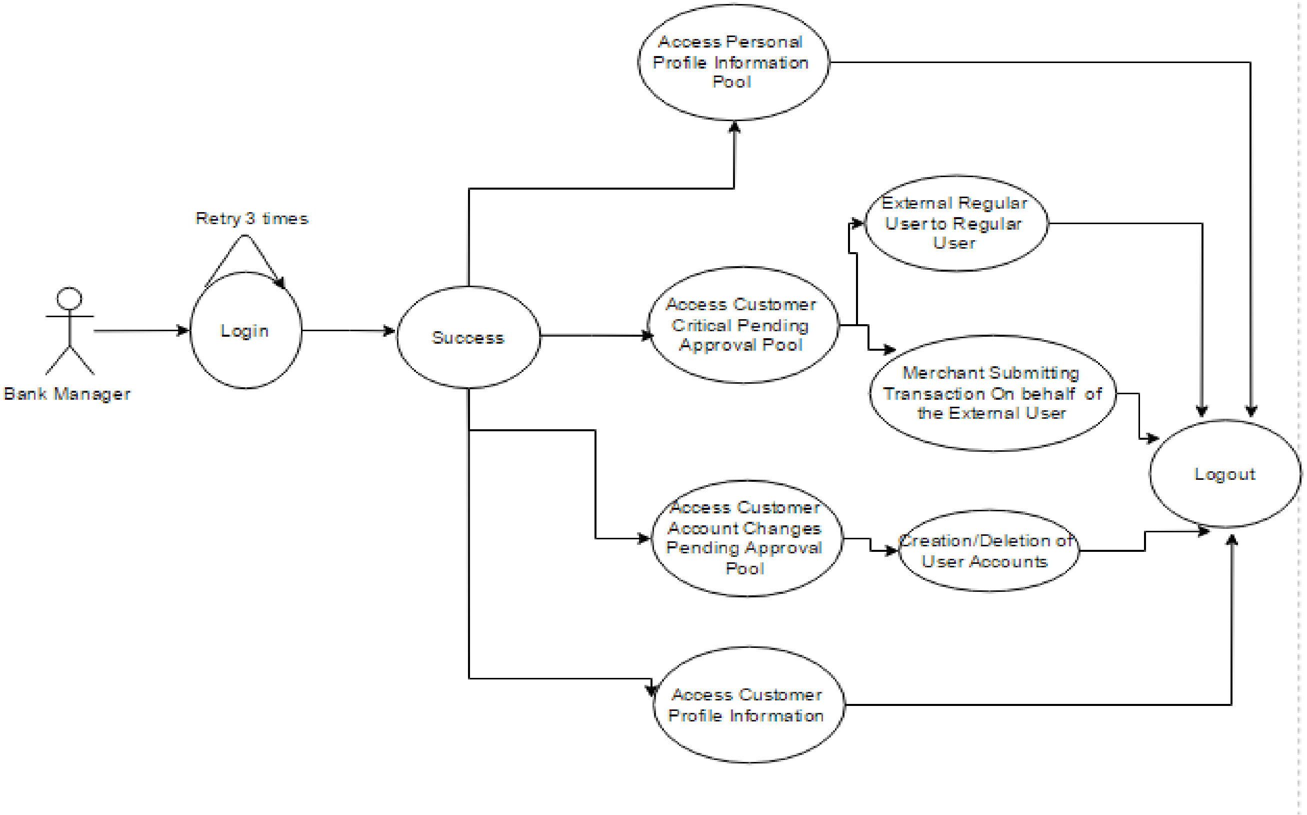
The users of the system can be broadly classified into two categories

- Internal Users – This group of users are further classified into three roles. The internal users of the system will be allowed to access different functionalities and features of the system as opposed to the external users. Here is a brief look of the various features that each category of internal users can access

