JSPM'S RSCOE, Department of Computer Engineering 2016-2017

SAVITRIBAI PHULE PUNE UNIVERSITY

A PROJECT REPORT ON

Enhanced Security Approach for Online User Authentication

SUBMITTED TOWARDS THE
PARTIAL FULFILLMENT OF THE REQUIREMENTS OF

BACHELOR OF ENGINEERING (Computer Engineering)

BY

Neeti Deshmukh	Exam No: B120374277
Isha Patil	Exam No: B120374287
Srinivasan Jayaraman	Exam No: B120374319
Taru Tak	Exam No: B120374320

Under The Guidance of
Prof.K.V.Deshpande

DEPARTMENT OF COMPUTER ENGINEERING

JSPMs RAJARSHI SHAHU COLLEGE OF ENGINEERING
TATHAWADE,PUNE -411033

JSPMs RAJARSHI SHAHU COLLEGE OF ENGINEERING
DEPARTMENT OF COMPUTER ENGINEERING

CERTIFICATE

This is to certify that the Project Entitled

Enhanced Security Approach for Online User Authentication

Submitted by

Neeti Deshmukh	Exam No:B120374277
Isha Patil	Exam No:B120374287
Srinivasan Jayaraman	Exam No:B120374319
Taru Tak	Exam No:B120374320

is a bonafide work carried out by Students under the supervision of Prof. K.V.Deshpande and it is submitted towards the partial fulfillment of the requirement of Bachelor of Engineering (Computer Engineering).

Prof. K.V.Deshpande
Internal Guide
Dept. of Computer Engg.

Prof. S.V.Kedar
H.O.D
Dept. of Computer Engg.

Dr. R.K.Jain
Principal
Rajarshi Shahu College of Engineering

Signature of Internal Examiner

Signature of External Examiner

PROJECT APPROVAL SHEET

A Project Titled

Enhanced Security Approach for Online User Authentication

Is successfully completed by

Neeti Deshmukh	Exam No:B120374277
Isha Patil	Exam No:B120374287
Srinivasan Jayaraman	Exam No:B120374319
Taru Tak	Exam No:B120374320

at

DEPARTMENT OF COMPUTER ENGINEERING

JSPMs RAJARSHI SHAHU COLLEGE OF ENGINEERING

SAVITRIBAI PHULE PUNE UNIVERSITY,PUNE

ACADEMIC YEAR 2016-2017

Prof. K.V.Deshpande	Prof. S.V.Kedar
Internal Guide	H.O.D
Dept. of Computer Engg.	Dept. of Computer Engg.

Abstract

Quick Response (QR) codes can be used efficiently to store small data. They are two dimensional barcodes. Smartphones can be used as QR code scanners. As the market of Smartphone is increasing day by day, the no. of applications in which QR codes are used is increasing. Even though QR codes have many advantages because of which they are very popular, there are many security risks and issues associated with them. While the user is reading the QR code in the foreground, he may be subject to many security risks in the background like running malicious code, identity theft, violation of their privacy and loss of information. In this project, a security system for QR codes that guarantees both users and generators security concerns is implemented. The system is backward compatible with current standard used for encoding QR codes. The implementation of the system and its testing is done by using an Android-based Smartphone application. It was found that the system introduces a little overhead in terms of the delay required for integrity verification and content validation.

Acknowledgments

*It gives us great pleasure in presenting the project report on **‘Enhanced Security Approach for Online User Authentication’**.*

*We would like to take this opportunity to thank our internal guide **Prof. K.V.Deshpande** for giving us all the help and guidance we needed. We are really grateful to her for her kind support. Her valuable suggestions were very helpful.*

*We are also grateful to **Prof.S.V.Kedar**, Head of Computer Engineering Department, Rajarshi Shahu College of Engineering for her indispensable support, suggestions.*

*In the end our special thanks to **Dr.R.K.Jain** for providing various resources such as laboratory with all needed software platforms, continuous Internet connection, for Our Project.*

Neeti Deshmukh
Isha Patil
Srinivasan Jayaraman
Taru Tak
(B.E. Computer Engg.)

Contents

List of Figures

List of Tables

Chapter 1

Synopsis

1.1 Project Title

Enhanced Security Approach for Online User Authentication

1.2 Project Option

INTERNAL PROJECT

1.3 Internal Guide

Prof. K.V.Deshpande

1.4 Sponsorship and External Guide

NA

1.5 Technical Keywords (As per ACM Keywords)

1. QR codes
2. Online Privacy
3. Mobile Security
4. Secured Authentication

5. One Time Password
6. Authentication
7. Smartphone
8. Security Middleware

1.6 Problem Statement

To create an application that will run on android based devices. Its primary purpose would be to make use of QR code for banking transaction.

1.7 Abstract

- Quick Response (QR) codes can be used efficiently to store small data. They are two dimensional barcodes. Smartphones can be used as QR code scanners. As the market of smartphones is increasing day by day, the no of applications in which QR codes are used is increasing. Even though QR codes have many advantages because of which they are very popular, there are many security risks and issues associated with them. While the user is reading the QR code in the foreground, he may be subject to many security risks in the background like running malicious code, identity theft, violation of their privacy and loss of information. In this project, a security system for QR codes that guarantees both users and generators security concerns is implemented. The system is backward compatible with current standard used for encoding QR codes. The implementation of the system and its testing is done by using an Android-based smartphone application. It was found that the system introduces a little overhead in terms of the delay required for integrity verification and content validation.

1.8 Goals and Objectives

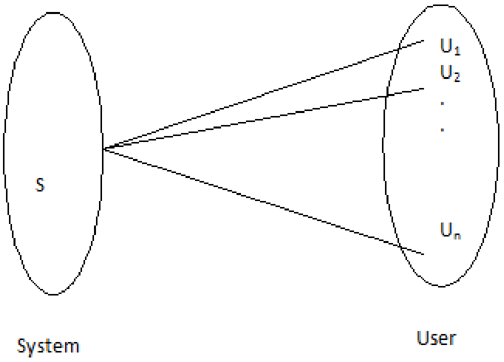
1. The main objective and motivation of the proposed system is to eliminate the use of alpha numeric passwords in online banking transaction by making use of random QR code generation.
2. The final scenario would be that a person or a firm would be able to do the transaction which would be secure from different cyber-attacks

like phishing.The user would be able to do the transaction using untrusted system.
3. We aim to have three modules that will be the main functioning units of the application. First would be the QR code generation and scanning module then AES encryption module and a final communication module. There will be two phase of a System Registration phase and login phase.
4. At the end, user would be able to use the android application and a website to do an online banking transaction which will be safe from cyber-attacks. Mainly this will be helpful for a huge and complete secure transaction.

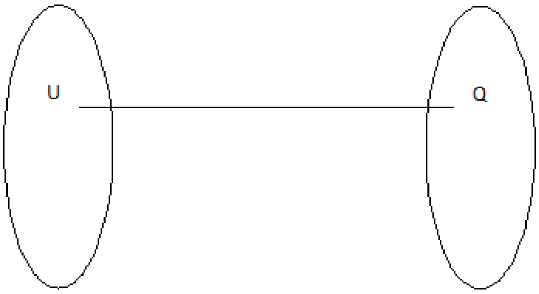
1.9 Relevant mathematics associated with the Project

Mapping

1] One system will have many users. Hence one to many relationship is observed here.



One user will be have one QR code for identification. Hence one to one relationship will be observed here.



Set Theory:

System S = Input, Output, constraint

Input

- For Register operation
  Input = User Details
  User Details D = D1, D2 Dn
  D = Username, Firstname, Lastname, Password, Email Id, Contact,

IMEI

- For Login operation
  Input = Login Credentials
  Login Credentials C = C1, C2 Cn
  C = Username, Password

Output

- For Register operation
  Output = Account Creation Summary
  Account Creation Summary = Username, Password, Token, Correct User Id, IMEI

- For Login operation
  Output = Authentication Notification

Constraints:

- Constraint C = C1, C2
  Where,
  C1 = All Servers and Client Machines should be connected in one network
  C2 = User should be logged in to the website

1.10 Names of the Journal where paper is published

1. JETIR

1.11 Review of Conference/Journal Papers supporting Project idea

1. Mukhopadhyay, S.; Argles, D., An Anti-Phishing mechanism for single sign-on based on QR-code, Information Society (i-Society), 2011 International Conference on , vol., no., pp.505,508, 27-29 June 2011

2. A.S. Narayanan. QR Codes and security solutions, International Journal of Computer Science and Telecommunications Volume 3, Issue 7, July 2012

3. Soon,TanJin.,QR Code. ,Synthesis Journal: 59-78

4. Aviel.D.Rubin.Independent OTPs, June 1995.Website- http://avirubin.com/onetime.pdf6

5. Azhar,Rizwan.Camera Based Authentication Methods. Website www.ida.liu.se/ TDDD17/old projects/2010/projects/ 011.pdf

6. Open ID Foundation, Get an Open ID. [Online]. Available: http://openid.net/get-an-openid.

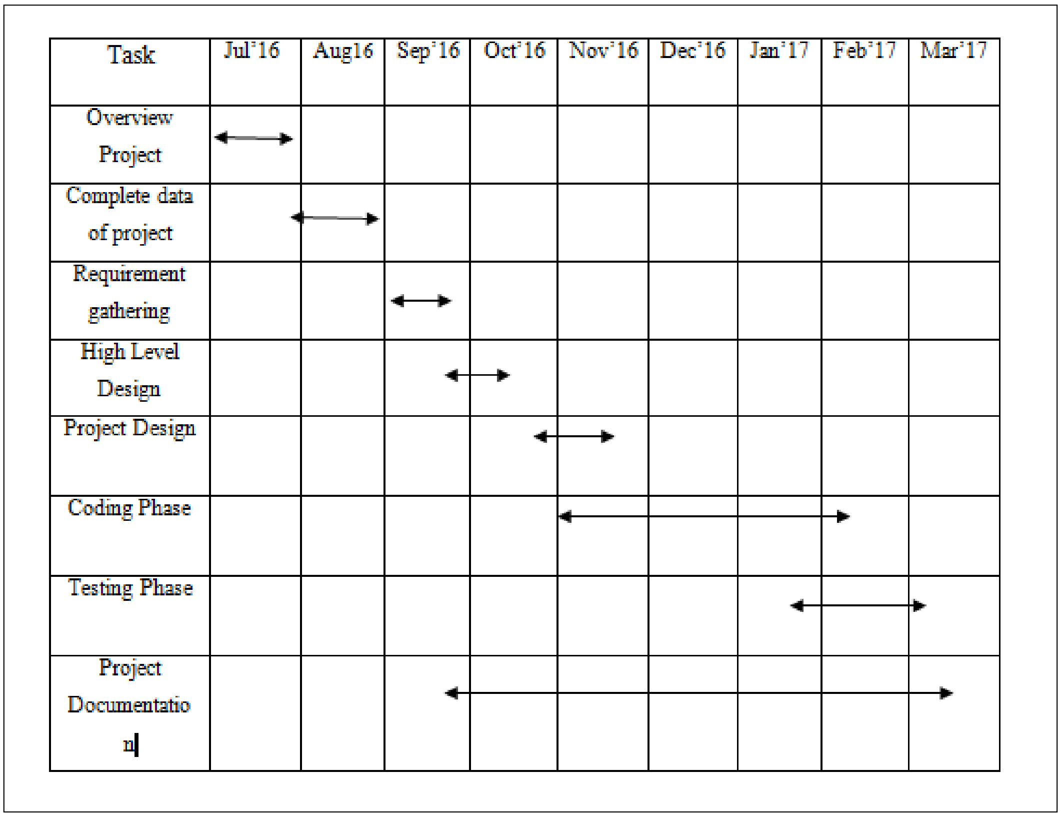
7. C.Herley and P.C van Oorschot,A research agenda acknowledging the persistence of passwords,IEEE Security and Privacy,vol.10,no. 1,pp 2836, 2012.

8. Kroenke.D, Experiencing MIS in 5/E 2014 Prentice Hall. P.696.

9. Kan T.W, C.H.Teng and M.Y.Chen, QR code based augmented reality applications in handbook of augmented reality, B.Furht Editor 2011 Springer: New York p 339-354.

10. NIST SP800-63 Electronic Authentication Guideline,NIST Special Publication V1.0 June2004

1.12 Plan of Project Execution



Task	Jul'16	Aug16	Sep'16	Oct'16	Nov'16	Dec'16	Jan'17	Feb'17	Mar'17
Overview Project	↔								
Complete data of project		↔							
Requirement gathering			↔						
High Level Design			↔	↔					
Project Design				↔	↔				
Coding Phase					↔	↔	↔	↔	
Testing Phase							↔	↔	↔
Project Documentation			↔	↔	↔	↔	↔	↔	↔

Figure 1.1: Project Execution Plan

Chapter 2

Technical Keywords

2.1 Area of Project

Cyber Security

2.2 Technical Keywords

1. QR codes
2. Online Privacy
3. Mobile Security
4. Secured Authentication
5. One Time Password
6. Authentication
7. Smartphone
8. Security Middleware

Chapter 3

Introduction

3.1 Project Idea

To create an application that will run on android based devices. Its primary purpose would be to make use of QR code for banking transaction. It would be consisting of three modules, QR code generation and scanning, AES encryption module and communication module. Two phase of System Registration phase and login phase. Firstly user will open the websites login page and will enter user ID and is sent to server. Output QR code is generated and displayed, user scans the QR code using android application and the generated QR code is sent to untrusted system.

3.2 Motivation of the Project

- Today Internet is the most widely used medium for accessing the information. On the internet, many websites are available for providing the information and also most of the services are getting Online such cloud security, banking, insurance, shopping etc. These services providing websites requires the strong authentication. Multiple authentication methods have been developed such smart card based system, one time password, SMS based OTP system and some using biometric features. Some of these authentication systems require hardware devices, and this increases the cost. Users also have their accounts at many web sites, and they have to remember passwords of all these sites.

- To make the access easier, many websites support the concept of federated identity management, in which the user having a single account can log on to the other websites by authenticating themselves to a single identity provider. Android smart phones are getting more popular. In this project, a system is proposed for secured authentication using Challenge Response, Quick Response Code, the identity provider and mobile phone, the most commonly used device. A Quick Response code is a two dimensional matrix code. It can store large amount of encrypted data, and it also has error correction ability.

3.3 Literature Survey

- Kyeongwon Choi, Changbin Lee, Woongryul Jeon, Kwangwoo Lee and Dongho Won, A Mobile based Anti-Phishing Authentication Scheme using QR code ACM SIGMOD Record, vol. 39, no. 4, pp. 1227, 2010.

  Due to the development of information and communication technology, protecting the personal authentication information from infected computer or web phishing has become a crucial task to be achieved. Using a pair of username and password authentication scheme is no more secure since attacker can collect information from web phishing and computer infection. Various malwares or intended programs attempt to capture the sensitive information from personal computer. Therefore, secure authentication scheme is required. In this paper, we propose a anti phishing single sign-on (SSO) authentication model using QR code. This scheme is secure against phishing attack and even on the distrusted computer environment.

- SyamantakMukhopadhyay, David Argles. An Anti-Phishing mechanism for Single Sign-On based on QR-Code. International Journal of Video Image Processing and Network Security IJVIPNS 10, no. 04.

  Today internet users use a single identity to access multiple services. With single sign-on (SSO), users don't have to remember separate username and password for each service provider, which helps the user to browse through the web seamlessly. SSO is however susceptible to phishing attacks. This paper describes a new anti phishing SSO model based on mobile QR code. Apart from preventing phishing attacks this new model is also safe against man in the middle attack and reply attacks

- A Novel Approach for User Authentication to Industrial Components Using QR Codes. Alexander Borisov, Robert Bosch.

First, common requirements for a secured communicationin an industrial environment will be presented. Second, thecomparison of different authentication techniques with focus onone-time passwords will be given. Third, a new model for userauthentication with QR codes will be presented. Additionally,a procedure for generating time based one-time passwords isshown. Finally, the presented approach is compared to otherpopular authentication techniques with an analysis in terms ofsecurity, deployability and usability.

- Hoba A., Podlaski K., Milczarski P. (2014) Applications of QR Codes in Secure Mobile Data Exchange. In: Kwiecie A., Gaj P., Stera P. (eds) Computer Networks. CN 2014. Communications in Computer and Information Science, vol 431. Springer, Cham

  In the paper new method of secure data transmission between mobile devices is proposed. Already existing applications demand on the user to care about secure issues himself or herself. Derived method focuses on secure channel creation using well known QR codes technology, which allows prevent the eavesdropper from interception transmitted data during connection establishing process.

Chapter 4

Problem Definition and scope

4.1 Problem Statement

To create an application that will run on android based devices. Its primary purpose would be to make use of QR code for banking transaction. It would be consisting of three modules, QR code generation and scanning, AES encryption module and communication module. Two phase of System Registration phase and login phase. Firstly user will open the websites login page and will enter user ID and is sent to server. Output QR code is generated and displayed, user scans the QR code using android application and the generated QR code is sent to untrusted system.

4.1.1 Goals and objectives

Goals and Objectives:

- The main objective and motivation of this project is to eliminate the use of alpha numeric passwords in online banking transaction by making use of random QR code generation. The final scenario would be that a person or a firm would be able to do the transaction which would be secure from different cyber-attacks like phishing. The user would be able to do the transaction using untrusted system.

- We aim to have three modules that will be the main functioning units of the application. First would be the QR code generation and scanning module then AES encryption module and a final communication module. There will be two phase of a System Registration phase and login phase.

- At the end, user would be able to use the android application and a website to do an online banking transaction which will be safe from cyber-attacks. Mainly this will be helpful for a huge and complete secure transaction.

4.1.2 Statement of scope

- Quick Response (QR) codes are two dimensional barcodes that can be used to efficiently store small amount of data. They are increasingly used in all life fields, especially with the wide spread of smart phones which are used as QR code scanners. While QR codes have many advantages that make them very popular, there are several security issues and risks that are associated with them. Running malicious code, stealing users sensitive information and violating their privacy and identity theft are some typical security risks that a user might be subject to in the background while he/she is just reading the QR code in the foreground. In this project, a security system for QR codes that guarantees both users and generators security concerns is implemented. The system is backward compatible with the current standard used for encoding QR codes. The system is implemented and tested using an Android-based smartphone application. It was found that the system introduces a little overhead in terms of the delay required for integrity verification and content validation.

4.2 Major Constraints

- Login time required may vary.

- Smartphone is required.

4.3 Methodologies of Problem solving and efficiency issues

- In this project the basic requirement is an un-trusted pc and android application for performing the required tasks

- There are two phases in the project:
  1. Registration phases
  2. Login phase

- The project executes in the following manner:
  1. The user first registers itself to the bank server with credentials name, phone number, username, IMEI number and the password. In this way the user gets registered in the bank database.
  2. In the login phase, the user logins to the website
  3. After the user logs in, a QR code is generated on the website.
  4. The android application is used for the scanning of QR code. After scanning we get the username, random number and IMEI number.
  5. The password is entered on the android application and all the details are encrypted and the QR code is generated again on the application.
  6. The newly generated application is then sent to the bank server for transaction purpose.
  7. The bank server then verifies the received QR code with the bank server and then grants the user access to the system.
  8. Advanced Encryption Standard (AES) algorithm is used for the encryption purpose.

4.4 Outcome

- User would be able to use the android application and a website to do an online banking transaction which will be safe from cyber-attacks. Mainly this will be helpful for a huge and complete secure transaction.

