

Secure Password Manager

BY

Mst. Farzana Khatun

ID: 152-15-5896

AND

Md. Tanbir Hossain

ID: 152-15-5959

This Report Presented in Partial Fulfillment of the Requirements for the
Degree of Bachelor of Science in Computer Science and Engineering

Supervised By

Ahmed Al Marouf

Lecturer

Department of CSE

Daffodil International University

Co-Supervised By

Shah Md. Tanvir Siddiquee

Senior Lecturer

Department of CSE

Daffodil International University



DAFFODIL INTERNATIONAL UNIVERSITY

DHAKA, BANGLADESH

MAY 2018

APPROVAL

This Project titled “**Secure Password Manager**” submitted by Mst. Farzana Khatun (ID:152-15-5896) and Md. Tanbir Hossain (ID:152-15-5959) to the Department of CSE, Daffodil International University, has been accepted as satisfactory for the partial fulfillment of the requirements for the degree of B.Sc. in Computer Science and Engineering and approved as to its style and contents. The presentation has been held on May 7, 2018.

BOARD OF EXAMINERS



Dr. Syed Akhter Hossain
Professor and Head
Department of Computer Science and Engineering
Faculty of Science & Information Technology
Daffodil International University

Chairman



Dr. Sheak Rashed Haider Noori
Associate Professor and Associate Head
Department of Computer Science and Engineering
Faculty of Science & Information Technology
Daffodil International University

Internal Examiner



Md. Zahid Hasan
Assistant Professor
Department of Computer Science and Engineering
Faculty of Science & Information Technology
Daffodil International University

External Examiner



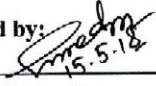
Dr. Mohammad Shorif Uddin
Professor
Department of Computer Science and Engineering
Jahangirnagar University

External Examiner

DECLARATION

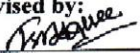
We hereby declare that, this project have been done by us under the supervision of **Ahmed Al Marouf, Lecturer, Department of CSE** Daffodil International University. We also declare that neither this project nor any part of this project have been submitted elsewhere for award of any degree or diploma.

Supervised by:



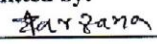
Ahmed Al Marouf
Lecturer
Department of Computer Science and Engineering
Daffodil International University

Co-Supervised by:




Shah Md. Tanvir Siddiquee
Senior Lecturer
Department of Computer Science and Engineering
Daffodil International University

Submitted by:



Mst. Farzana Khatun
ID: 152-15-5896
Department of Computer Science and Engineering
Daffodil International University



Md. Tanbir Hossain
ID: 152-15-5959
Department of Computer Science and Engineering
Daffodil International University

ACKNOWLEDGEMENT

First, we express our heartiest thanks and gratefulness to almighty God for His divine blessing makes us possible to complete the final year project/internship successfully.

We grateful and wish our profound our indebtedness to **Ahmed Al Marouf, Lecturer**, Department of CSE Daffodil International University, Dhaka. Deep Knowledge & keen interest of our supervisor in the field of “*Cryptography & Human Computer Interaction (HCI)*” to carry out this project. His endless patience, scholarly guidance, continual encouragement, constant and energetic supervision, constructive criticism, valuable advice, reading many inferior draft and correcting them at all stage have made it possible to complete this project.

We would like to express our heartiest gratitude to **Dr. Syed Akhter Hossain, Professor & Head**, Department of CSE, for his kind help to finish our project and also to other faculty member and the staff of CSE department of Daffodil International University.

We would like to thank our entire course mate in Daffodil International University, who took part in this discuss while completing the course work.

Finally, we must acknowledge with due respect the constant support and patients of our parents.

ABSTRACT

In these days there are lots Password Managers such as LastPass, 1Password, KeePass, Dashlane and Browser's password manager. All of these are very popular web based password managers. We study the security of popular password manager's and their policies. After study, we got result that these password managers suffer different web attacks and someone is more expensive or complex UI such as LastPass was hacked in 2015, Dashlane is expensive and Browser's password manager faced many online attacks. Therefore, we will present a design for a password manager which is web-based that name is **Secure password manager**. Secure password manager is the solution of these problems. It can keep your password in secure place by passing different security level. It will provide database security from hackers and different online attacks, simple UI, easy login system, user authentication. Users can also keep important short note.