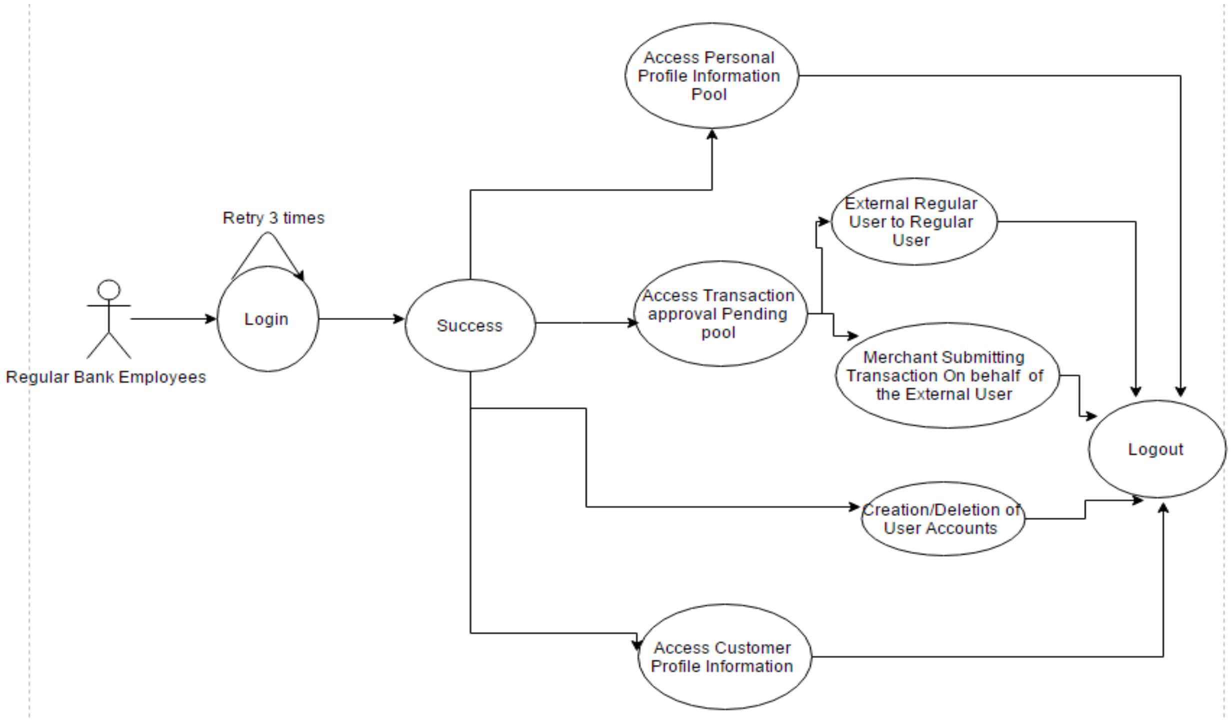
- System Administrators


Retry 3 times
System Admin
Login
Success
Management of Internal User Accounts With assigned Roles
Maintenance of System Log
Providing PII to Government Users
Logout

