Software Requirements Specification (SRS)

Version 1.0

“e-Banking Management System”

Project By:

Bhagvat Giri

## Introduction:

## Purpose:

## The Purpose of this document is to present a detailed

## description of the e-banking management system. This

## document will explain the purpose, and features of the system,

## the interfaces of the system, what the system will do, the

## constraints under which it must operate and how the system will

## react to external stimuli. This document is intended for both

## stakeholders and the developers of the system and will be liable

## for the approval of the project by the community of the Bank.

## The Traditional way of handling details of a user in a bank

## was to enter the details and record them. If user wants to check

## their transaction or balance inquire, they have to go online on

## bank website for different banks and download a statement for

## their transactions and statement details. And for some

## transactions he/she has to go to bank and review all the details.

## Online banking system is more focused and developed for

## internet banking for Balance Enquiry, funds transfer, mini

## statements and everything else related to bank. This project

## reflects real life understanding of e-Banking and various

## activities performed by different roles in supply chain.

## Scope:

## An e-banking management system will be applicable

## 

## everywhere, where banking exists. It will be more efficient and

## easier way to have a Record on systems through which everyone

## can easily access it according to his/her rights as compared to

## the traditional banking system. People should be motivated to

## use e-banking management system instead of the traditional

## banking system as it contains man features and fastest

## techniques for the information transactions and display.

## Definitions and Abbreviations:

## eBMS – e-Bank Management System

## Validation- checking if something is accurate or officially

## Acceptable

## Database- collection of all the data and information managed

## by a system

## Stakeholder- A person with an interest in a project who is

## not a developer

## Visitor/ User: Anyone who is using this website or has

## active account on it

## 

## Software Requirement

## Specifications: A paper or a document that lists out all the

## features or functions of a system and the

## conditions under which it must operate.

## 

## Credentials: Some inputs needed to authorize and validate

## One’s identity

## 

## PIN: Personal Identification number

## References:

## <http://tomcat.apache.org/>

## <https://www.researchgate.net/publication/289247259_E-Banking_Management_Issues_Solutions_and_Strategies>

## <https://journals.sagepub.com/doi/abs/10.1177/2393957517736457>

## <https://www.onespan.com/blog/top-banking-regulations-security-compliance-requirements>

## <https://byjus.com/govt-exams/functions-of-bank/>

## <https://www.geeksforgeeks.org/data-flow-diagram-for-online-banking-system/>

## 

## 

## 2)Overall Description:

## 2.1. System Environment:

## 

## 2.2. System Environment Description:

## 

## The User will have Web interface and login page to visit the

## 

## eBMS system which he/she can interact with. Initial page is a

## login page for an active user to login with the right credentials.

## If login creds of user are authentic then he/she will be redirected

## to eBMS system home page where he/she can perform actions

## according to his/her requests. All of these actions are limited for

## normal user activities.

## If there are some wrong creds input are given or suspicious

## activities are detected then, warning massage will pop to alert

## user to input correct creds and log will be created for that user,

## 

## and if such activity keeps occurring then system time-out for 40

## mins will be initiated, and security mechanisms will be activated

## while creating logs.

## Authorized user will have access to his/her records and account

## details and statement/transaction history. And rights to fetch

## data from database also, under normal user restrictions he/she

## will be able to perform insert/view/delete operations for new

## entries.

## Administrator will have access to Admin panel and CMS system

## with his/her authorized credentials. Admin panel will also check

## admin creds and will validate authorized inputs. and only then

## admin will be able to access that page and do administrator

## activities like data input, output, checking logs, registering user,

## taking or providing backups, deleting users, viewing user history

## and account details etc.

## 2.3. System Functions:

## This Section provides brief descriptions and information about

## the working and functions of the system. The system will

## require back-end database MYSQL running. Various functional

## modules of the system are listed below:

## Login

## Validation

## Get Account details

## Get Customer Records

## Get Transaction/ statement history

## Registering User/Deleting User

## User Info.

## 2.3.1. User Use cases and Miss-use cases

## 🡺Use Case: Login

## Diagram:

## 

## Description: The user visits the web Interface and login uses his/her

## Credentials

## The user first chooses login option on the website if it’s an

## active user.

## The system shows login page to user where, he/she inputs

## correct credentials to login into his/her account, and if

## credentials are authenticated, he/she will be to login in to his/her

## account.

## Miss-use case: Login

## Description: The user visits the web interface and try to login with

## some malicious input or input something that system doesn’t

## recognise and cannot authenticate, which results in to system failure.

## Use Case: Validation

## Diagram:

## 

## Assumption: User has Logged in to the system.

## Description: Now that user is in the system, he/she will be at the

## home page of the eBMS system, where he/she will be able to do

## different normal user operations

## The user performs basic operation of finding something on the

## system.