4.5 Applications

- Banking Sector
- Digital Lockers
- Email accounts
- Military applications

4.6 Hardware Resources Required

1. RAM 2GB or more.
2. Processor Intel Core i5 or above versions.
3. Android Smartphone with 512 MB RAM.

4.7 Software Resources Required

Platform : Windows

1. Operating System: Windows 7 or above
2. Netbeans
3. Java JDK 1.6 or above
4. Android SDK 2.3.3 or above.
5. MySQL
6. Android OS V4.0 and above

Chapter 5

Project Plan

5.1 Project Estimates

5.1.1 Reconciled Estimates

5.1.1.1 Cost Estimate

None (All software and technology used are open source and avalaible freely on the internet)

5.1.1.2 Time Estimates

1 year

5.1.2 Project Resources

- People:4
- Hardware:

Sr. No.	Parameter	Minimum Requirement
1	CPU Speed	2 GHz
2	RAM	4 GB
3	Mobile	Android

Table 5.1: Hardware Requirements

Software:

1. Operating System:
   - Operating System: Windows 7 or above
   - Netbeans
   - Java JDK 1.6 or above
   - Android SDK 2.3.3 or above.
   - MySQL

5.2 Risk Management w.r.t. NP Hard analysis

This section discusses Project risks and the approach to managing them.

5.2.1 Risk Identification and Management

Risk Management

Risk management is the identification, assessment, and prioritization of risks followed by coordinated and economical application of resources to minimize, monitor, and control the probability and/or impact of unfortunate events or to maximize the realization of opportunities. The process of risk management is an on-going iterative process. It must be repeated indefinitely. Project Risk Factors This document describes the risks that team may encounter while designing and managing the project, and the strategies and the actions that team will conduct to mitigate these risks. This document will be mainly used by the team, as part of the overall project plan, in monitoring the project. Some project risk factors are: Whether the application is beneficial for the institution as well as users. Whether the scope of the application is well defined Whether the technology being used in the application consists of new or existing software, hardware, languages and tools

RMMM Plan

The goal of the risk mitigation, monitoring and management plan is to identify as many potential risks as possible.

When all risks have been identified, they will then be evaluated to determine their probability of occurrence, and how the project will be affected if they do occur. Plans will then be made to avoid each risk, to track each risk to determine if it is more or less likely to occur, and to plan for those risks should they occur.

Risk Mitigation, Monitoring and Management

Risk: Computer Crash

Mitigation The cost associated with a computer crash resulting in a loss of data is crucial. A computer crash itself is not crucial, but rather the loss of data. If there is a loss of data Administrator will not be able to access the details of the registered users. He, then would not be able to perform his functions efficiently.

Monitoring When working on the application, the Administrator should always be aware of the stability of the computing environment he/she is working in. Any changes in the stability of the environment should be recognized and taken seriously.

Management To manage the risk of computer crash, multiple copies should be maintained, hence in the event of computer crash, recovery of data is possible.

Risk: Registered Users Resist System

Mitigation

In order to prevent this from happening, the application is developed with the users in mind. The graphic user-interface is designed in a way to make use of the program convenient and pleasurable. Also the system is designed to make minimum amount of intervention in the regular work of the user.

Monitoring

We have asked for the opinion of various outside sources throughout the development phases for our application.

Management

Should the application be resisted by the users, it will be thoroughly examined to make necessary changes. Specifically the user interface will be investigated and if necessary, revamped into a solution.

SQA Plan

Software quality assurance is an umbrella activity that is applied at each step in the software process. SQA encompasses procedures for the effective application of methods and tools, formal technical reviews, testing strategies and techniques, procedures for change control, procedures for assuring compliance to standards and measurement and reporting mechanisms.

Purpose of the SQA plan

This SQA plan provides a road map for instituting software quality assurance. This plan serves as template for SQA activities that are instituted for every software project.

Management

Management section of the application involves a user friendly graphic user interface, proper validations for every field during registration, better algorithm which ensures security of the details of the registered users.

Documentation

Purpose: The purpose of this documentation part in SQA is to describe each of the work products produced as part of the software processes.

Required software engineering documents:

The various software engineering documents that we produced in the process are as described below:

5.2.2 Risk Analysis

The risks for the Project can be analyzed within the constraints of time and quality

ID	Risk Description	Probability	Impact		
			Schedule	Quality	Overall
1	Hardware Availability	Low	Low	High	High
2	Software Availability	Low	Low	High	High

Table 5.2: Risk Table

Probability	Value	Description
High	Probability of occurrence is	$> 75\%$
Medium	Probability of occurrence is	$26 - 75\%$
Low	Probability of occurrence is	$< 25\%$

Table 5.3: Risk Probability definitions

Impact	Value	Description
Very high	$> 10\%$	Schedule impact or Unacceptable quality
High	$5 - 10\%$	Schedule impact or Some parts of the project have low quality
Medium	$< 5\%$	Schedule impact or Barely noticeable degradation in quality Low Impact on schedule or Quality can be incorporated

Table 5.4: Risk Impact definitions

5.2.3 Overview of Risk Mitigation, Monitoring, Management

Following are the details for each risk.

Risk ID	1
Risk Description	Hardware Availability
Category	Development Environment.
Source	Software requirement Specification document.
Probability	Low
Impact	High
Response	Mitigate
Strategy	Strategy
Risk Status	Occurred

Table 5.5: Risk definitions

Risk ID	2
Risk Description	software Availability
Category	Requirements
Source	Software Design Specification documentation review.
Probability	Low
Impact	High
Response	Mitigate
Strategy	Better testing will resolve this issue.
Risk Status	Identified

Table 5.6: Risk definitions

5.3 Project Schedule

5.3.1 Project task set

Major Tasks in the Project stages are:

- Task 1:Initial project plan
- Task 2:Literature Survey
- Task 3:Requirement Analysis
- Task 4: Mathematical Model
- Task 5:UML diagrams
- Task 6:Report
- Task 7:Presentation
- Task 8:Implementation
- Task 9:Testing
- Task 10:Final report

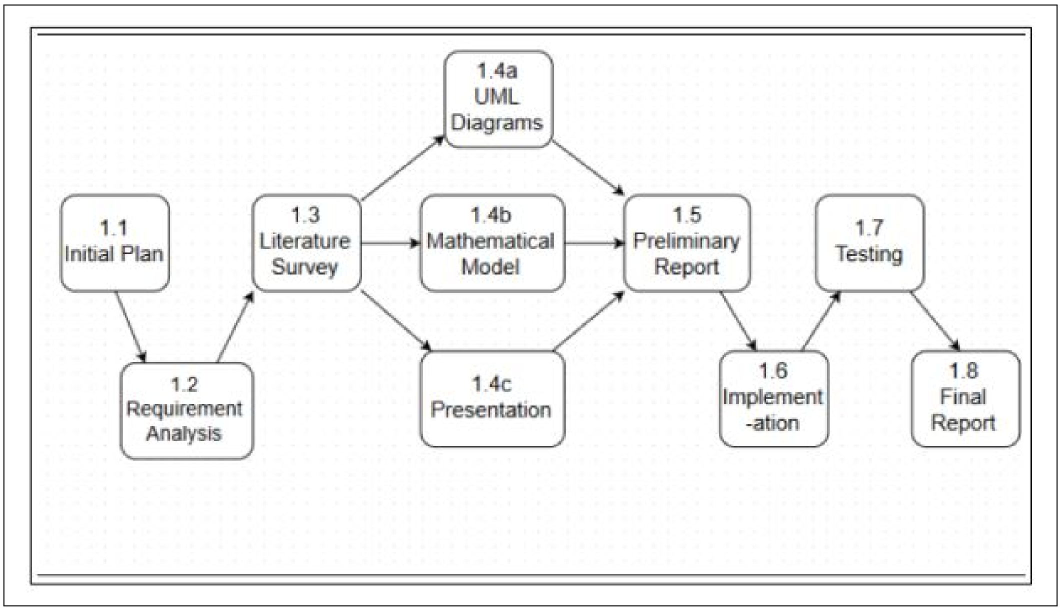


Figure 5.1: task network

5.3.2 Task network

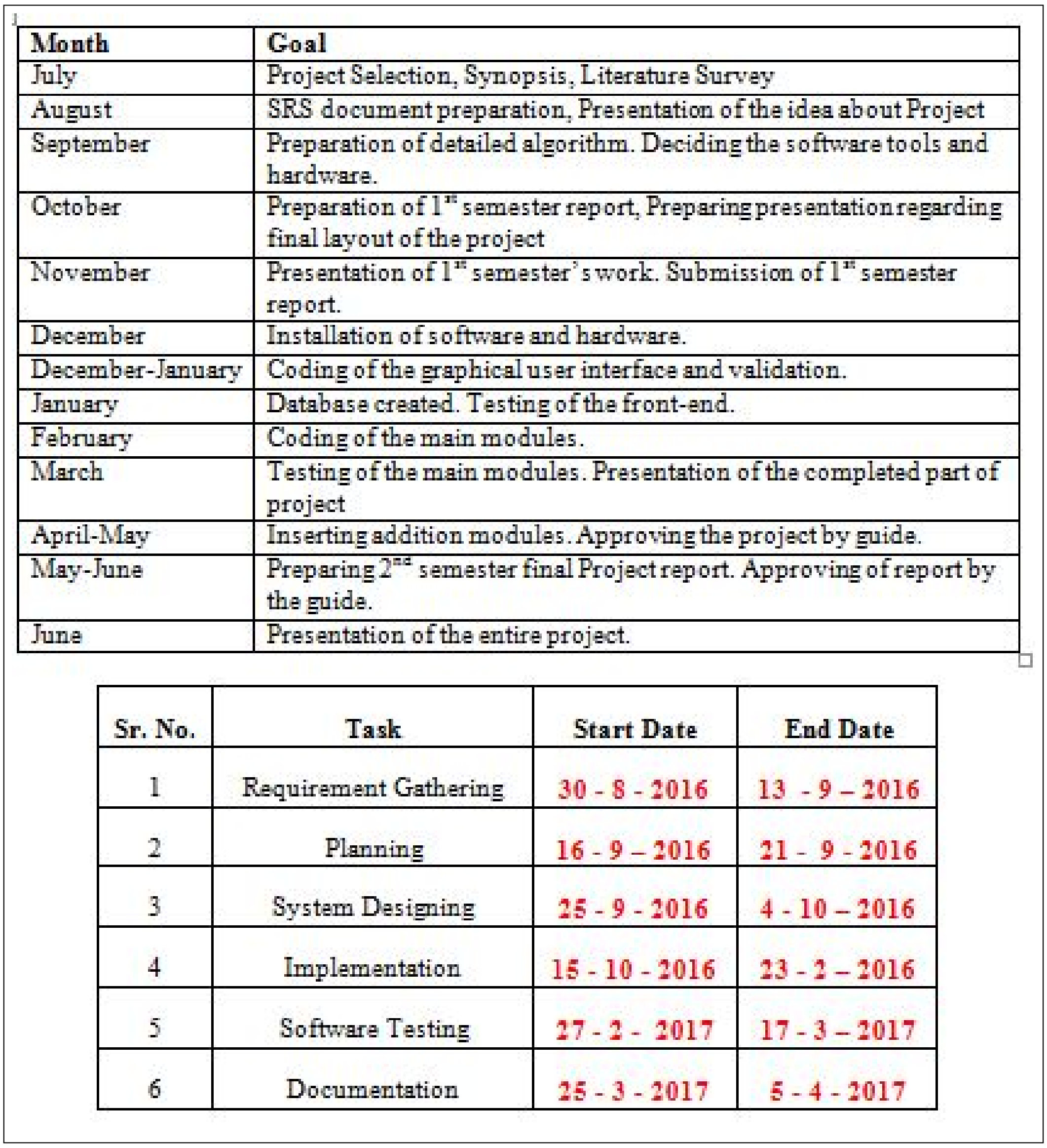
5.3.3 Timeline Chart

5.4 Team Organization

The sta organized the project team including the four member in each group. Each group is allocated one internal guide for project guidance. We have to report and submit the task given to our project guide and project coordinator.

5.4.1 Team structure

The team structure consists of four members : 1. Taru Tak 2. Srinivasan Jayaraman 3. Neeti Deshmukh 4. Isha Patil



Month	Goal
July	Project Selection, Synopsis, Literature Survey
August	SRS document preparation, Presentation of the idea about Project
September	Preparation of detailed algorithm. Deciding the software tools and hardware.
October	Preparation of 1st semester report, Preparing presentation regarding final layout of the project
November	Presentation of 1st semester's work. Submission of 1st semester report.
December	Installation of software and hardware.
December-January	Coding of the graphical user interface and validation.
January	Database created. Testing of the front-end.
February	Coding of the main modules.
March	Testing of the main modules. Presentation of the completed part of project
April-May	Inserting addition modules. Approving the project by guide.
May-June	Preparing 2nd semester final Project report. Approving of report by the guide.
June	Presentation of the entire project.

Sr. No.	Task	Start Date	End Date
1	Requirement Gathering	30 - 8 - 2016	13 - 9 – 2016
2	Planning	16 - 9 – 2016	21 - 9 - 2016
3	System Designing	25 - 9 - 2016	4 - 10 – 2016
4	Implementation	15 - 10 - 2016	23 - 2 – 2016
5	Software Testing	27 - 2 - 2017	17 - 3 – 2017
6	Documentation	25 - 3 - 2017	5 - 4 - 2017

Figure 5.2: timeline chart

5.4.2 Management reporting and communication

We have to report and submit the task given by our project guide and project co-ordinator.We need to keep record of our daily and weekly task of our project in the assessment sheet

Chapter 6

Software requirement specification

6.1 Introduction

6.1.1 Purpose and Scope of Document

The purpose of this SRS document is to provide a detailed overview of our software product Enhanced Security Approach For Online User Authentication,its parameters and goals.This document describes the projects target audience,user interface,hardware and software requirements.It defines how our client,team and audience see the product and its functionality.

6.1.2 Overview of responsibilities of Developer

What all activities carried out by developer?

6.2 Usage Scenario

This section provides various usage scenarios for the system to be developed.

6.2.1 User profiles

The profiles of all user categories are described here.(Actors and their Description)

6.2.2 Use-cases

All use-cases for the software are presented. Description of all main Use cases using use case template is to be provided.

Sr No.	Use Case	Description	Actors	Assumptions
1	Use Case 1	Description	Actors	Assumption

Table 6.1: Use Cases

6.2.3 Use Case View

Use Case Diagram. Example is given below

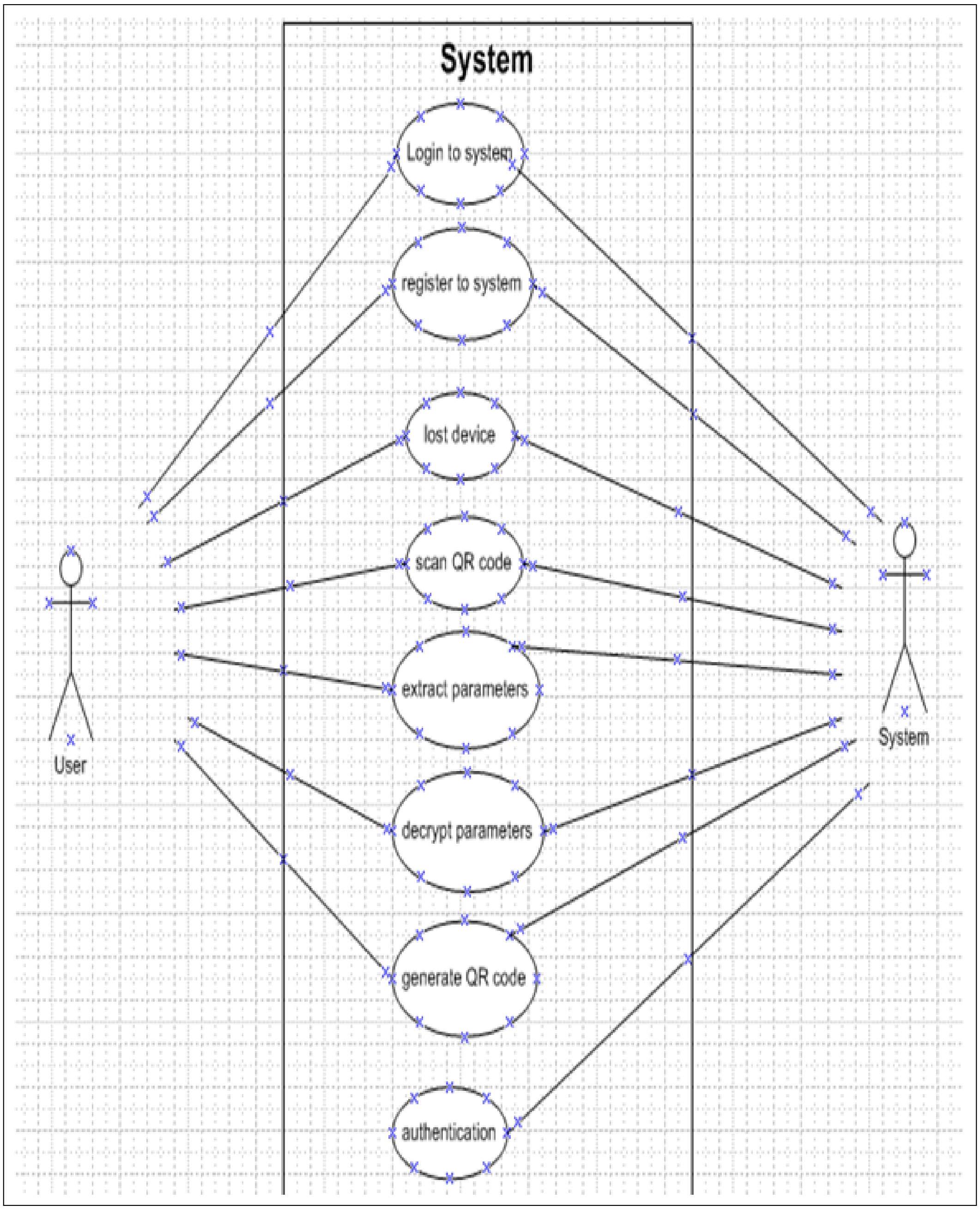


Figure 6.1: Use case diagram

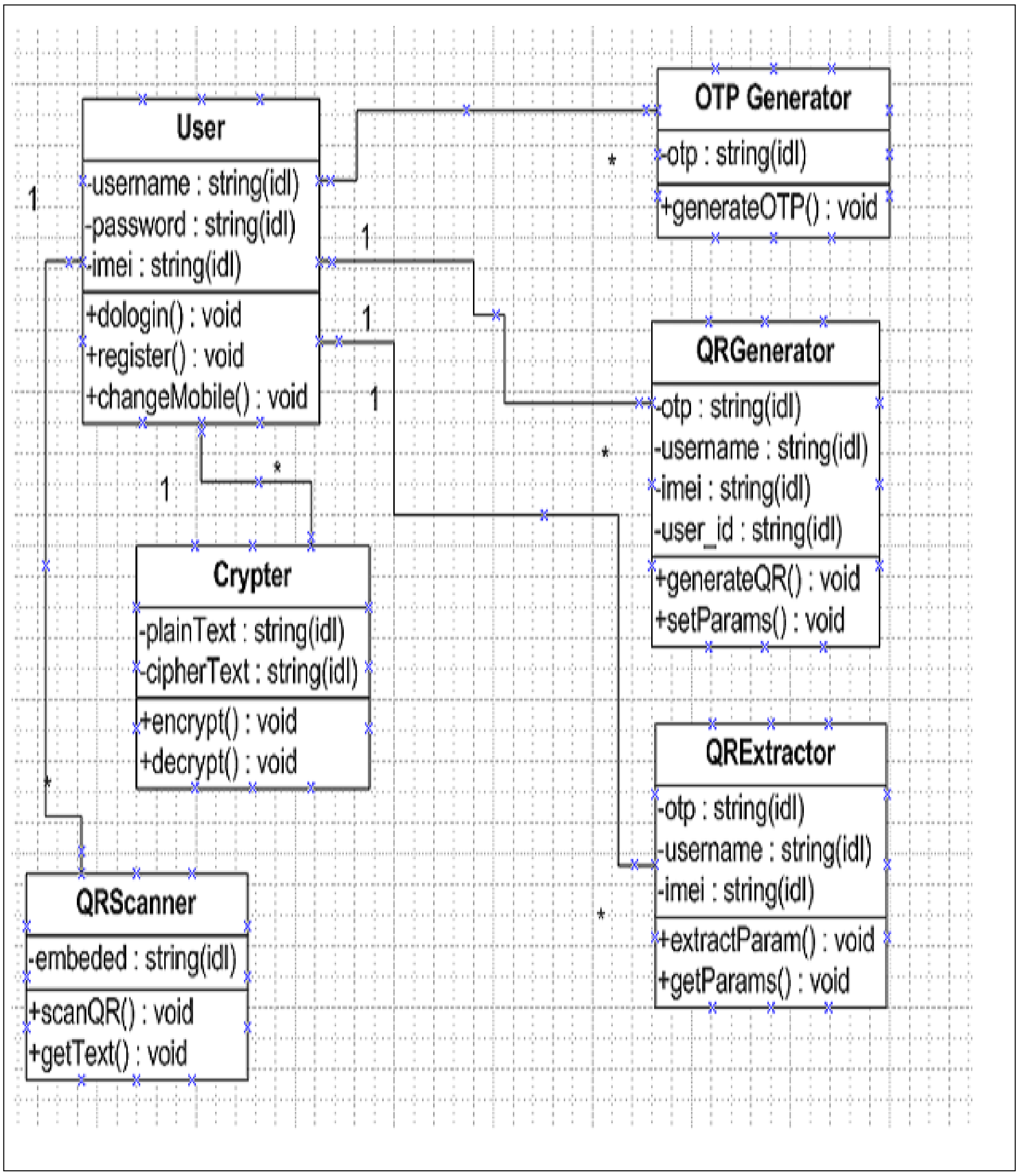


Figure 6.2: class diagram

6.3 Data Model and Description

6.3.1 Data Description

Data objects that will be managed/manipulated by the software are described in this section. The database entities or files or data structures required to be described. For data objects details can be given as below

6.3.2 Data objects and Relationships

Data objects and their major attributes and relationships among data objects are described using an ERD- like form.