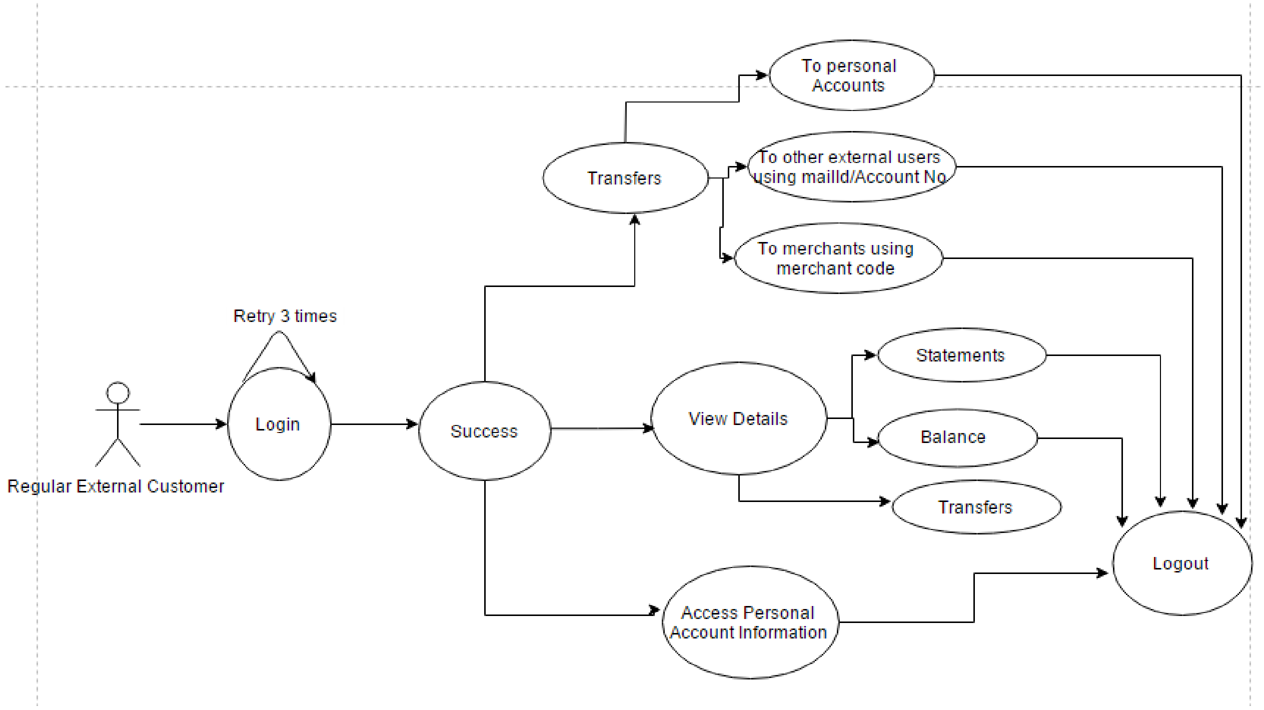
- System Managers


Access Personal Profile Information Pool
Retry 3 times
External Regular User to Regular User
Bank Manager
Login
Success
Access Customer Critical Pending Approval Pool
Merchant Submitting Transaction On behalf of the External User
Logout
Access Customer Account Changes Pending Approval Pool
Creation/Deletion of User Accounts
Access Customer Profile Information