## He/she will be to access search bar or can see the different

## options on the home page of his/her account.

## If user types something into the search bar to search bar, the

## results will be shown after validating the input and finding that

## keyword into the database and fetching that data according to

## that query and showing that results to the User.

## Miss-Use case: Input Validation

## Description: The User can create a malicious input to type in and

## pass it to the database with the intent to get unauthorized database.

## Use case: Get Account Details

## Diagram:

## 

## Assumptions: User has logged in to the system

## Description: User is in the system and now working on limited user

## Condition to see his/her data.

## User will pass some query to the database in simple text form to

## Get his result, for authenticated user database will show his/her

## Details.

## This whole procedure is working under the secure medium and

## Database stores every data in secure database and in encrypted

## format.

## After verifying and validating everything system shows

## requested customer details to the user.

## Miss-Use Case: get Customer Details

## Description: ill-intended user might try access another customer

## details with his/her account, by passing some malicious inputs to the

## database.

## Use case: Get customer Records

## Diagram:

## 

## Assumptions: User has logged in to the system

## Description: Now user is passing some queries to the database to get

## his records through eBMS system.

## User will pass some input to the database to get his/her records.

## According to authorised user input database will show his/her

## records to the user in presentable form,

## Again, all the transaction between user and database happens

## through secure channel.

## Miss-use case: Get Customer Records

## Description: Some User might try to access another user’s

## 

## customer records with some scripted inputs, which he/her

## doesn’t have authorisation to do so.

## Use case: Get Transaction/statement history

## Diagram:

## 

## Assumption: User has logged in to the system

## Description: User who wants their transaction/statement history from a system will go to the option of transaction history or statement

## history.

## User will give some input to eBMS system in simple text format

## and within authorised scope he/she will try to get the data from

## the database.

## After verifying all the inputs eBMS system will send that query

## to the database and database will fetch that data back to eBMS

## and user will be presented with that data.

## Miss-Use Case: Get Transaction/statement history

## Description: Some User might try to get unauthorised data while

## bypassing the security protocols with scripted inputs from the

## database.

## Use case: Registering User/Deleting User and User Info.

## Diagram:

## 

## Assumption: Admin is logging in to the portal and inputting and

## updating the database.

## Description: Admin is a person who has full control of the system.

## 

## And who manages the whole system with required updates, logging,

## monitoring

## Admin have privilege to access everything and update it or

## delete it.

## For example, admin can register user or delete user, or he/she

## can update the database of every user manually, he/she can get

## customer information or user information with web interface

## admins are allowed to use.

## Every admin of the system is asked to authenticate their

## identity just as simple use by inputting login credentials.

## Then system will verify the credentials and authorised

## admins will be able to login in to the control panel of the

## website and modify the data as they seem right, with certain

## policies.

## Miss-use case: Registering User/Deleting User and User Info.

## Description: Any user who bypasses the admin page security will be

## able to access all the database based on admin privileges, which will

## be very critical security breach. He/she might try to delete any user or

## change information about any user or get that information.

## 3)Requirements: -

## 3.1. Interface Requirements:

## Interface must be web-based interface, with easy to access

## Description, must be compatible with all the browser available

## in documentation.

## User should be comfortably accessing the information available

## on the web interface without any previous technical knowledge.

## Proper security message should be displayed at most of the

## places.

## 3.2. Performance Requirements-:

## The system running the back-end database or handling all the

## traffic of the website should be compatible enough to hold the

## General traffic.

## The system should be fast enough to meet the general

## requirements of the customer/user. And if it seems that

## system failure might happen because of some process it should

## not affect the user data or their credentials.

## 3.3. Security Requirements-:

## All the available data in the database should be protected all the

## time and login credentials stored in the database should be

## encrypted, so that even if breach occurs data should not be

## leaked.

## Every interaction between user and system should happen in

## secure environment, and should not be breached.

## The banking management system must be fully and only

## accessible to the authentic users only. Any third party

## software or another unauthorised user should not be able

## to access the system without active user or admin

## permission.

## If any of the security protocols are breached or unauthorised

## entries are logged, legal actions will be taken against such

## activities.

## Database backups and regular software updates, monitoring and

## logging should be on periodic intervals, and should be handled

## by admin or someone who has permission of admin to do this

## actions.