6.3.3 Data Flow Diagram

6.3.3.1 Level 0 Data Flow Diagram

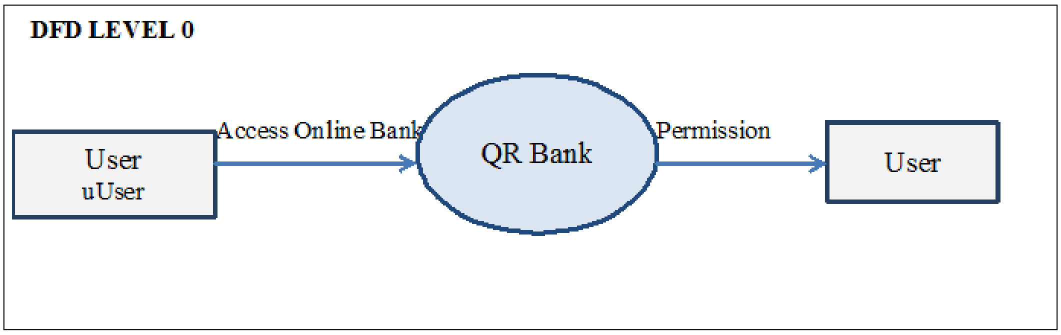


Figure 6.3: DFD level 0

6.3.3.2 Level 1 Data Flow Diagram

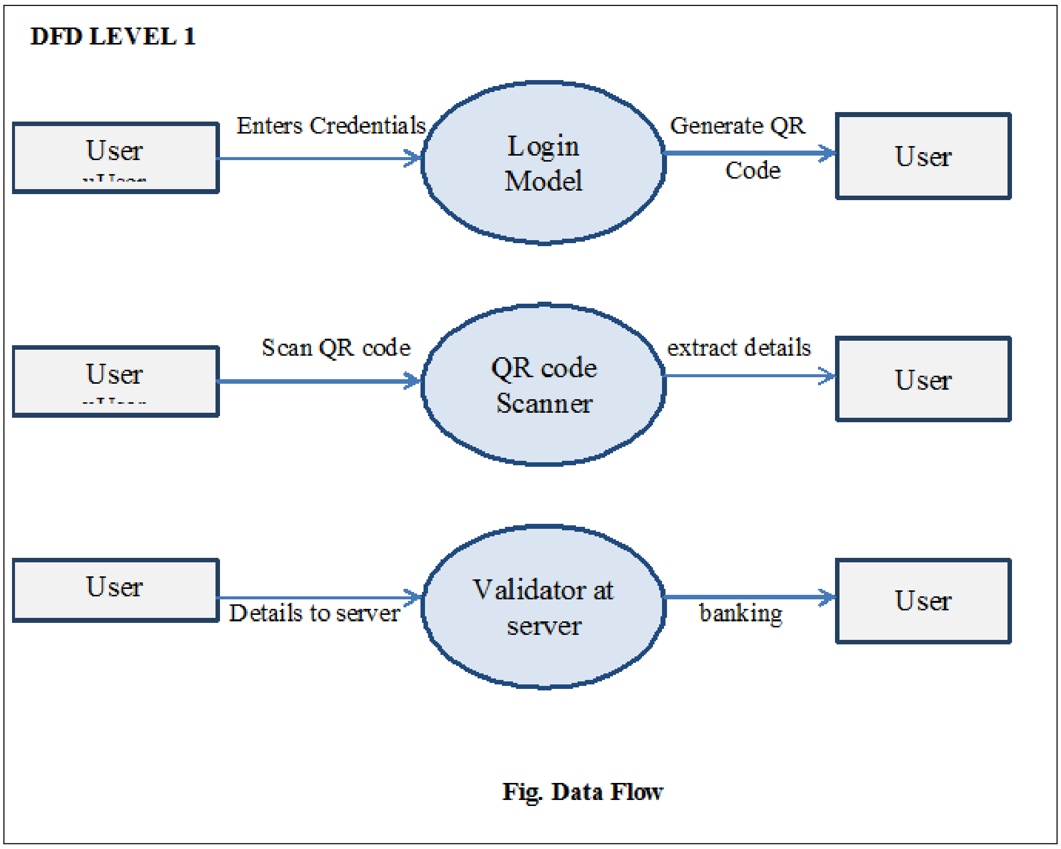


Figure 6.4: DFD level 1

6.4 Functional Model and Description

A description of each major software function, along with data flow (structured analysis) or class hierarchy (Analysis Class diagram with class description for object oriented system) is presented.

6.4.1 Activity Diagram:

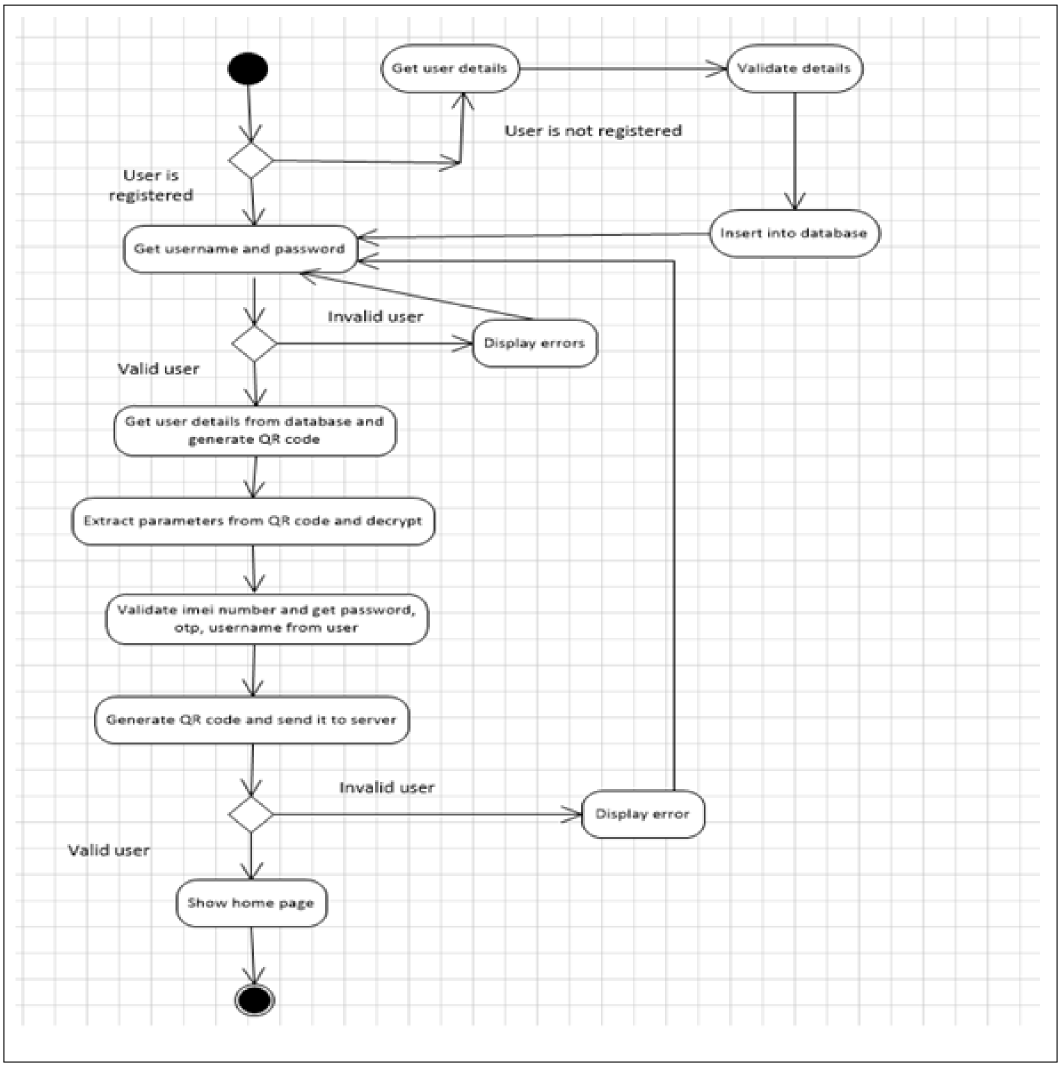

Get user details
Validate details
User is not registered
User is registered
Get username and password
Insert into database
Invalid user
Display errors
Valid user
Get user details from database and generate QR code
Extract parameters from QR code and decrypt
Validate imei number and get password, otp, username from user
Generate QR code and send it to server
Invalid user
Display error
Valid user
Show home page

Figure 6.5: activity diagram

6.4.2 Non Functional Requirements:

- Interface Requirements
- Performance Requirements

- Software quality attributes such as availability [related to Reliability], modifiability [includes portability, reusability, scalability] , performance, security, testability and usability[includes self adaptability and user adaptability]

6.4.3 Design Constraints

- Registration Data Collection and preprocessing.
- Design database for storage of user credential.
- Installation of application in mobile phone.
- encryption and decryption of data.
- increased time to login.

6.4.4 Software Interface Description

The software interface(s)to the outside world is(are) described. The requirements for interfaces to other devices/systems/networks/human are stated.

- Java (1.6 and above) : Java is used as a front end programming language owned by Oracle Inc.
- SQL : SQL is a backend querying language which is used to store data in structured format.
- Net Beans/Eclipse : This is the IDE which is being used.
- Windows : Windows is the operating system which is being used with versions XP and above..
- Latex : Used for documentation purpose

Chapter 7

Detailed Design Document using Appendix A and B

7.1 Introduction

Today Internet is the most widely used medium for accessing the information. On the internet, many websites are available for providing the information and also most of the services are getting Online such cloud security, banking, insurance, shopping etc. These services providing websites requires the strong authentication. Multiple authentication methods have been developed such smart card based system, one time password, SMS based OTP system and some using biometric features. Some of these authentication systems require hardware devices, and this increases the cost. Users also have their accounts at many web sites, and they have to remember passwords of all these sites. To make the access easier, many websites support the concept of federated identity management, in which the user having a single account can log on to the other websites by authenticating themselves to a single identity provider. Android smart phones are getting more popular. In this paper, a system is proposed for secured authentication using Challenge Response, Quick Response Code, the identity provider and mobile phone, the most commonly used device. A Quick Response code is a two dimensional matrix code. It can store large amount of encrypted data, and it also has error correction ability.

7.2 Architectural Design

The following are the points that mention the overall working of the proposed application:

A mobile banking transaction on untrusted system.
Server adds session id, random number and timestamp and creates QR code.
Generates and scans QR code using android application.
Users password along with generated session id, random number and timestamp is encrypted and a new QR code is generated.
User transfers the image to the untrusted computer.
The transferred QR code along with user id is entered on the website home page.
If verified then transaction proceeds.

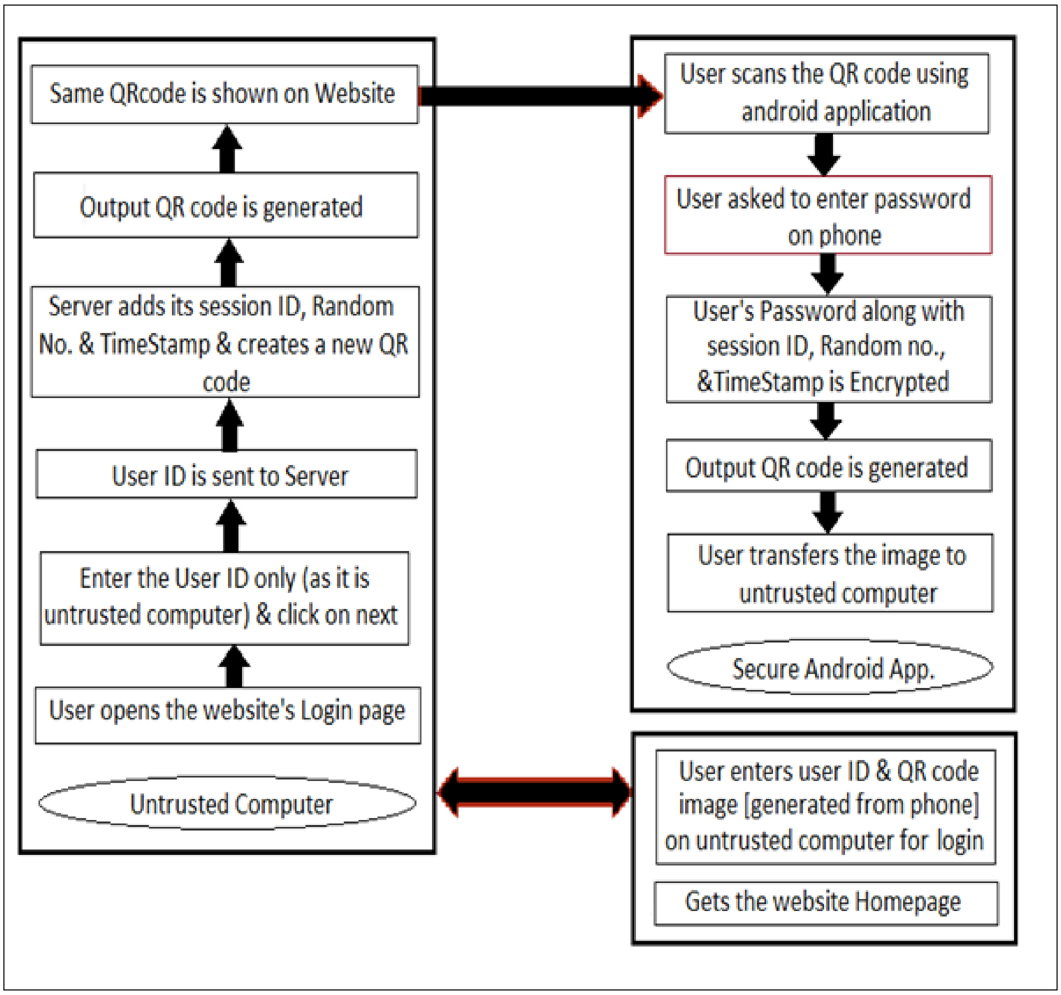

Same QRcode is shown on Website
Output QR code is generated
Server adds its session ID, Random No. & TimeStamp & creates a new QR code
User ID is sent to Server
Enter the User ID only (as it is untrusted computer) & click on next
User opens the website's Login page
Untrusted Computer
User scans the QR code using android application
User asked to enter password on phone
User's Password along with session ID, Random no., &TimeStamp is Encrypted
Output QR code is generated
User transfers the image to untrusted computer
Secure Android App.
User enters user ID & QR code image [generated from phone] on untrusted computer for login
Gets the website Homepage

Figure 7.1: Architecture diagram

7.3 Data design (using Appendices A and B)

A Data design is used to describe all the data structure which contains internal, global as well as temporary data structure.

7.3.1 Internal software data structure

When java classes will send the result of the customer credential from database which sent to a login of an particular user for identifying authorized user for accessing particular data by using various internal data structures.

7.3.2 Global data structure

As java class send register user data from database for accessing data it can record keystroke by using various algorithm data can be encrypted and decrypted data.

7.3.3 Temporary data structure

We are not using any temporary data structure in this project.

7.3.4 Database description

MySQL is the database used in keystroke project for storing register user data for future data accessing using user name and password credentials

7.4 Component Design

Class diagrams, Interaction Diagrams, Algorithms. Description of each component description required.