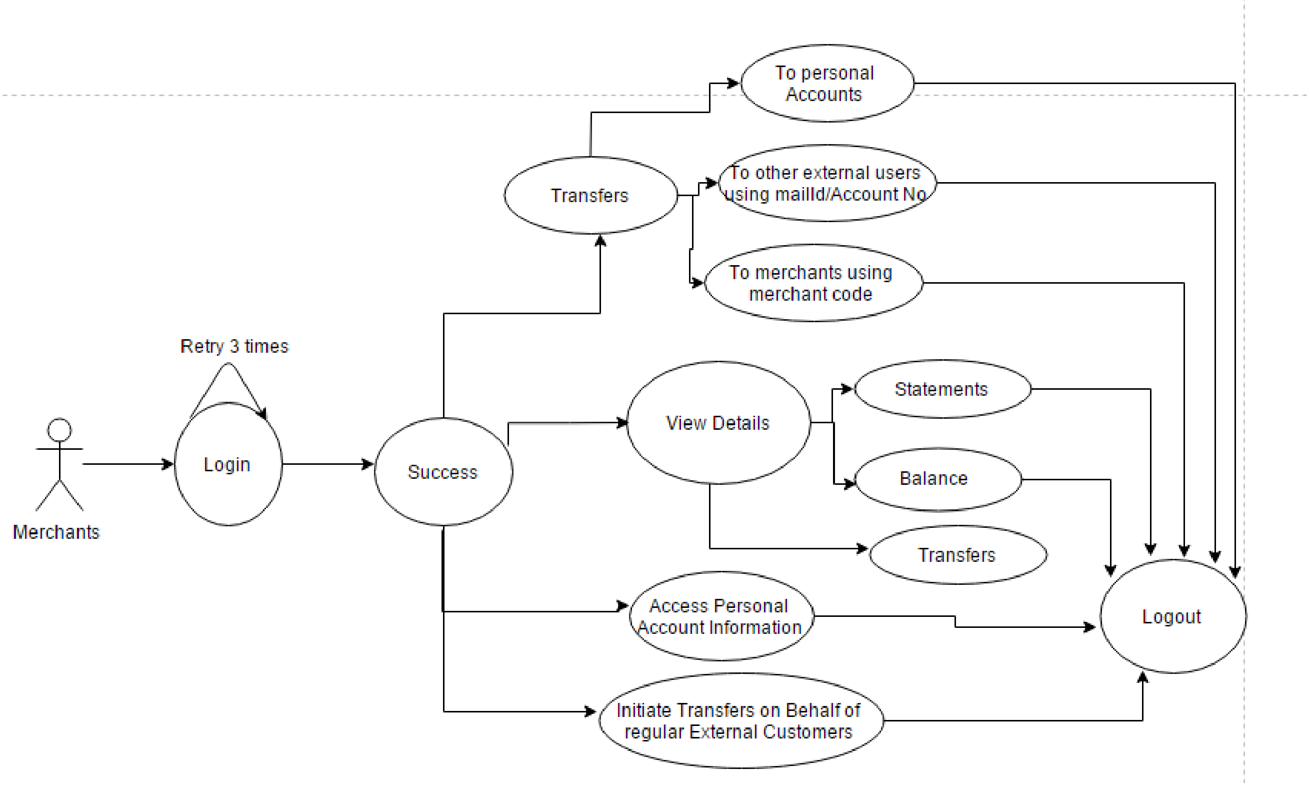
- Regular Employees


Access Personal Profile Information Pool
Retry 3 times
External Regular User to Regular User
Login
Success
Access Transaction approval Pending pool
Merchant Submitting Transaction On behalf of the External User
Regular Bank Employees
Logout
Creation/Deletion of User Accounts
Access Customer Profile Information

- External Users – This group is further classified into two roles
  - Individual Customers


To personal Accounts
Transfers
To other external users using mailId/Account No
To merchants using merchant code
Retry 3 times
Statements
Login
Success
View Details
Balance
Regular External Customer
Transfers
Logout
Access Personal Account Information

- Merchants


To personal Accounts
Transfers
To other external users using mailId/Account No
To merchants using merchant code
Retry 3 times
Statements
View Details
Login
Success
Balance
Merchants
Transfers
Access Personal Account Information
Logout
Initiate Transfers on Behalf of regular External Customers

2.5. Constraints

The following are the constraints of the software application designed for the users of the system.

- Each user of the system will be able to perform critical transaction using the system only upon approval from the bank employees.
- The regular bank employees will be able to perform modify the user accounts only upon permissions from the individual customers.

2.6. Assumptions and Dependencies

- Implementation of certain functionalities like e-mailing is dependent on third party tools and any bug found with respect to these should be resolved by communicating with the owner of the tools.
- The developed application will be deployed in the virtual provided by vlab.asu.edu and it is assumed that the machine is available at all times.

3. Specific Requirements

3.1. Functional Requirements

System software should support following types of users and corresponding capabilities –

3.1.1. Internal Users

These are the bank employees maintaining external users' accounts and completing transactions on behalf of them. Proposed SBS will support following types of internal users –

3.1.1.1.Regular Employee

- User is responsible for low priority transactions.
- User can view, create, modify, delete and authorize transactions upon having necessary authorization from the users and/or merchants.
- User does not have access privilege to view or modify any user account unless he/she has been authorized to do so.
- User can access transactions with necessary authorization from users/merchants or system administrator.

3.1.1.2.System Manager

- User is responsible for higher priority banking operations and responsible for the authorization of critical transactional operations.
- User can verify external users' requests.
- User can authorize for critical transactions.
- User can access transactions with necessary authorization from users/merchants or system administrator.
- User can add/modify/delete external user accounts with necessary request from external user and respective regular employee.

3.1.1.3.System Administrator

- User maintain all the internal user accounts and the banking system.
- User can verify internal users' requests to update account details.
- User can add /modify /delete internal users' account.
- User can access and download the system log file.
- User can access PII with necessary authorization/request from government agencies (no automatic PII access).

3.1.2. External Users

These are the customers of the bank who have their saving/checking accounts with the bank. SBS should support following types of external users -

3.1.2.1.Individual Customer

- These are the individuals having banking activities, each of whom have an user account for performing personal banking transactions such as personal fund transfer, debit and credit from personal user account.
- User can retrieve and download the account balance statements.
- User can view, debit, credit and transfer money from his/her personal bank account.
- User can initiate modification personal information change or transactional review.
- User can authorize bank official requests to review transactions on accounts he/she is responsible for.

3.1.2.2.Merchant/Organization

- These are the users having specialized banking transaction processing requirements, such as client payment processing.
- User can submit an individual users/merchants payment to the bank with proper authorization from users/merchants.
- User can view, debit, credit and transfer money from merchants' bank account.
- User can initiate modification personal information change or transactional review.
- User can authorize bank official requests to review transactions on accounts the merchant is responsible for.

3.2. External Interface Requirements

External interface of the SBS is in the form of web pages opened in browser. The front page will have login window which will require email as username, password and captcha to log into account. Unauthorized user won't be able to pass beyond this page. After logging in each user will have user interface based on his role.

3.2.1. Login View

- Username text field
- Password text field [pops up virtual keyboard on clicking inside.
- Login button
- Forget password button

3.2.2. Regular Employee

- List of pending transaction pool in the form of table
- View and edit external user and merchant's account information. Some of the fields will be editable based on the external user authorization
- List of pending account update requests (from external user and merchants) in the form of table.
- New bank account creation request option for an external user (with manager's approval)
- Logout button

3.2.3. System Manager

- List of pending transaction pool in the form of table
- Filter button to filter out non-critical transactions
- View and edit external user and merchant's account information. Some of the fields will be editable based on the external user authorization.
- A list of pending external users' bank accounts to be created in the form of table
- A search box to pull up any user and linked account
- List of pending account update requests(from external user and merchants) in the form of table
- Logout button

3.2.4. System Administrator

- View and edit internal user account details in the form of table
- List of system logs in the form of table
- Search box to pull up internal users PII and ability to update it
- Logout button

3.2.5. Individual Customer

- Retrieve and download Balance
- Button to download statements in the specified date range
- Transfer button which pull up empty transfer form
- Transfer form to transfer money with send button
- Account information with some of the field editable
- List of changes done by bank employees to user's account in the form of table with approve or deny button for each change
- Newsfeed section listing history of account changes
- History of past transactions in the form of table
- Limit field to set daily transaction upper cap
- Logout button

3.2.6. Merchant/Organization

- All of the interface items listed for individual user
- Special transfer button to transfer amount to another merchant
- List of transactions for received money with accept/decline buttons
- Logout button

3.3. Internal Interface Requirements

System's internal interface will follow following architecture -

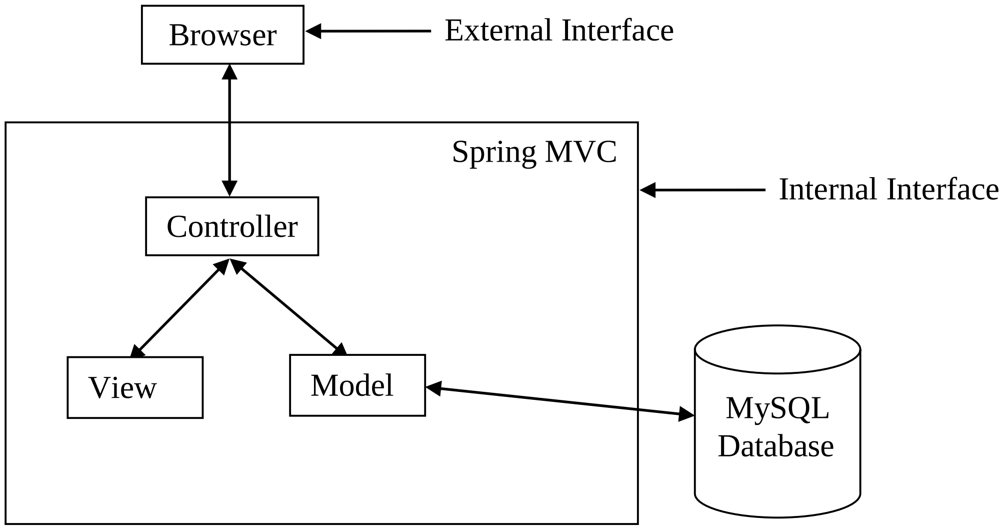


Fig. 2 *- Internal and External Interface for SBS*

3.4. Internal Data Requirements

All data in SBS will be stored in the MySQL database. Data transfer over internet will be done securely using public key infrastructure and https protocol.

3.5. Design and Implementation Constraints

- OTP will be valid for 20 minutes only after generation.
- External individual user will be able to do transaction up to a maximum of $10000 each day.
- User can set limit for max transaction per day.
- After 3 unsuccessful attempts user won't be able to login for 1 hour.
- Regular employee will not be able to view/edit external user's account information without proper authorization.
- Only system admin can view and update internal users PII.