7.4.1 Class Diagram

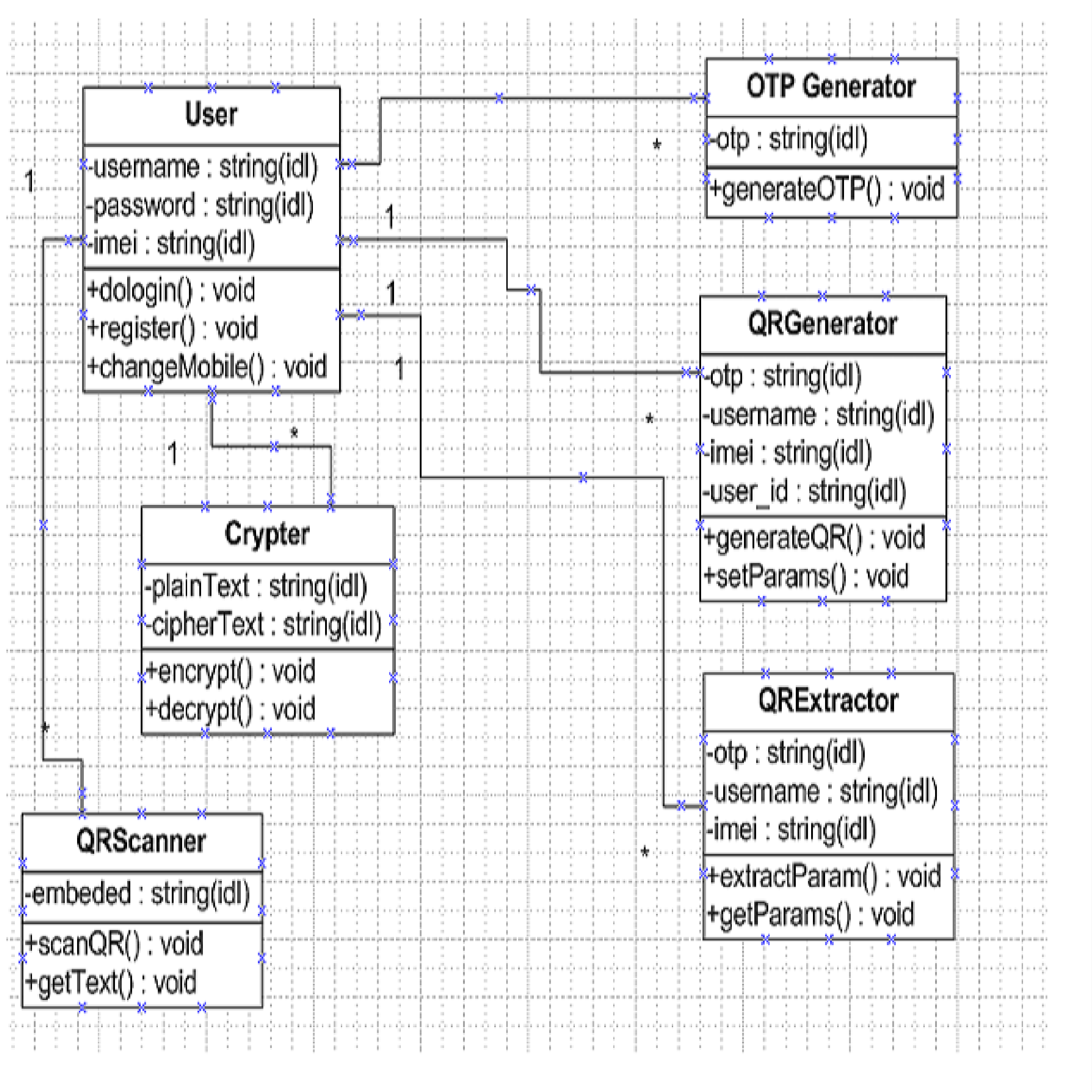


Figure 7.2: Class Diagram

Chapter 8

Project Implementation

8.1 Introduction

- Today Internet is the most widely used medium for accessing the information. On the internet, many websites are available for providing the information and also most of the services are getting Online such cloud security, banking, insurance, shopping etc. These services providing websites requires the strong authentication. Multiple authentication methods have been developed such smart card based system, one time password, SMS based OTP system and some using biometric features. Some of these authentication systems require hardware devices, and this increases the cost. Users also have their accounts at many web sites, and they have to remember passwords of all these sites.

- To make the access easier, many websites support the concept of federated identity management, in which the user having a single account can log on to the other websites by authenticating themselves to a single identity provider. Android smart phones are getting more popular. In this paper, a system is proposed for secured authentication using Challenge Response, Quick Response Code, the identity provider and mobile phone, the most commonly used device. A Quick Response code is a two dimensional matrix code. It can store large amount of encrypted data, and it also has error correction ability.

8.2 Tools and Technologies Used

- NetBeans
  NetBeans is a software development platform written in Java. The

NetBeans Plat-form allows applications to be developed from a set of modular software components called modules. Applications based on the NetBeans Platform, including the Net-Beans integrated development environment (IDE), can be extended by third party developers. The NetBeans IDE is primarily intended for development in Java,but also supports other languages, in particular PHP, C/C++ and HTML5. NetBeans is cross-platform and runs on Microsoft Windows, Mac OS X, Linux, Solaris and other platforms supporting a compatible JVM.NetBeans platform provides good and easy support to create web applications.It provides support to Berkeley Parser which we have used for parsing.Interactive user interfaces can be design using NetBeans.NetBeans has a great support to load and store various types of data.

- JDK
  Java is used to write and run computer programs and Apps. To run Java programs on Windows you need to install the Java Runtime En vironment (JRE). To write Java programs on Windows you need to install the Java Development Kit (JDK). The JDK includes the JRE. The JDK is required for Java Integrated Development Environ-ments (IDEs).IDEs make writing, testing and debugging software easier.

- JSP
  JSP ie. Javascript was used to create web application. JavaScript is the programming language of HTML and the Web.Programming makes computers do what you want them to do.JavaScript is easy to learn.

8.3 Methodologies/Algorithm Details

8.3.1 Methodology

- In this project the basic requirement is an un-trusted pc and android application for performing the required tasks

- There are two phases in the project:
  1. Registration phases
  2. Login phase

- The project executes in the following manner:
  1. The user first registers itself to the bank server with credentials name, phone number, username, IMEI number and the password. In this way the user gets registered in the bank database.
  2. In the login phase, the user logins to the website

3. After the user logs in, a QR code is generated on the website.
4. The android application is used for the scanning of QR code. After scanning we get the username, random number and IMEI number.
5. The password is entered on the android application and all the details are encrypted and the QR code is generated again on the application.
6. The newly generated application is then sent to the bank server for transaction purpose.
7. The bank server then verifies the received QR code with the bank server and then grants the user access to the system.
8. Advanced Encryption Standard (AES) algorithm is used for the encryption purpose.

8.3.2 AES

- The Advanced Encryption Standard or AES is a symmetric block cipher used by the U.S. government to protect classified information and is implemented in software and hardware throughout the world to encrypt sensitive data.

- AES comprises three block ciphers, AES-128, AES-192 and AES-256. Each cipher encrypts and decrypts data in blocks of 128 bits using cryptographic keys of 128-, 192- and 256-bits, respectively. (Rijndael was designed to handle additional block sizes and key lengths, but the functionality was not adopted in AES.) Symmetric or secret-key ciphers use the same key for encrypting and decrypting, so both the sender and the receiver must know and use the same secret key. All key lengths are deemed sufficient to protect classified information up to the "Secret" level with "Top Secret" information requiring either 192- or 256-bit key lengths. There are 10 rounds for 128-bit keys, 12 rounds for 192-bit keys, and 14 rounds for 256-bit keys – a round consists of several processing steps that include substitution, transposition and mixing of the input plaintextand transform it into the final output of ciphertext.

- Various researchers have published attacks against reduced-round versions of the Advanced Encryption Standard, and a research paper published in 2011 demonstrated that using a technique called a biclique attack could recover AES keys faster than a brute-force attack by a factor of between three and five, depending on the cipher version. Even this attack, though, does not threaten the practical use of AES due to its high computational complexity.

8.4 Verification and Validation for Acceptance

In our system verification is done to check the user is valid user or not weather the user credential is correct than user will access data ,user credentials is check from database ,when new user can register the data is stored in an database and this data can be retrieved when login in existing user by using this various encryption decryption algorithm.

Chapter 9

Software Testing

9.1 Type of Testing Used

- Unit Testing
  Unit testing is the testing of an individual unit or group of related units. It falls under the class of white box testing. It is often done by the programmer to test that the unit he/she has implemented is producing expected output against given input.

- Integration testing
  Integration testing is testing in which a group of components are combined to produce output. Also, the interaction between software and hardware is tested in integration testing if software and hardware components have any relation. It may fall under both white box testing and black box testing.

- Functional Testing
  Functional testing is the testing to ensure that the specified functionality required in the system requirements works. It falls under the class of black box testing.

- System Testing
  System testing is the testing to ensure that by putting the software in different environments (e.g., Operating Systems) it still works. System testing is done with full system implementation and environment. It falls under the class of black box testing.

- Stress Testing
  Stress testing is the testing to evaluate how system behaves under un-

favourable conditions. Testing is conducted at beyond limits of the specifications. It falls under the class of black box testing.

- Performance Testing
  Performance testing is the testing to assess the speed and effectiveness of the system and to make sure it is generating results within a specified time as in performance requirements. It falls under the class of black box testing.

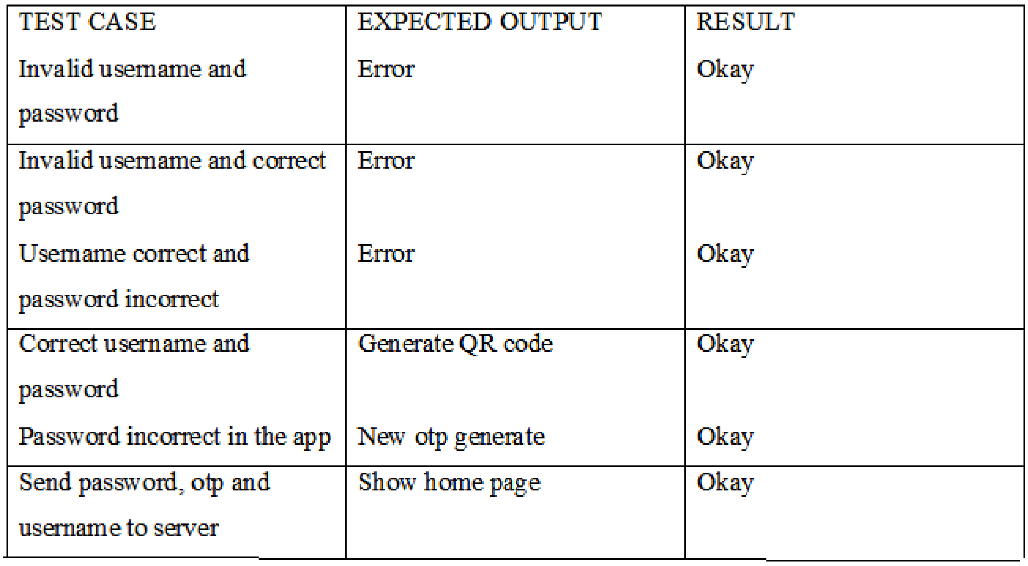
- Usability Testing
  Usability testing is performed to the perspective of the client, to evaluate how the GUI is user-friendly? How easily can the client learn? After learning how to use, how proficiently can the client perform? How pleasing is it to use its design? This falls under the class of black box testing.

- Acceptance Testing
  Acceptance testing is often done by the customer to ensure that the delivered product meets the requirements and works as the customer expected. It falls under the class of black box testing.

- Regression Testing
  Regression testing is the testing after modification of a system, component, or a group of related units to ensure that the modification is working correctly and is not damaging or imposing other modules to produce unexpected results. It falls under the class of black box testing.

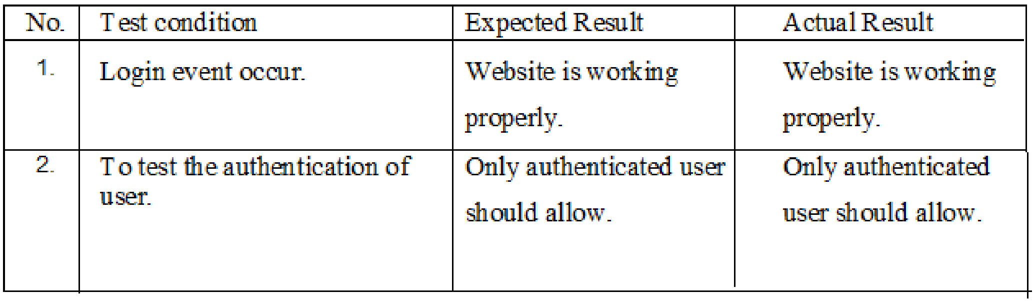
- Beta Testing
  Beta testing is the testing which is done by end users, a team outside development, or publicly releasing full pre-version of the product which is known as beta version. The aim of beta testing is to cover unexpected errors. It falls under the class of black box testing.

9.2 Test Cases and Test Results



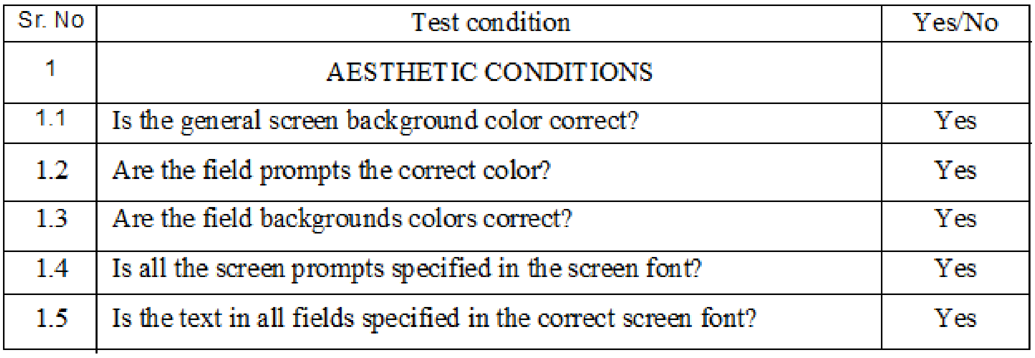
TEST CASE	EXPECTED OUTPUT	RESULT
Invalid username and password	Error	Okay
Invalid username and correct password	Error	Okay
Username correct and password incorrect	Error	Okay
Correct username and password	Generate QR code	Okay
Password incorrect in the app	New otp generate	Okay
Send password, otp and username to server	Show home page	Okay

- Login test cases



No.	Test condition	Expected Result	Actual Result
1.	Login event occur.	Website is working properly.	Website is working properly.
2.	To test the authentication of user.	Only authenticated user should allow.	Only authenticated user should allow.

- GUI test cases



Sr. No	Test condition	Yes/No
1	AESTHETIC CONDITIONS	
1.1	Is the general screen background color correct?	Yes
1.2	Are the field prompts the correct color?	Yes
1.3	Are the field backgrounds colors correct?	Yes
1.4	Is all the screen prompts specified in the screen font?	Yes
1.5	Is the text in all fields specified in the correct screen font?	Yes

2	VALIDATION CONDITION	
2.1	Is the user required to fix entries which have failed validation test?	Yes
2.2	Does the failure of validation on every field cause a sensible user error message?	Yes
2.3	Do all mandatory fields require user input?	Yes

3	NAVIGATION CONDITIONS	
3.1	Can the screen be accessed correctly from the menu?	Yes
3.2	Can all screens accessible via buttons on this screen be accessed correctly?	Yes

4	USABILITY CONDITIONS	
4.1	Is all data entry required in the correct format?	Yes
4.2	Have the menu options which applied to your screen got fast keys associated and should they have?	No
4.3	Is there default button specified in the screen?	Yes

5	DATA INTEGRITY CONDITIONS	
5.1	Is the data saved when the window is closed by double clicking on the close box?	Yes
5.2	If numeric fields except negative values can these be stored correctly on the database and does it make sense for the field to accept negative numbers.	No