3.6. Other Requirements

- This system software will be written in Java (Spring MVC).
- Apache will be used for web hosting.
- MySQL database will be used to store data.
- Basic security features will be implemented using spring and some of them could be accomplished using third party product.

4. Non-Functional Requirements

4.1. Safety Requirements

Software Reliability is the probability of failure-free software operation for a specified period of time in a specified environment. Software Reliability is also an important factor affecting system reliability. Maintaining Reliability and security in a banking application should be a priority as it deals with the users secure information and banking transactions. The safety requirements that are implemented in the design of the system are

- A stable internet connection for the users of the system to access the web application.
- Stable power to run the server to host the web application.
- A strong login username and password should be enforced to increase the safety of the user accounts.
- The system should be designed to prevent various attacks like session hijacking, cross scripting, SQL injection.
- Inactive sessions after a set time period will be automatically closed and the user has to be authenticated again before providing access to the system.

4.2. Security and Privacy Requirements

- The users should have an active login account with the system to access the bank application. This mechanism ensures that all users are authenticated before they are provided access to the system.
- One Time Password mechanism will be implemented in two use cases – the first case during the merchant’s payments. The second case being for the critical transactions i.e. the user’s transactions should be validated with OTP before they are processed.
- Role Based Access Mechanism has been designed so that we can prevent attacks like Excessive privilege attacks.
- The different features and functionalities of the application is restricted based on the designated role of the user accessing the system. This helps us to prevent against Privilege Elevation Attacks
- Validating the input in multiple views for alphanumeric characters, entered by the users for SQL Injection attacks, verifying the access by the users to the application for any denial of service attacks are few of the security measures that to be implemented in the system. The users will also be restricted to enter critical information only through a secure virtual keyboard.
- Added to the mentioned security features, encryption of critical data using Public Key infrastructure will be enforced.

4.3. Environmental Requirements

The following is the environment setting required to host the application server in vlab.asu.edu

- Operating System : Windows 7
- A stable internet connection at both the server and client for communication. The minimum bandwidth at which the internet connection can operate at the server side is and the client side is

4.4. Computer Resource Requirements

4.4.1. Computer Hardware Requirements

The hardware required to host the server are

- RAM : 512Mb
- HardDrive: 10GB
- Processor: 2GHZ
- Internet Bandwidth : 1Mbps

The application is designed to be easily accessed by the users at any time with access to internet and a working browser.

4.4.2. Computer Hardware Resource Utilization Requirements

Since the project is a complete online banking system, there are no additional hardware resources that are required other than the server hardware requirements that has been mentioned in section 4.4.1. The client accessing the application can do so with access to stable internet connection.

4.4.3. Computer Software Requirements

The following are the software that is used in the server. Admin access to the following applications and system is also required to troubleshoot any issues.

- Web Server : Apache Tomcat
- Database : MySQL

Any user accessing the system should have a working browser that runs JavaScript functions that are used in the application for validations.

4.4.4. Computer Communication Requirements

- The system communicates with the user in the following scenarios
    - To receive the OTP during the first time login through a device and for various critical transactions
    - To notify the user of change in personal Information
    - To notify the users communication of dispute in transaction(mainly rejection of the transaction initiated)

4.5. Software Quality Factors

The following are the minimum quality that is expected out of the software applications

- Availability: The system will be designed so that multiple users can access the system simultaneously without ambiguity in any of the transactions.
- Reliability: The system should be accessible by all users 24/7. We have also ensured that there are no data loss through session time outs and closing the connection to the server every time the user closes the session.
- Maintainability: The system should be designed such that the code should be easily maintainable and any future enhancements desired should be developed with minimum changes of the current system design.
- User Friendly: The system is designed to have user friendly interface for the user to access all features and functionalities. The system is also accessible through multiple platforms.
- Efficiency: An efficient system ensures high performance and execution of the requests once the application has been deployed and our system will be designed to have a high efficiency rate.
- Security: Proper security features have been implemented to thwart potential threats and vulnerabilities.

4.6. Packaging Requirements

A user guide has been documented providing instructions to load the system into multiple environments along with the details of the installation of any third party libraries used in the system. This will ensure easy migration of the system to multiple platforms without minimal effort.

4.7. Precedence and Criticality of Requirements

Based on the requirements identified so far, we have classified the requirements according to the importance of the requirement to the application has been classified as Required, Optional, Critical requirements. The following table also indicates the order in which the requirements should be implemented for developing the application on time.

S.No.	**Requirements**	**Precedence**	**Classification**
1	Functional Requirements	1	Required
2	External Interface Requirements	2	Required
3	Internal Interface Requirements	2	Required
4	Internal Data Requirements	1	Critical
5	Safety Requirements	2	Critical
6	Security and Privacy Requirements	1	Critical
7	Environmental requirements	3	Required
8	Computer Resource Requirements	4	Required
9	Computer Hardware Requirements	3	Required
10	Computer Software Requirements	3	Required
11	Software Quality Requirements	1	Critical

5. Qualification Provisions

This section defines a set of qualification methods. Qualification methods are characterized into: -

- ***Demonstration*** – A qualification method which relies on observable functional operation and do not require any special test or elaborate instrumentation.
- ***Test*** – A qualification method which is carried out by relying on the data fed to the system.
- ***Analysis*** – A qualification method which is carried out by analyzing the accumulated data.
- ***Inspection*** – A qualification method which is carried out by visual examination of software item.
- ***Special*** – A qualification method which relies on any special method like special tools, techniques, procedures etc.

5.1. Qualification Matrix

S.No	Requirement	Compliance Synopsis	Qualification Method
1.	The system should provide access according to the user login.	Login as different users like regular employee, manager, etc and check if access is available only to designated page.	Analysis
2.	The system should provide password recovery option.	Security Questions will be used for user authentication.	Test
3.	System should validate username/password.	Check if system denies access to the system with incorrect username/password.	Test
4.	System should facilitate all features which the designated user has privilege for.	Login as different users and check if all the available links are working.	Demonstration
5.	Credit/Debit should be made from/to correct account.	While transferring fund check if money is debited/ credited to correct account	Inspection

6.	Transfers should be made only when its acceptable.	Check if the transfer amount is not more than available balance	Analysis
7.	Transfers below minimum threshold should be denied.	If amount entered to be transferred is below 1 dollar, transaction shouldn't be allowed.	Test
8.	Internal Employees shouldn't be able to view/modify any user account unless authorized to do so.	Check if internal employee is able to view any account only on authorization by the user.	Demonstration
9.	Fund transfer should be secured.	Check if the site provides an SSL and PKI.	Inspection

6. Requirements Traceability

S.No	Functional Requirement	Login	Create Account	Internal Account Mgmt.	External Account Mgmt.	Transaction Mgmt.	Transaction	Authorization	Syslog
1.	**Regular Employee**	X	X		X	X	X		
1.1	Approve low priority transaction						X		
1.2	Can view, create, modify and delete transactions upon having necessary authorization from users / merchant					X	X		
1.3	Doesn’t have access to view/modify user account unless authorized to do so.				X				
2.	**System Manager**	X	X		X	X	X		
2.1	Authorize critical transactions						X		
2.2	Can view, create, modify and delete transactions upon having necessary authorization from users / merchant					X	X		
2.3	Can add/modify/delete user accounts with necessary authorization				X				
3.	**System Administrator**	X	X	X					X
3.1	Maintain all internal user accounts		X						

3.2	Can add/modify/delete internal user accounts			X					
3.3	Can access system log file								X
4.	**Individual User**	X					X	X	
4.1	Can view, debit, credit & transfer money his/her personal account						X		
4.2	Can authorize bank official’s requests to review transactions on account he/she is responsible for.							X	
5.	**Merchant**	X					X	X	
5.1	Can submit an individual users/merchants payment to the bank with proper authorization from users/merchant.						X		
5.2	Can view, debit, credit and transfer money from merchants bank account						X		
5.3	Can authorize bank official requests to review transactions on accounts the merchant is responsible for.							X	
S.No	**Non-Functional Requirement**	**Login**	**Create Account**	**Internal Account Mgmt.**	**External Account Mgmt.**	**Transaction Mgmt.**	**Transaction**	**Authorization**	**Syslog**
1.	User should have an active account to access banking system	X							
2.	OTP	X					X		

3.	Role Based Access Control							X	
4.	Public Key Infrastructure						X		
5.	Secure Socket Layer(SSL) Protection	X							