Chapter 10

Results

10.1 Screen shots and Outputs

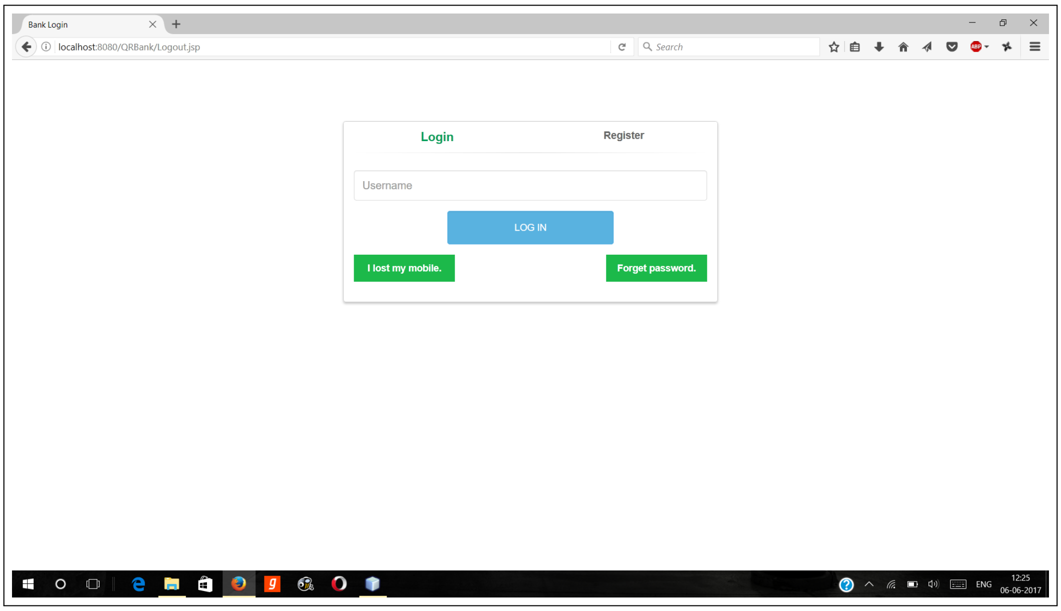


Figure 10.1: Website login page

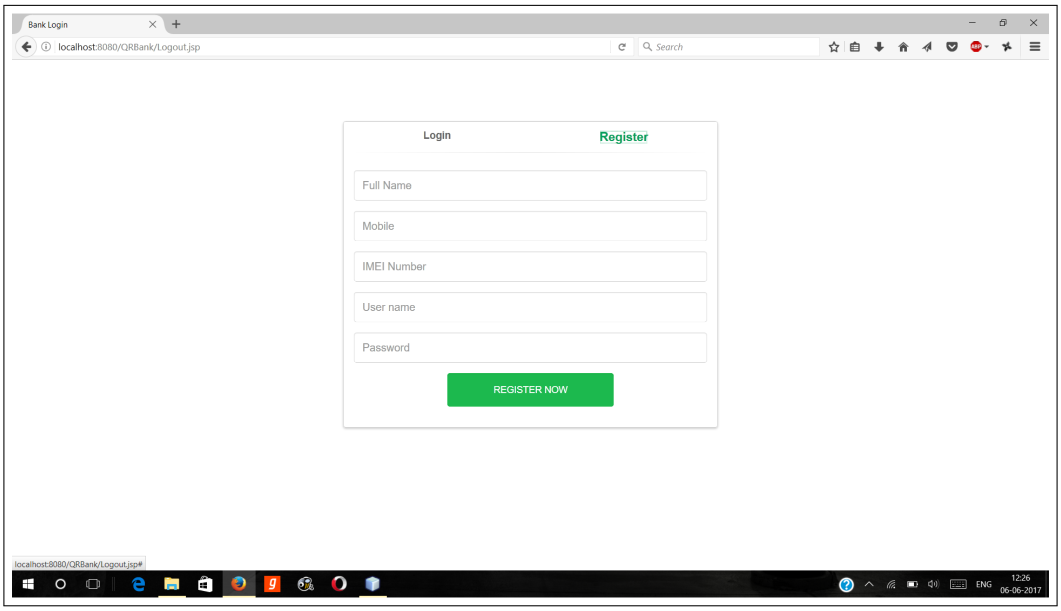


Figure 10.2: Website register page

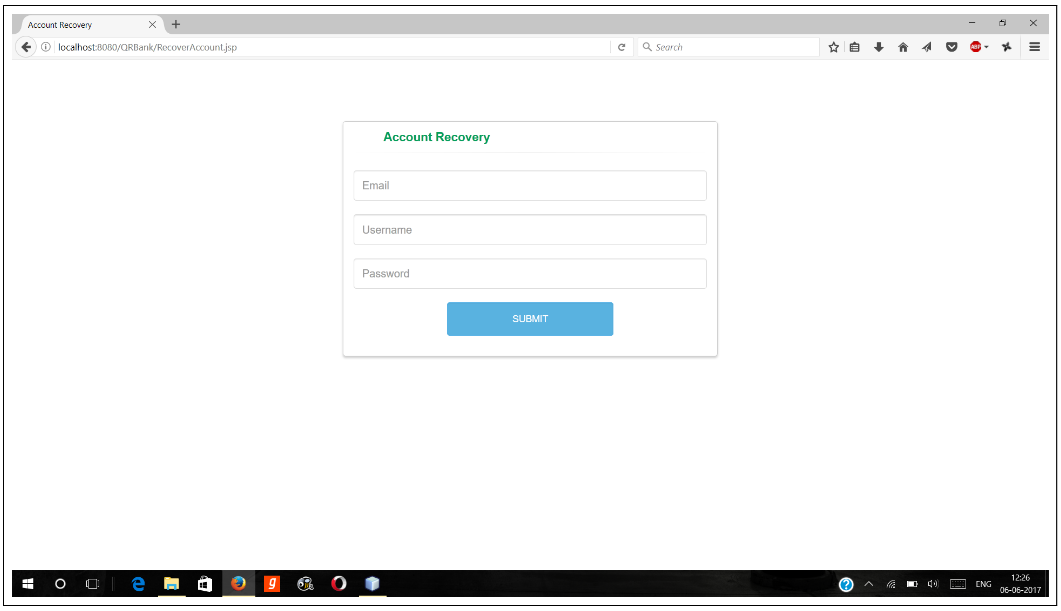


Figure 10.3: Website account recovery

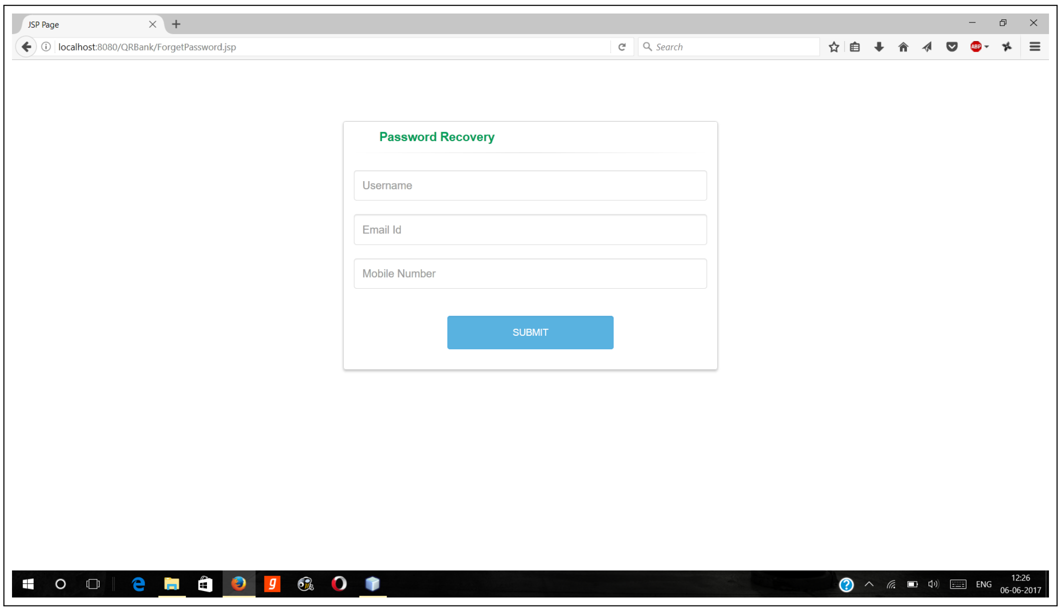
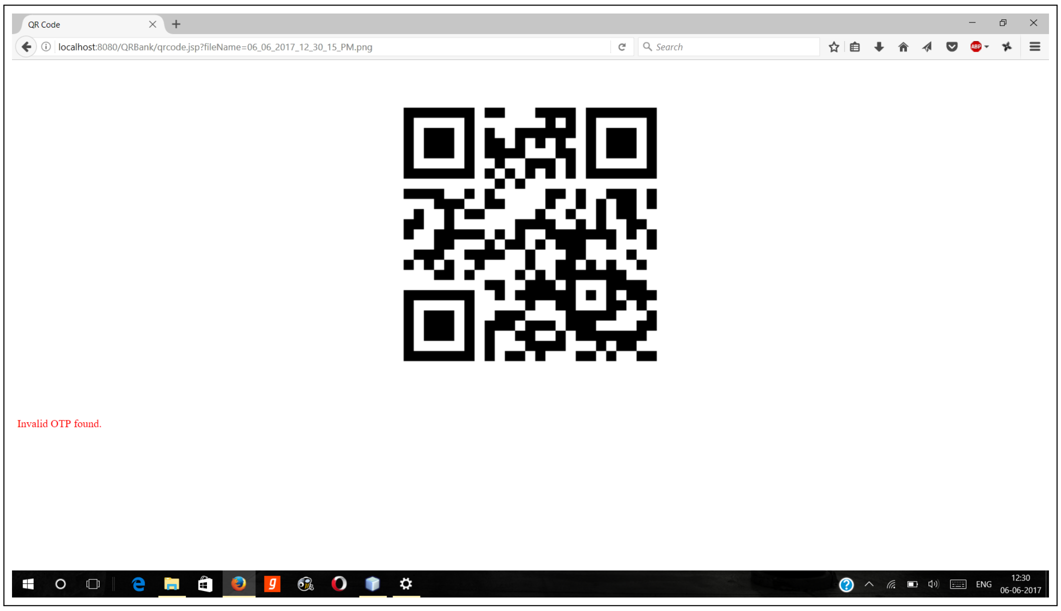


Figure 10.4: Website password recovery


QR Code
localhost:8080/QRBank/qrcode.jsp?fileName=06_06_2017_12_30_15_PM.png
Search
ENG
12:30
06-06-2017

Invalid OTP found.

Figure 10.5: Website QR code

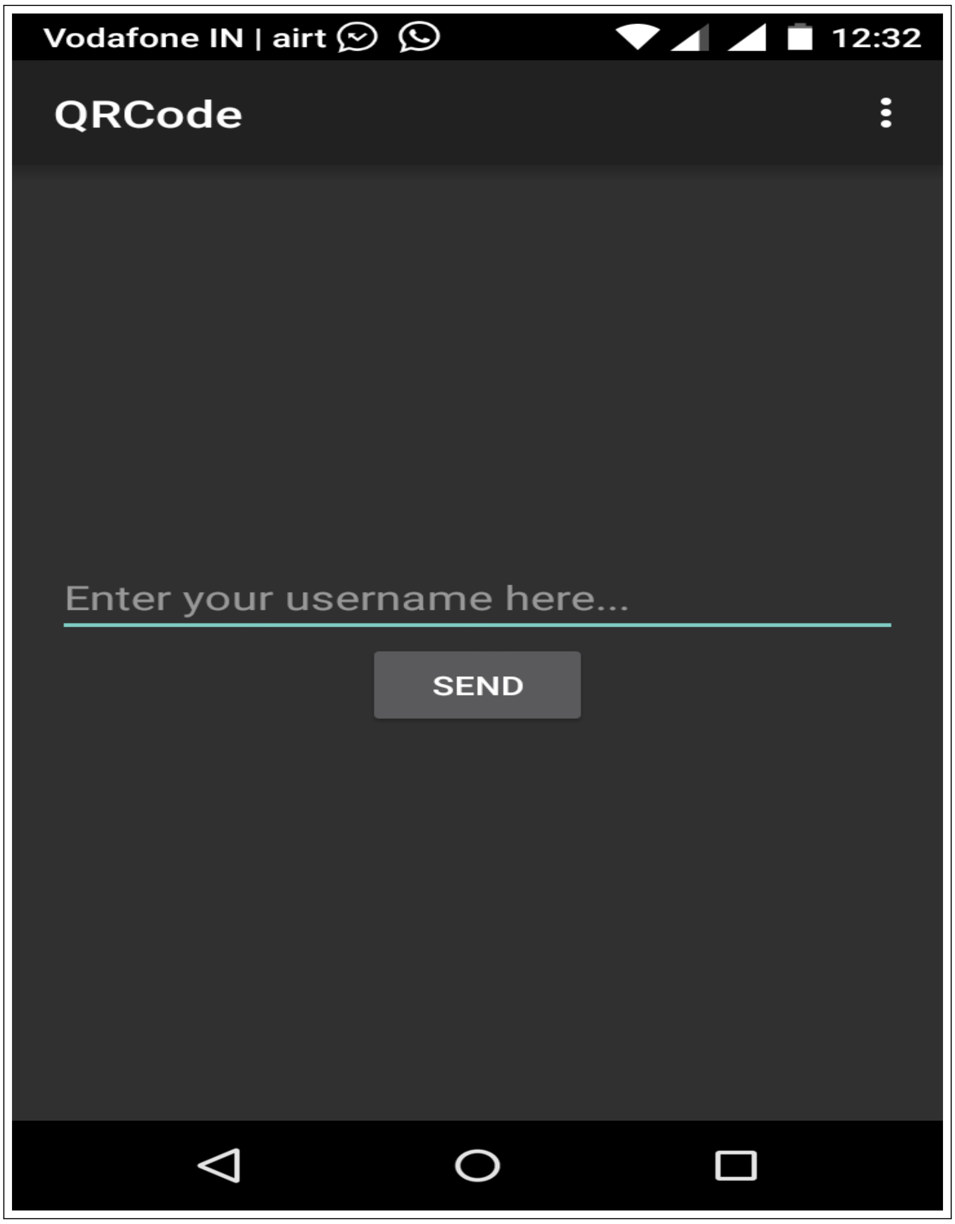
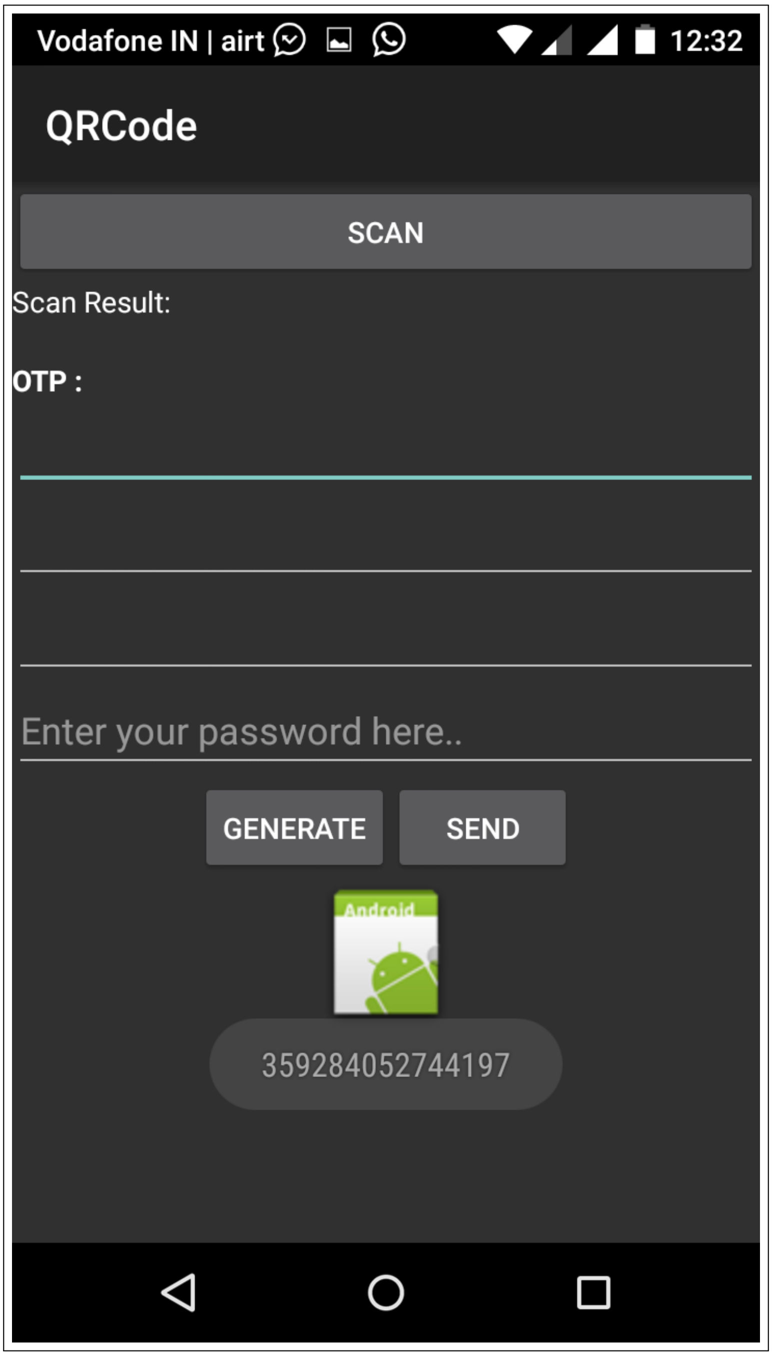


Figure 10.6: App login



Vodafone IN | airt 12:32

QRCode

SCAN

Scan Result:

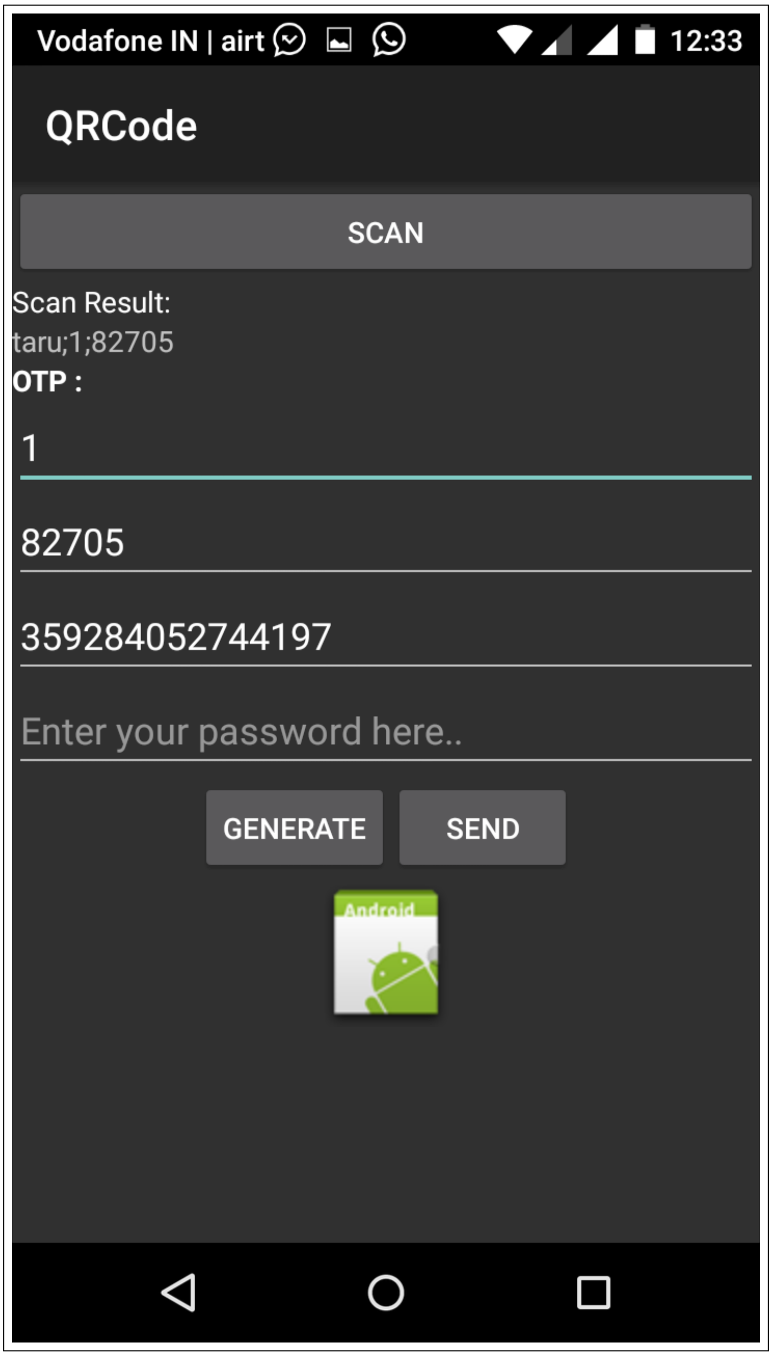
OTP :

Enter your password here..

GENERATE SEND

359284052744197

Figure 10.7: App scanner interface



Scan Result:

taru;1;82705

OTP :

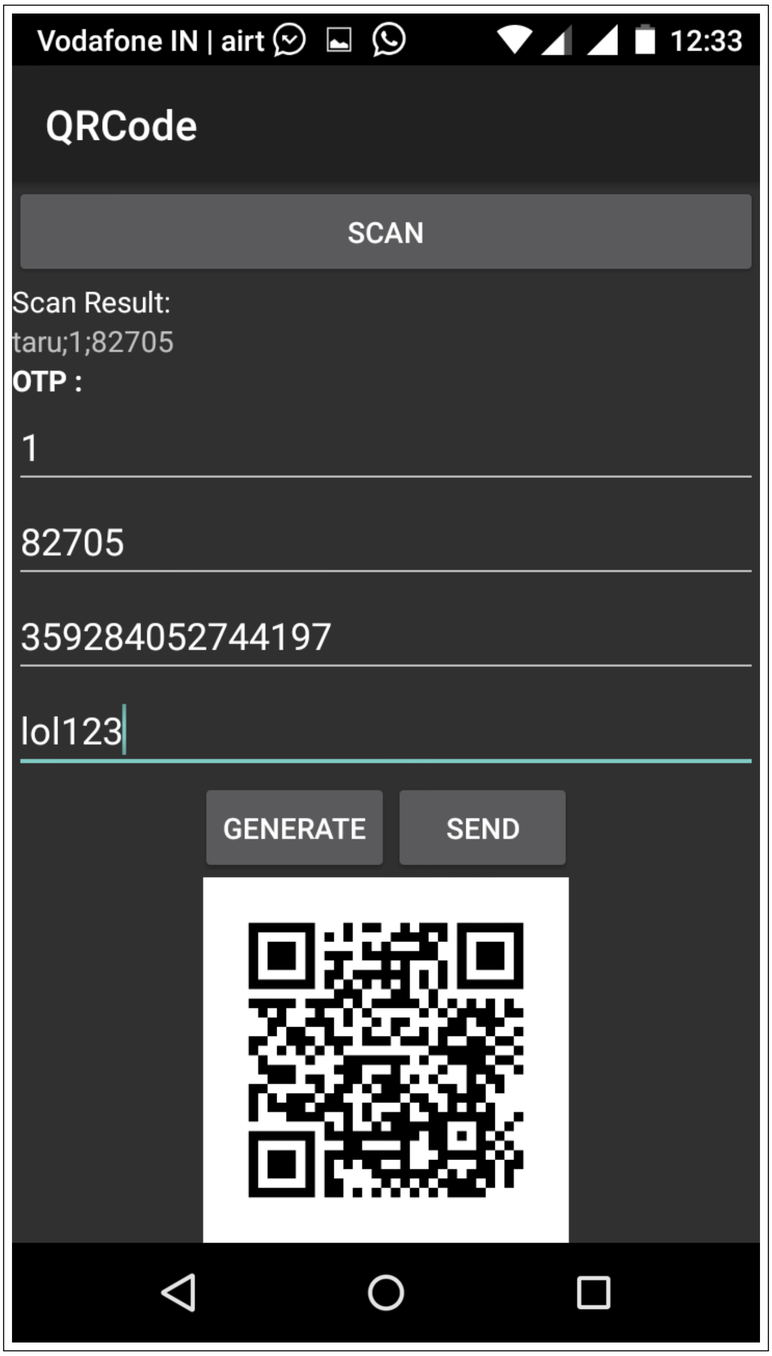
1

82705

359284052744197

Enter your password here..

Figure 10.8: App scanner interface2



Vodafone IN | airt

12:33

QRCode

Scan Result:

taru;1;82705

OTP :

1

82705

359284052744197

lol123

Figure 10.9: App QR code generated

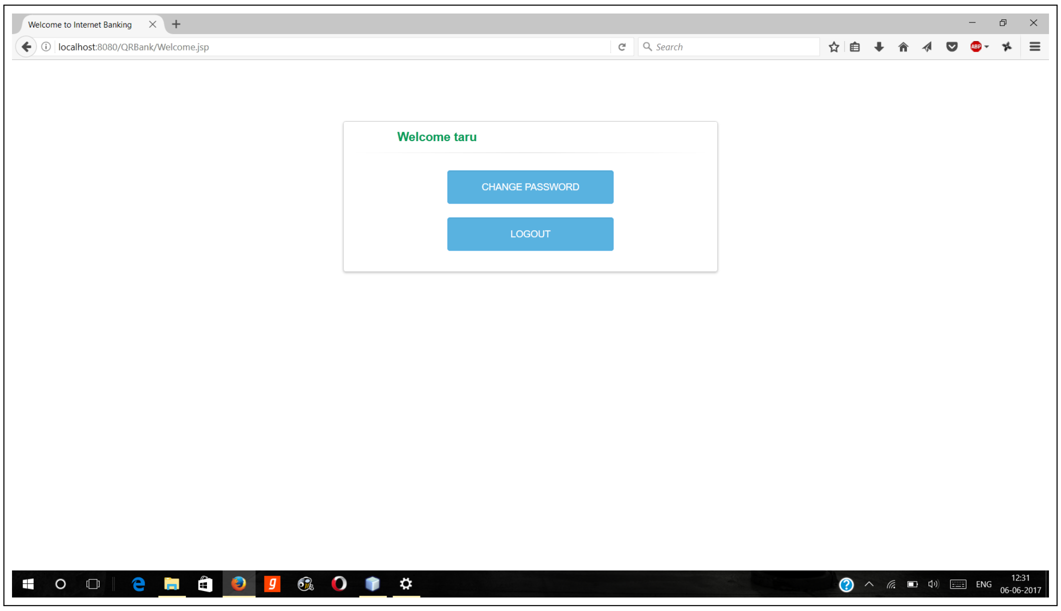

Welcome to Internet Banking
localhost:8080/QRBank/Welcome.jsp
Search
Welcome taru
CHANGE PASSWORD
LOGOUT
ENG
12:31
06-06-2017

Figure 10.10: Website login success

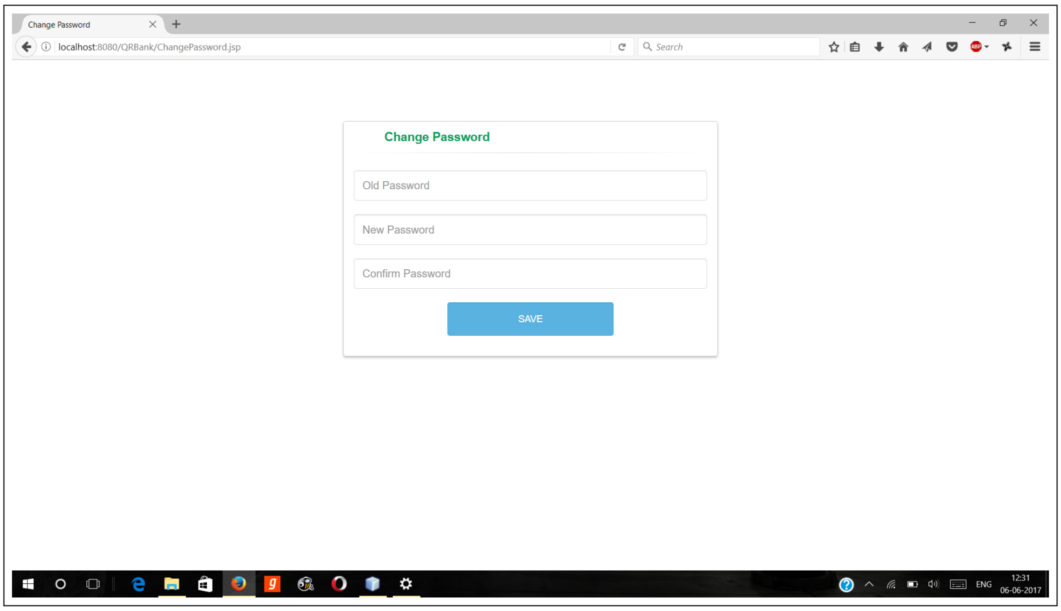


Figure 10.11: Website change password

Chapter 11

Deployment and Maintenance

11.1 Installation and un-installation

11.1.1 MySQL

- Step 1: Download MySQL 5.1 for Windows Download the latest MySQL version.

- Step 2: Install MySQL Double click the MSI installer to start installing MySQL. You will go through a setup wizard so it's fairly simple. Just follow the installation instructions step by step.
  (1) Welcome to the Setup Wizard for MySQL Server 5.1. Click Next to continue.

  (2) Select a setup type - Typical, Complete, Custom. Select Typical and click Next. The default insllation directory will be C:FilesServer 5.0

  (3) Ready to install MySQL. After review the settings, click Install. If you want to change any settings, click [Back] button.

  (4) Installation in progress.

  (5) More information about MySQL Enterprise Subscription. This step is just an informational step for MySQL Enterprise Subscription. Click the [More...] button if you want to know more. Otherwise, click [Next] to go to next step.

  (6) Setup Wizard Completed. Make sure you have selected 'Configure the MySQL Server now' checkbox if you want to configure it after clicking Finish button.

1. Start MySQL Server Instance Configuration Wizard. If you have selected the checkbox 'Configure the MySQL Server now' in the last step when installing MySQL 5.1, the configuration wizard should start automatically when you click the Finish button.
Alternatively, you can launch the wizard from Start menu. Start -¿ Programs -¿ MySQL -¿ MySQL Server 5.1 -¿ MySQL Server Instance Config Wizard.

- Steps to configure to MySQL server Instance

  2. Select configuration type. Select Detailed Configuration here. If this is the only MySQL server installed on your computer, you can select Standard Configuration.

  3. Select a server type. As this MySQL server is running on a development box, select Developer Machine as the server type.

  4. Select the database usage. Depends on the purpose of your development box, you can select either Multifunctional Database or Transactional Database Only. Here we selected Transactional Database Only.

  5. Set InnoDB table space settings. InnoDB table type is the storage engine for a transactional database. Use the default settings here.

  6. Set the database engine's concurrent connections option. Here we selected Online Transaction Processing (OLTP) as it is the most common use of MySQL server. If the MySQL server on your development machine is used for decision support such as data warehousing or data mining, select the first option.

  7. Set networking options. By default, make your selection the same as screenshot below. If port 3306 has been used by another instance of MySQL server, you can select port 3307 or a different port. This will allow two instances of MySQL server to be accessed via different ports on the same box.

  8. Select the default character set. By default, the Standard Character Set is selected, but you may want to select the second option - Best Support For Multilingualism. This allows our database to store text in many different languages.

  9. Install MySQL server as a Windows service. Below is the recommended way to run MySQL server on Windows. Making the service name as MySQL51 clearly identifies the service as a MySQL server version 5.1 database engine because you might install other versions of MySQL server on the same machine.

10. Set the root password. Set a new password to the root account. Enter the same password to all three boxes. See below. Don't select the Create An Anonymous Account checkbox. This can lead to an insecure system.

11. Ready to execute the configuration. Now everything is ready to execute. Click [Execute] button.

12. Configuration successfully completed. The configuration file has been created successfully. Click [Finish] to close the wizard.

11.1.2 NetBeans

- NetBeans is an open-source integrated development environment (IDE) for developing primarily with Java, but also with other languages, in particular PHP, C/C++, and HTML5. It is also an application platform framework for Java desktop applications and others.

- The NetBeans IDE is written in Java and can run on Windows, OS X, Linux, Solaris and other platforms supporting a compatible JVM.

- We have used NetBeans 7.1.2. NetBeans IDE 7.1.2 is an update to NetBeans IDE 7.1 and NetBeans IDE 7.1.1, and contains the following highlights:
  - Java SE 7u4 Support, which includes the first Oracle JDK release for Mac OS X
  - JavaFX 2.1 Support (Bundled with the JDK)
  - Ant upgrade to version 1.8.3
  - Support for GlassFish 3.1.2
  - Integration of recent patches
  - Minor performance improvements

Chapter 12

Conclusion and future scope

Security has become extremely important in the digital society. Authentication methods should be seriously considered by services that store sensitive information. Most of the users have android smart phones. These Smart phones have good processing power and memory size.
As a mobile phone has become an indispensable accessory and carry-on device in real life, compared with the traditional key or access card, sending the authentication image by using mobile phones through MMS (Multimedia Messaging Service) allows the user to carry fewer objects and no extra specific hardware cost needed. So some security features can be deployed on them in order to identify a user to the service provider.
Using QR Code, successful authentication can be done. The use of QR code image for authentication makes it difficult to be accessed, modified and copied, and it can be applied to many services that require authentication.

Annexure A

References

- Mukhopadhyay, S.; Argles, D., An Anti-Phishing mechanism for single sign-on based on QR-code, Information Society (i-Society), 2011 International Conference on , vol., no., pp.505,508, 27-29 June 2011

- A.S. Narayanan. QR Codes and security solutions, International Journal of Computer Science and Telecommunications Volume 3, Issue 7, July 2012

- Soon,TanJin.,QR Code. ,Synthesis Journal: 59-78

- Aviel.D.Rubin.Independent OTPs, June 1995.Website- http://avirubin.com/onetime.pdf6

- Azhar,Rizwan.Camera Based Authentication Methods. Website www.ida.liu.se/ TDDD17/old projects/2010/projects/ 011.pdf

- Open ID Foundation, Get an Open ID. [Online]. Available: http://openid.net/get-an-openid.

- C.Herley and P.C van Oorschot,A research agenda acknowledging the persistence of passwords,IEEE Security and Privacy,vol.10,no. 1,pp 2836, 2012.

- Kroenke.D, Experiencing MIS in 5/E 2014 Prentice Hall. P.696.

- Kan T.W, C.H.Teng and M.Y.Chen, QR code based augmented reality applications in handbook of augmented reality, B.Furht Editor 2011 Springer: New York p 339-354.

- NIST SP800-63 Electronic Authentication Guideline,NIST Special Publication V1.0 June2004

Annexure B

Laboratory assignments on Project Analysis of Algorithmic Design

- To develop the problem under consideration and justify feasibilty using concepts of knowledge canvas and IDEA Matrix.Knowledge canvas is one that depicts the knowledge forces and knowledge flow across the organization. It captures the current knowledge state and knowledge forces in the environment. It tries to build the bigger and broader knowledge scenario for you and your environment. It is simple representation of knowledge opportunities with reference to the environment.

I	D	E	A
Increase	Drive	Educate	Accelerate
Improve	Deliver	Evaluate	Associate
Ignore	Decrease	Eliminate	Avoid

Table B.1: IDEA Matrix

- Feasibility
  Feasibility study on the system proposal regarding its work ability, impact on the organization, ability to meet user nodes, and effective use of resources, this when a new application is proposed, it normally goes through a feasibility study before it is approved for development. For any project to be successful there is a need for an effective feasibility study. The purpose of feasibility study is not to solve the problem but to determine if the problem is worth solving. We have feasibility

studies to be connected. But there are three primary feasibility tests to be performed.
Economical feasibility
Technical feasibility
Operational feasibility

- Economical Feasibility
  This study is carried out to check the economic impact that the system will have on the organization. The amount of fund that the company can pour into the research and development of the system is limited. The expenditures must be justified. Thus the developed system as well within the budget and this was achieved because most of the technologies used are freely available. Only the customized products had to be purchased.

- Technical Feasibility
  This study is carried out to check the technical feasibility, that is, the technical requirements of the system. Any system developed must not have a high demand on the available technical resources. This will lead to high demands on the available technical resources. This will lead to high demands being placed on the client. The developed system must have a modest requirement, as only minimal or null changes are required for implementing this system.

- Operational Feasibility
  The aspect of study is to check the level of acceptance of the system by the user. This includes the process of training the user to use the system efficiently. The user must not feel threatened by the system, instead must accept it as a necessity. The level of acceptance by the users solely depends on the methods that are employed to educate the user about the system and to make him familiar with it. His level of confidence must be raised so that he is also able to make some constructive criticism, which is welcomed, as he is the final user of system.

Annexure C

Laboratory assignments on Project Quality and Reliability Testing of Project Design

C.1 UML Diagrams

C.1.1 Class Diagram

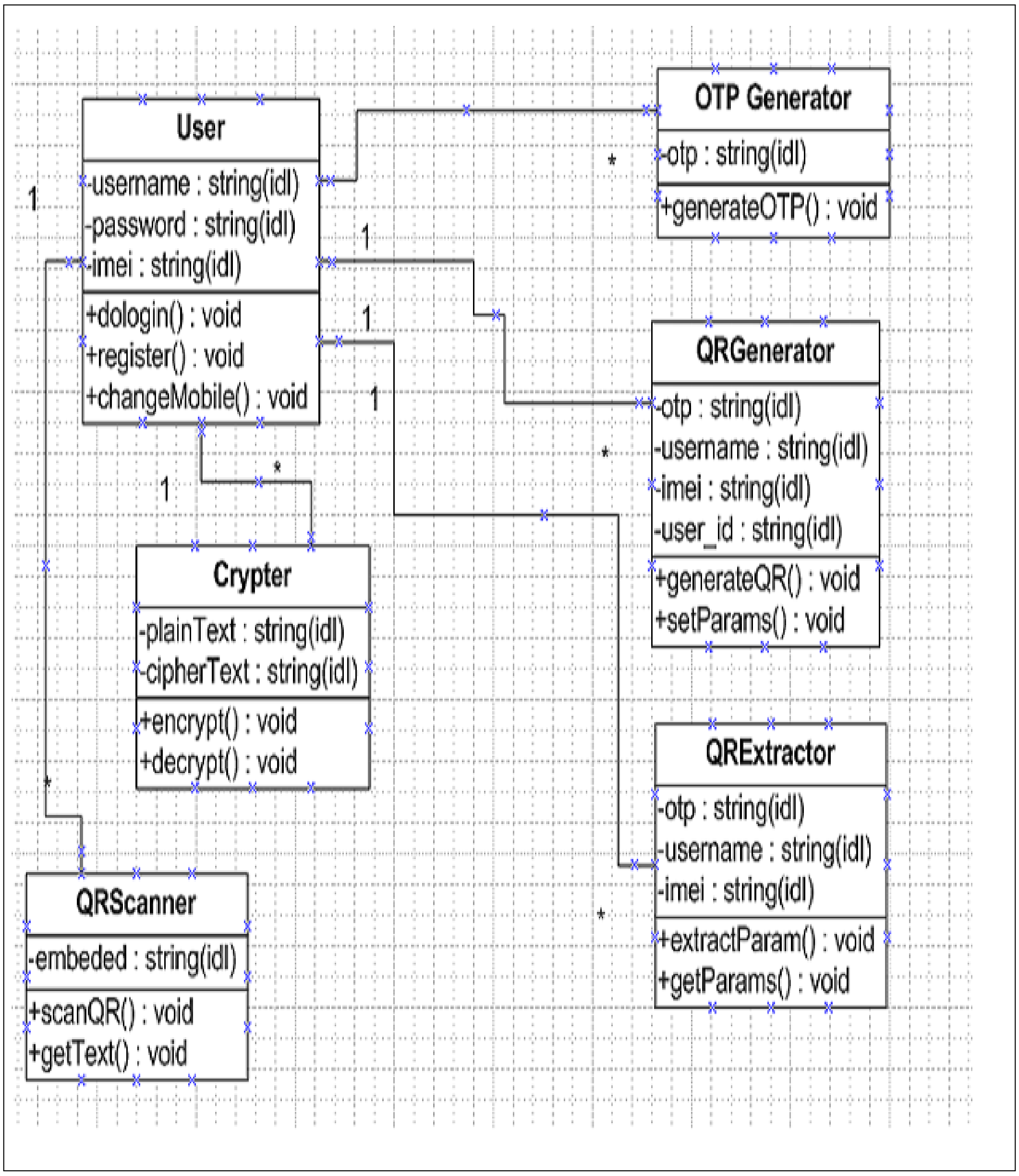


Figure C.1: Class Diagram

C.2 Use Case Diagram

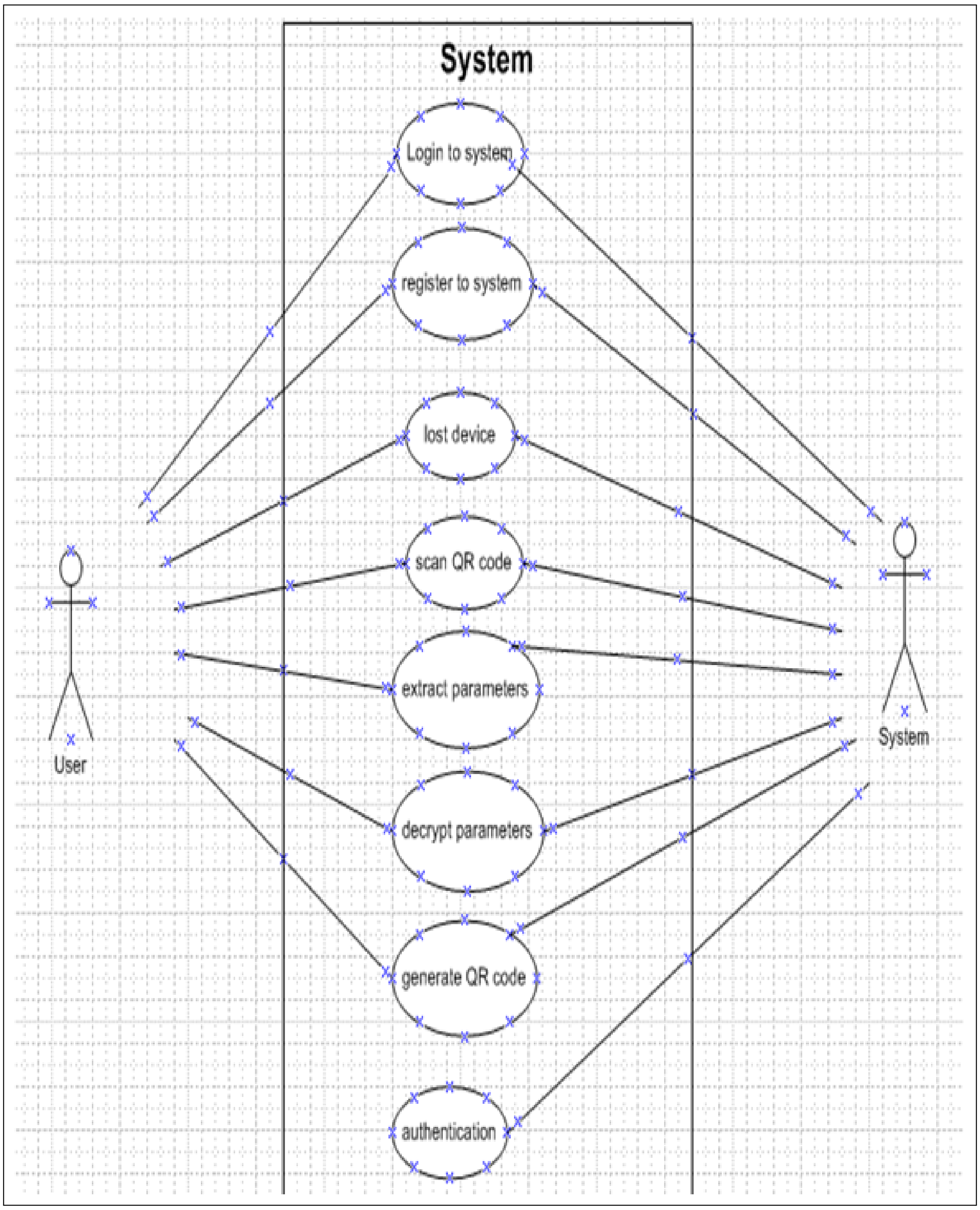


Figure C.2: Use Case Diagram

C.3 Activity Diagram

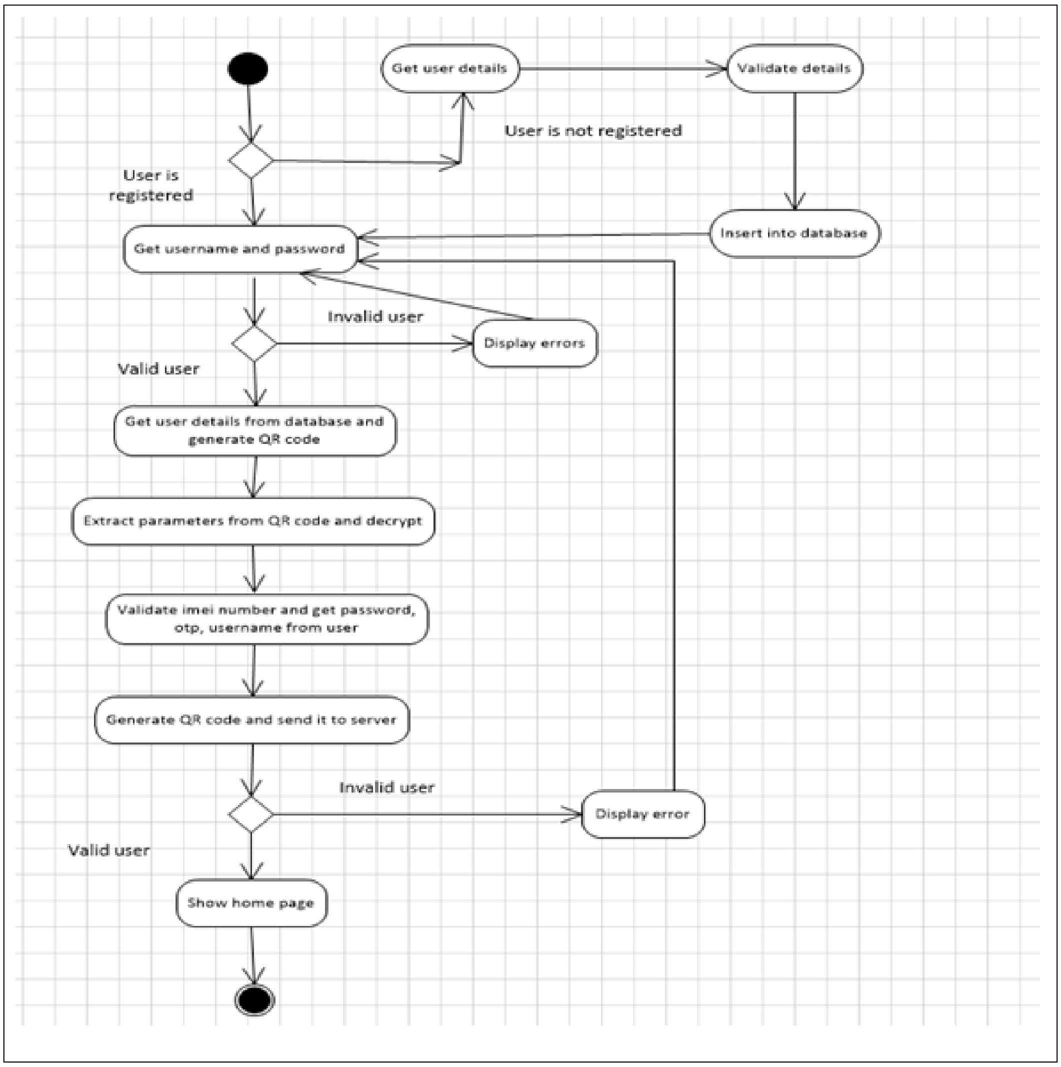
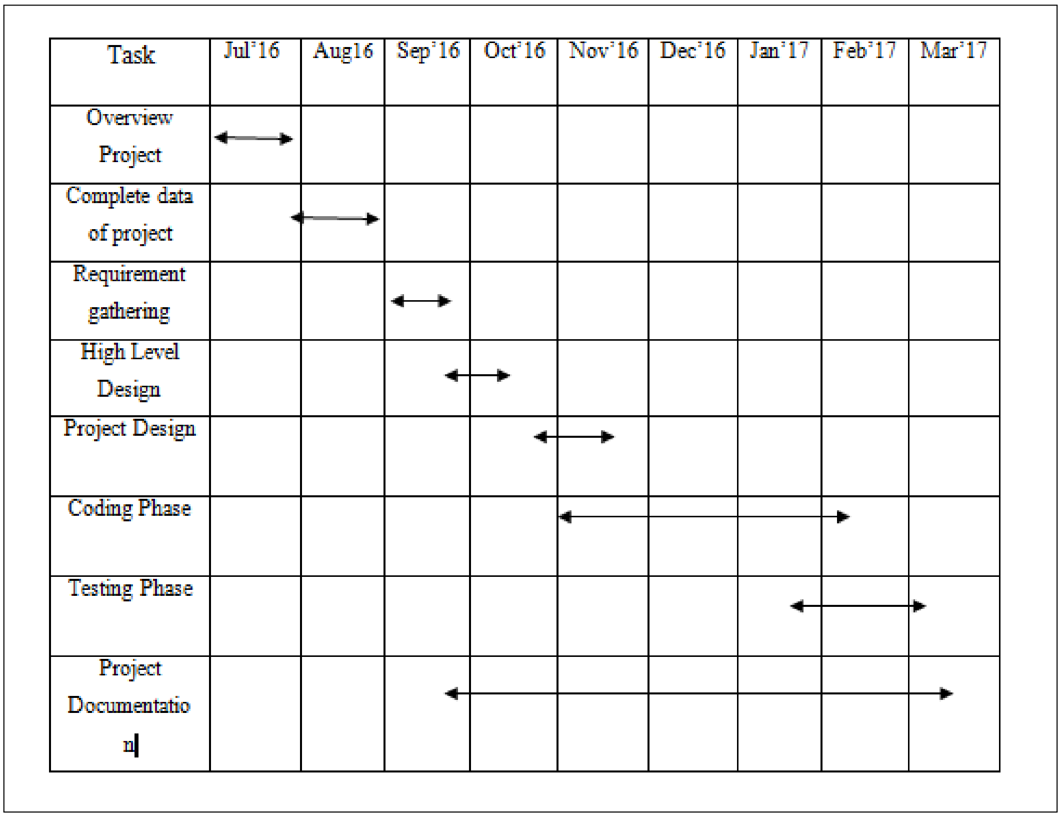

Get user details
Validate details
User is not registered
User is registered
Insert into database
Get username and password
Invalid user
Display errors
Valid user
Get user details from database and generate QR code
Extract parameters from QR code and decrypt
Validate imei number and get password, otp, username from user
Generate QR code and send it to server
Invalid user
Display error
Valid user
Show home page

Figure C.3: Activity Diagram

Annexure D

Project Planner



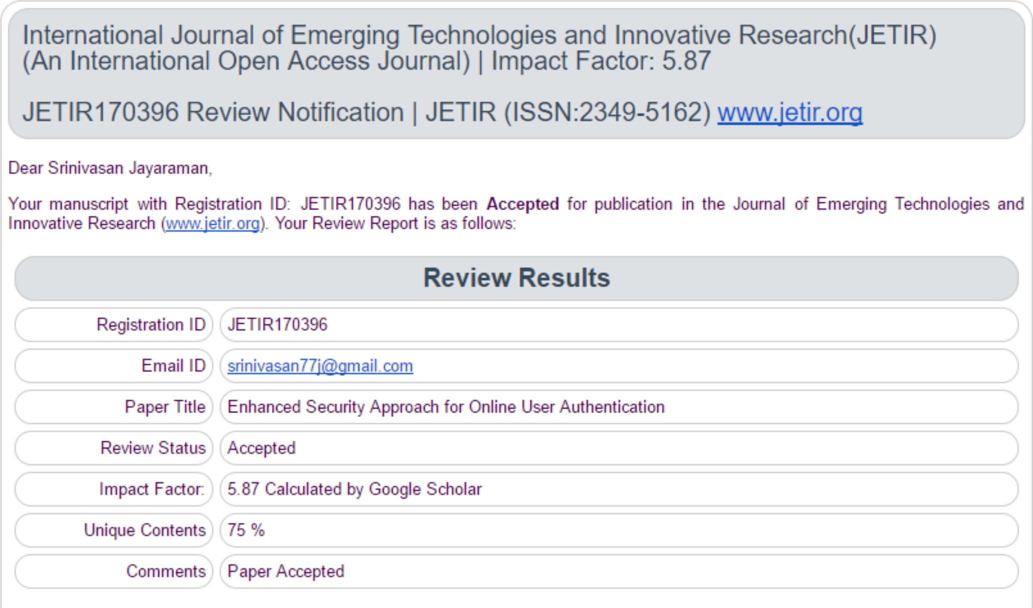
Task	Jul'16	Aug16	Sep'16	Oct'16	Nov'16	Dec'16	Jan'17	Feb'17	Mar'17
Overview Project	↔								
Complete data of project		↔							
Requirement gathering			↔						
High Level Design			↔	↔					
Project Design				↔	↔				
Coding Phase					↔	↔	↔	↔	
Testing Phase							↔	↔	↔
Project Documentatio n			↔	↔	↔	↔	↔	↔	↔

Figure D.1: project planner

Annexure E

Reviewers Comments of Paper Submitted

1. Paper Title:Enhanced Security Approach for Online User Authentication
2. Name of the Conference/Journal where paper submitted :JETIR
3. Paper accepted/rejected : Accepted
4. Review comments by reviewer :None
5. Corrective actions if any :None



International Journal of Emerging Technologies and Innovative Research(JETIR)
(An International Open Access Journal) | Impact Factor: 5.87

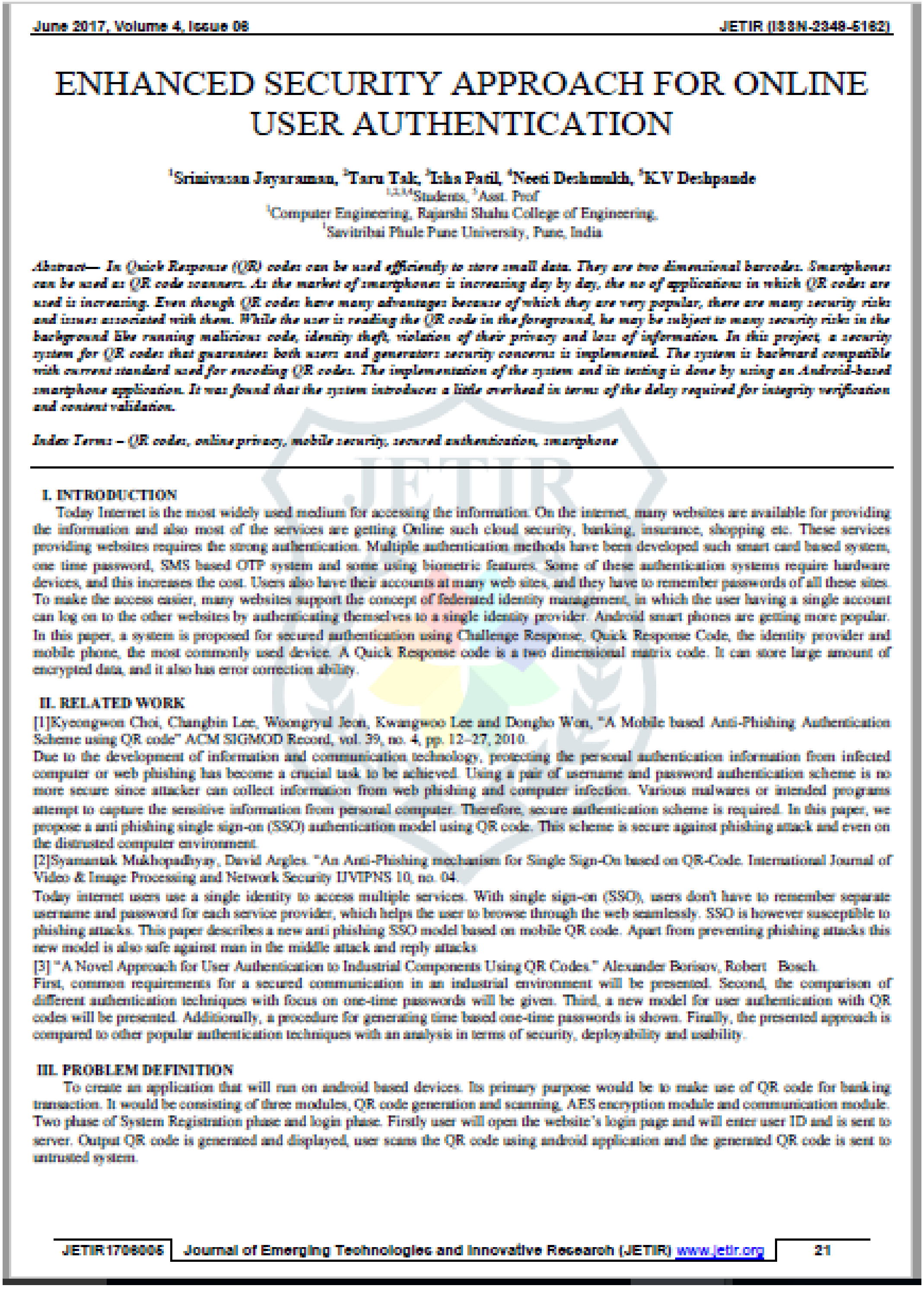
JETIR170396 Review Notification | JETIR (ISSN:2349-5162) www.jetir.org

Dear Srinivasan Jayaraman,

Your manuscript with Registration ID: JETIR170396 has been **Accepted** for publication in the Journal of Emerging Technologies and Innovative Research (www.jetir.org). Your Review Report is as follows:

Review Results

Registration ID	JETIR170396
Email ID	srinivasan77j@gmail.com
Paper Title	Enhanced Security Approach for Online User Authentication
Review Status	Accepted
Impact Factor:	5.87 Calculated by Google Scholar
Unique Contents	75 %
Comments	Paper Accepted



June 2017, Volume 4, Issue 06 JETIR (ISSN-2349-5162)

ENHANCED SECURITY APPROACH FOR ONLINE USER AUTHENTICATION

[1]Srinivasan Jayaraman, [2]Taru Tak, [3]Isha Patil, [4]Neeti Deshmukh, [5]K.V Deshpande
[1,2,3,4]Students, [5]Asst. Prof
[1]Computer Engineering, Rajarshi Shahu College of Engineering,
[1]Savitribai Phule Pune University, Pune, India

***Abstract—** In Quick Response (QR) codes can be used efficiently to store small data. They are two dimensional barcodes. Smartphones can be used as QR code scanners. As the market of smartphones is increasing day by day, the no of applications in which QR codes are used is increasing. Even though QR codes have many advantages because of which they are very popular, there are many security risks and issues associated with them. While the user is reading the QR code in the foreground, he may be subject to many security risks in the background like running malicious code, identity theft, violation of their privacy and loss of information. In this project, a security system for QR codes that guarantees both users and generators security concerns is implemented. The system is backward compatible with current standard used for encoding QR codes. The implementation of the system and its testing is done by using an Android-based smartphone application. It was found that the system introduces a little overhead in terms of the delay required for integrity verification and content validation.*

***Index Terms** – QR codes, online privacy, mobile security, secured authentication, smartphone*

I. INTRODUCTION

Today Internet is the most widely used medium for accessing the information. On the internet, many websites are available for providing the information and also most of the services are getting Online such cloud security, banking, insurance, shopping etc. These services providing websites requires the strong authentication. Multiple authentication methods have been developed such smart card based system, one time password, SMS based OTP system and some using biometric features. Some of these authentication systems require hardware devices, and this increases the cost. Users also have their accounts at many web sites, and they have to remember passwords of all these sites. To make the access easier, many websites support the concept of federated identity management, in which the user having a single account can log on to the other websites by authenticating themselves to a single identity provider. Android smart phones are getting more popular. In this paper, a system is proposed for secured authentication using Challenge Response, Quick Response Code, the identity provider and mobile phone, the most commonly used device. A Quick Response code is a two dimensional matrix code. It can store large amount of encrypted data, and it also has error correction ability.

II. RELATED WORK

[1]Kyeongwon Choi, Changbin Lee, Woongryul Jeon, Kwangwoo Lee and Dongho Won, "A Mobile based Anti-Phishing Authentication Scheme using QR code" ACM SIGMOD Record, vol. 39, no. 4, pp. 12–27, 2010.

Due to the development of information and communication technology, protecting the personal authentication information from infected computer or web phishing has become a crucial task to be achieved. Using a pair of username and password authentication scheme is no more secure since attacker can collect information from web phishing and computer infection. Various malwares or intended programs attempt to capture the sensitive information from personal computer. Therefore, secure authentication scheme is required. In this paper, we propose a anti phishing single sign-on (SSO) authentication model using QR code. This scheme is secure against phishing attack and even on the distrusted computer environment.

[2]Syamantak Mukhopadhyay, David Argles. "An Anti-Phishing mechanism for Single Sign-On based on QR-Code. International Journal of Video & Image Processing and Network Security IJVIPNS 10, no. 04.

Today internet users use a single identity to access multiple services. With single sign-on (SSO), users don't have to remember separate username and password for each service provider, which helps the user to browse through the web seamlessly. SSO is however susceptible to phishing attacks. This paper describes a new anti phishing SSO model based on mobile QR code. Apart from preventing phishing attacks this new model is also safe against man in the middle attack and reply attacks

[3] "A Novel Approach for User Authentication to Industrial Components Using QR Codes." Alexander Borisov, Robert Bosch.

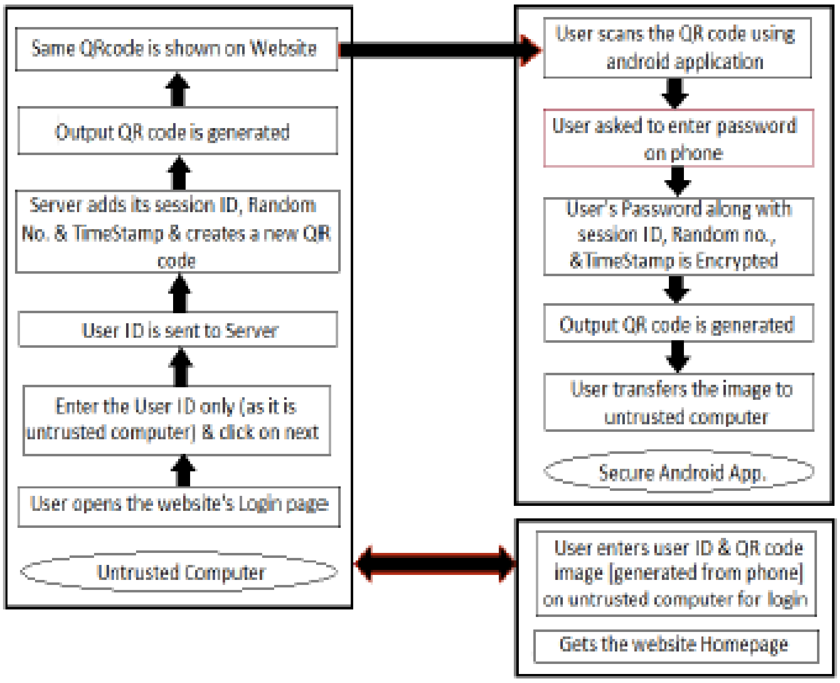
First, common requirements for a secured communication in an industrial environment will be presented. Second, the comparison of different authentication techniques with focus on one-time passwords will be given. Third, a new model for user authentication with QR codes will be presented. Additionally, a procedure for generating time based one-time passwords is shown. Finally, the presented approach is compared to other popular authentication techniques with an analysis in terms of security, deployability and usability.

III. PROBLEM DEFINITION

To create an application that will run on android based devices. Its primary purpose would be to make use of QR code for banking transaction. It would be consisting of three modules, QR code generation and scanning, AES encryption module and communication module. Two phase of System Registration phase and login phase. Firstly user will open the website's login page and will enter user ID and is sent to server. Output QR code is generated and displayed, user scans the QR code using android application and the generated QR code is sent to untrusted system.

JETIR1706005 Journal of Emerging Technologies and Innovative Research (JETIR) www.jetir.org 21

IV. PROPOSED SYSTEM


Same QRcode is shown on Website
Output QR code is generated
Server adds its session ID, Random No. & TimeStamp & creates a new QR code
User ID is sent to Server
Enter the User ID only (as it is untrusted computer) & click on next
User opens the website's Login page
Untrusted Computer
User scans the QR code using android application
User asked to enter password on phone
User's Password along with session ID, Random no., &TimeStamp is Encrypted
Output QR code is generated
User transfers the image to untrusted computer
Secure Android App.
User enters user ID & QR code image (generated from phone) on untrusted computer for login
Gets the website Homepage

The following are the points that mention the overall working of the proposed application:

- A mobile banking transaction on untrusted system.
- Server adds session id, random number and timestamp and creates QR code.
- Generates and scans QR code using android application.
- User's password along with generated session id, random number and timestamp is encrypted and a new QR code is generated.
- User transfers the image to the untrusted computer.
- The transferred QR code along with user id is entered on the website home page.
- If verified then transaction proceeds.

IV.CONCLUSION

Security has become extremely important in the digital society. Authentication methods should be seriously considered by services that store sensitive information. Most of the users have android smart phones. These Smart phones have good processing power and memory size.

As a mobile phone has become an indispensable accessory and carry-on device in real life, compared with the traditional key or access card, sending the authentication image by using mobile phones through MMS (Multimedia Messaging Service) allows the user to carry fewer objects and no extra specific hardware cost needed. So some security features can be deployed on them in order to identify a user to the service provider.

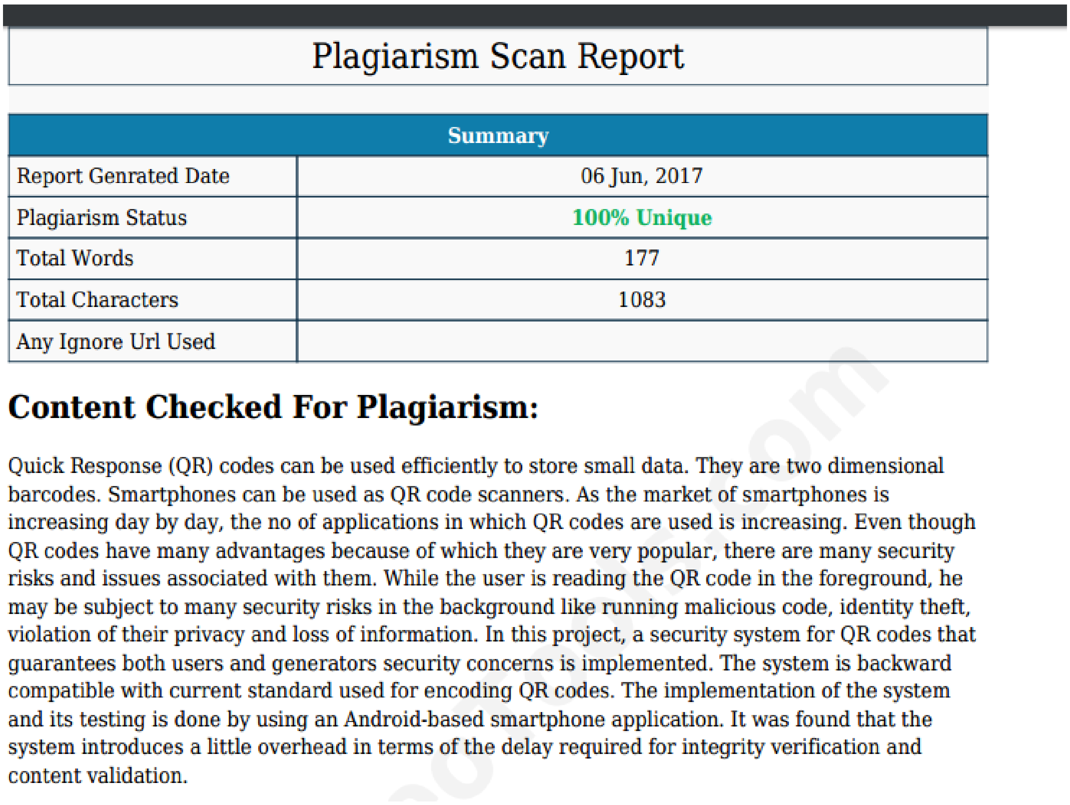
Using QR Code, successful authentication can be done. The use of QR code image for authentication makes it difficult to be accessed, modified and copied, and it can be applied to many services that require authentication.

V.REFERENCES

[1] Mukhopadhyay, S.; Argles, D., "An Anti-Phishing mechanism for single sign-on based on QR-code," Information Society (i-Society), 2011 International Conference on , vol., no., pp.505,508, 27-29 June 2011
[2] A.S. Narayanan. "QR Codes and security solutions," International Journal of Computer Science and Telecommunications Volume 3, Issue 7, July 2012
[3] Soon,TanJin.,"QR Code." ,Synthesis Journal: 59-78
[4] AvielD.Rubin. "Independent One-Time Passwords", June 1995. Website- http://avirubin.com/onetime.pdf6
[5] Azhar,Rizwan."Camera Based Authentication Methods". Website www. ida.liu.se/ TDDD17/old projects/2010/projects/ 011.pdf
[6] Open ID Foundation, "Get an Open ID". [Online]. Available:http://openid.net/get-an-openid

Annexure F

Plagiarism Report



Plagiarism Scan Report

Summary	
Report Genrated Date	06 Jun, 2017
Plagiarism Status	**100% Unique**
Total Words	177
Total Characters	1083
Any Ignore Url Used	

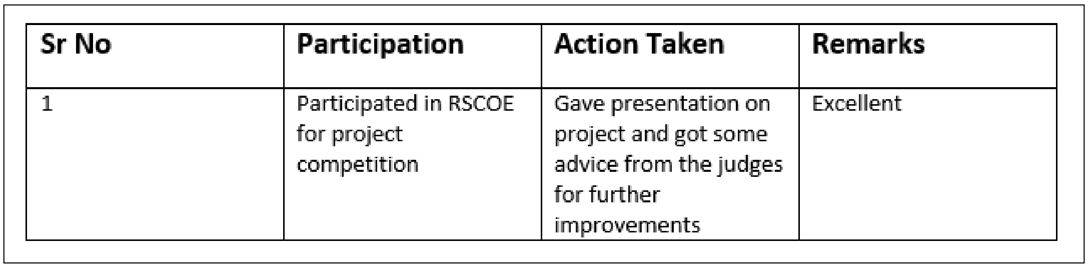
Content Checked For Plagiarism:

Quick Response (QR) codes can be used efficiently to store small data. They are two dimensional barcodes. Smartphones can be used as QR code scanners. As the market of smartphones is increasing day by day, the no of applications in which QR codes are used is increasing. Even though QR codes have many advantages because of which they are very popular, there are many security risks and issues associated with them. While the user is reading the QR code in the foreground, he may be subject to many security risks in the background like running malicious code, identity theft, violation of their privacy and loss of information. In this project, a security system for QR codes that guarantees both users and generators security concerns is implemented. The system is backward compatible with current standard used for encoding QR codes. The implementation of the system and its testing is done by using an Android-based smartphone application. It was found that the system introduces a little overhead in terms of the delay required for integrity verification and content validation.

Annexure G

Term-II Project Laboratory Assignments

1. Review of design and necessary corrective actions taking into consideration the feedback report of Term I assessment, and other competitions/conferences participated like IIT, Central Universities, University Conferences or equivalent centers of excellence etc.



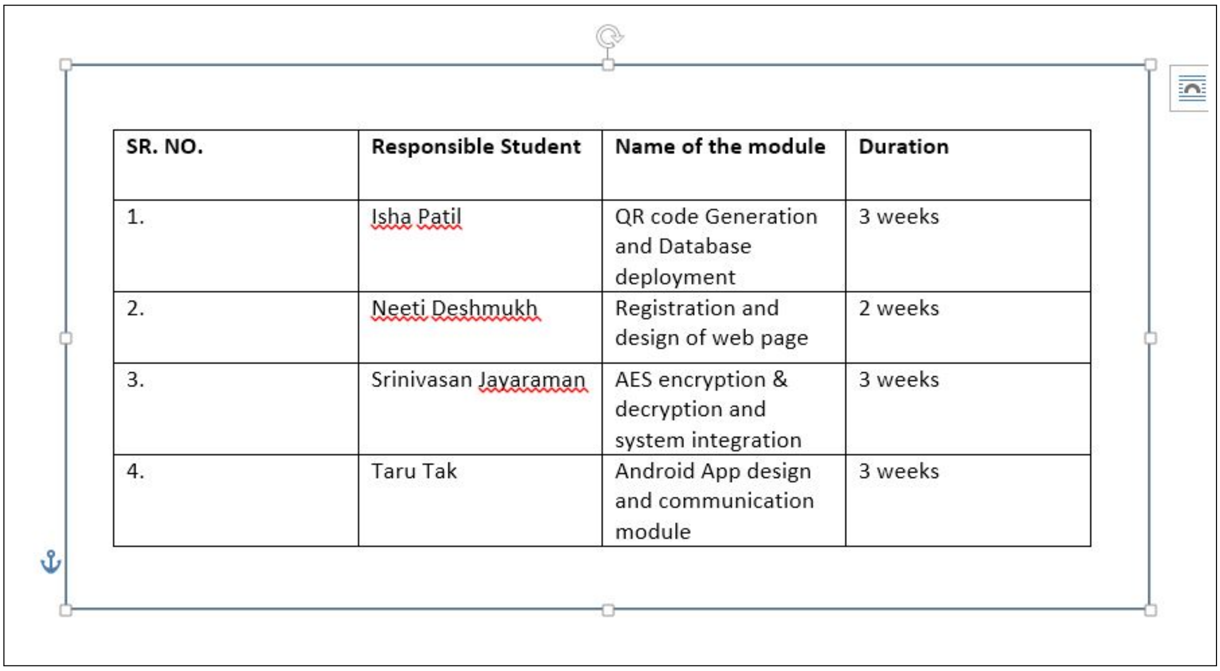
Sr No	Participation	Action Taken	Remarks
1	Participated in RSCOE for project competition	Gave presentation on project and got some advice from the judges for further improvements	Excellent

Figure G.1: Feedback

2. Project workstation selection, installations along with setup and installation report preparations.

   - SOFTWARE REQUIREMENTS 1. Java JDK 1.6. 2. Android SDK 2.3.3 or above. 3. Netbeans 7.4. 4. MySQL and SQLyog 5. Operating System : Windows 7 or above, Andorid OS

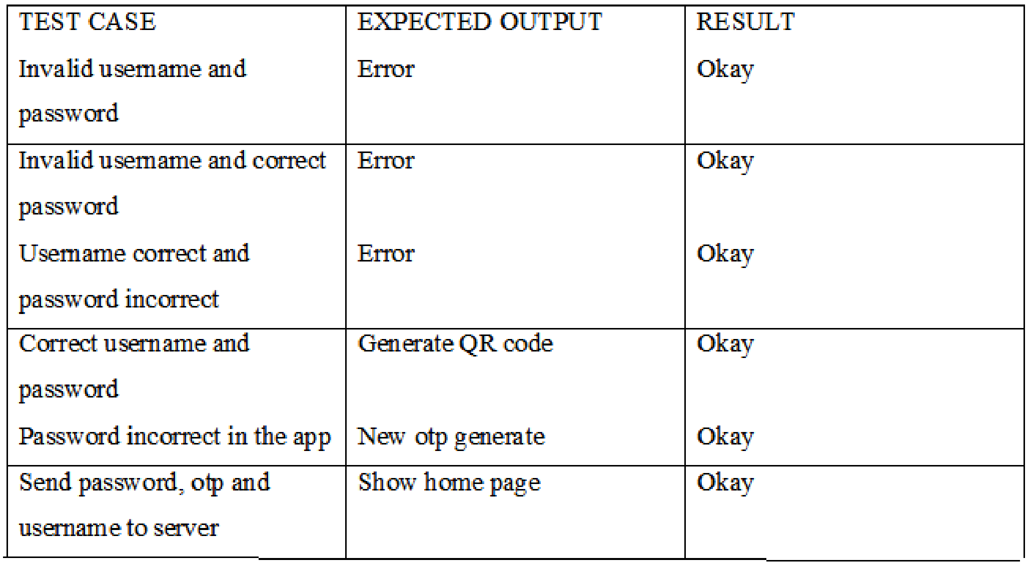
3. Programming of the project functions, interfaces and GUI (if any) as per 1 st Term term-work submission using corrective actions recommended in Term-I assessment of Term-work.



SR. NO.	Responsible Student	Name of the module	Duration
1.	Isha Patil	QR code Generation and Database deployment	3 weeks
2.	Neeti Deshmukh	Registration and design of web page	2 weeks
3.	Srinivasan Jayaraman	AES encryption & decryption and system integration	3 weeks
4.	Taru Tak	Android App design and communication module	3 weeks

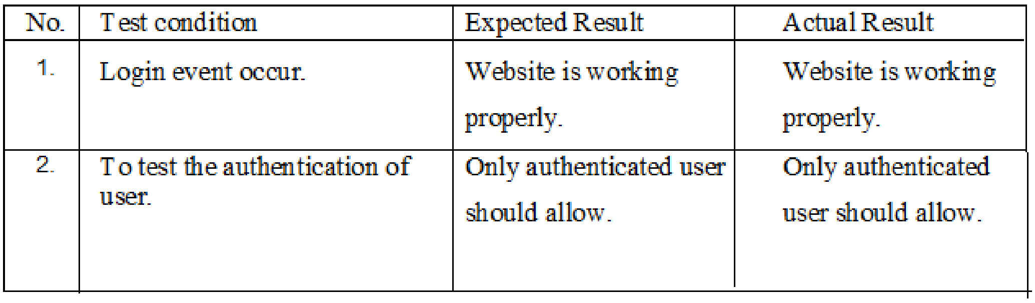
Figure G.2: Project Implementation

4. Test tool selection and testing of various test cases for the project performed and generate various testing result charts, graphs etc. including reliability testing.



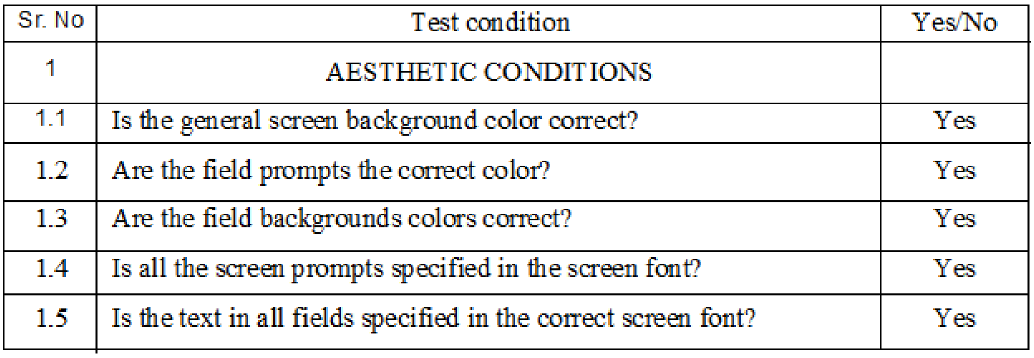
TEST CASE	EXPECTED OUTPUT	RESULT
Invalid username and password	Error	Okay
Invalid username and correct password	Error	Okay
Username correct and password incorrect	Error	Okay
Correct username and password	Generate QR code	Okay
Password incorrect in the app	New otp generate	Okay
Send password, otp and username to server	Show home page	Okay

- Login test cases



No.	Test condition	Expected Result	Actual Result
1.	Login event occur.	Website is working properly.	Website is working properly.
2.	To test the authentication of user.	Only authenticated user should allow.	Only authenticated user should allow.

- GUI test cases



Sr. No	Test condition	Yes/No
1	AESTHETIC CONDITIONS	
1.1	Is the general screen background color correct?	Yes
1.2	Are the field prompts the correct color?	Yes
1.3	Are the field backgrounds colors correct?	Yes
1.4	Is all the screen prompts specified in the screen font?	Yes
1.5	Is the text in all fields specified in the correct screen font?	Yes

2	VALIDATION CONDITION	
2.1	Is the user required to fix entries which have failed validation test?	Yes
2.2	Does the failure of validation on every field cause a sensible user error message?	Yes
2.3	Do all mandatory fields require user input?	Yes

3	NAVIGATION CONDITIONS	
3.1	Can the screen be accessed correctly from the menu?	Yes
3.2	Can all screens accessible via buttons on this screen be accessed correctly?	Yes

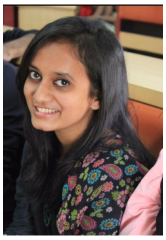
4	USABILITY CONDITIONS	
4.1	Is all data entry required in the correct format?	Yes
4.2	Have the menu options which applied to your screen got fast keys associated and should they have?	No
4.3	Is there default button specified in the screen?	Yes

5	DATA INTEGRITY CONDITIONS	
5.1	Is the data saved when the window is closed by double clicking on the close box?	Yes
5.2	If numeric fields except negative values can these be stored correctly on the database and does it make sense for the field to accept negative numbers.	No

Annexure H

Information of Project Group Members

1. Name : Neeti Deshmukh
2. Date of Birth : 03/06/1994
3. Gender : Female
4. Permanent Address : E-30,Shriramnagar,Aundh,Pune
5. E-Mail : neetideshmukh@gmail.com
6. Mobile/Contact No. : 8600201266
7. Placement Details : Amazon
8. Paper Published : JETIR



1. Name : Isha Patil
2. Date of Birth : 29/01/1996
3. Gender : Female
4. Permanent Address : B4,pancharatna, Baner
5. E-Mail : ishapatil1996@gmail.com
6. Mobile/Contact No. : +91-8806309157
7. Placement Details : NA
8. Paper Published : JETIR

1. Name : Srinivasan Jayaraman
2. Date of Birth : 07/07/1995
3. Gender : Male
4. Permanent Address : E-4,Chidanand hsg soc,Sus-rd,Pune
5. E-Mail : srinivasan77j@gmail.com
6. Mobile/Contact No. : 8390309885
7. Placement Details : TCS
8. Paper Published : JETIR

1. Name :Taru Tak
2. Date of Birth : 05/01/1995
3. Gender : Male
4. Permanent Address : f-703, Sollana Soceity, Thergaon
5. E-Mail : taktaru@gmail.com
6. Mobile/Contact No. : +91-9765018404
7. Placement Details : BYJU's- Think n learn
8. Paper Published : JETIR