TABLE OF CONTENTS

CONTENS	PAGE
Approval	v
Declaration	v
Acknowledgements	v
Abstract	v
List of Tables.....	vii
List of Figures	v- v
CHAPTER 1: Introduction	1-4
1.1 Introduction	1
1.2 Motivation	2
1.3 Objectives	2
1.4 Expected Outcome	3
1.5 Report Layout	4
CHAPTER 2: Background	5-9
2.1 Introduction	5
2.2 Related Works	5
2.3 Comparative Studies	5
2.4 Scope of the Problem	8
2.5 Challenges	8
CHAPTER 3: Requirement Specification	10-23
3.1 Business Process Modeling	09
3.2 Requirement Collection and Analysis	10
3.3 Use Case Modeling and Description	11
3.4 Logical Data Model.....	20
3.5 Design Requirements	22
CHAPTER 4: Design Specification	24-43
4.1 Front-end Design	23
4.2 Back-end Design	36
4.3 Interaction Design and UX	40
4.4 Implementation Requirements	41

CHAPTER 5: Implementation and Testing	44-49
5.1 Implementation of Database	42
5.2 Implementation of Front-end Design	45
5.3 Implementation of Interactions	46
5.4 Testing Implementation	47
5.5 Test Results and Reports	48
CHAPTER 6: Conclusion and Future Scope	51-51
6.1 Discussion and Conclusion	50
6.2 Scope for Further Developments	50
REFERENCES	51-52
APPENDIX	53-55
PLAGIARISM	56

LIST OF TABLES

TABLES NAME	PAGE
-------------	------

Table 2.3 Comparative studies	06
Table 3.3.1: Use case description of registration	12
Table 3.3.2: Use case description of login	13
Table 3.3.3: Use case description of homepage	13
Table 3.3.4: Use case description of add personal info.....	14
Table 3.3.5: Use case description of add sticky note	15
Table 3.3.6: Use case description of save account info.....	15
Table 3.3.7: Use case description of delete account info	16
Table 3.3.8: Use case description of generate security code.....	16
Table 3.3.9: Use case description of view personal info.....	16
Table 3.3.10: Use case description of view account info	17
Table 3.3.11: Use case description of view sticky note	17
Table 3.3.12: Use case description of update profile picture	18
Table 3.3.13: Use case description of update personal info.....	18
Table 3.3.14: Use case description of delete note	19
Table 3.3.15: Use case description of update account info.....	19
Table 3.3.16: Use case description of logout	20
Table 3.3.17: Use case description password recovery.....	21
Table 5.4: Testing Implementation	47

LIST OF FIGURES

FIGURES	PAGE
---------	------

Figure 3.1: Data follow diagram of the system.....	10
Figure 3.2: Waterfall model	11
Figure 3.3: Use case model	13
Figure 3.4: Logical data model	22
Figure 4.1.1: Home page	24
Figure 4.1.2: User registration UI	25
Figure 4.1.3: User registration UI	26
Figure 4.1.4: User registration UI part 3	26
Figure 4.1.5: User home page	27
Figure 4.1.6: Save account information popup window	27
Figure 4.1.7: View account information page	28
Figure 4.1.8: Selecting URL for seeing account information	28
Figure 4.1.9: Generating code for seeing account information	29
Figure 4.1.10: Edit account information	29
Figure 4.1.11: Delete account information popup window	30
Figure 4.1.12: Sticky note page	30
Figure 4.1.13: View sticky note page	31
Figure 4.1.14: Edit sticky note page	31
Figure 4.1.15: Personal information page	32
Figure 4.1.16: Account all information page	32
Figure 4.1.17: Edit basic information page	33
Figure 4.1.18: Edit personal information page	33
Figure 4.1.19: Reset password page	34
Figure 4.1.20: View profile picture page	34
Figure 4.1.21: Update profile picture page	35
Figure 4.1.22: Recovery password step one	35
Figure 4.1.23: Recovery password second step	36
Figure 4.1.24: Recovery password optional step	36
Figure 4.2.1: Model view controller diagram	37
Figure 4.2.3: View class	38
Figure 4.2.4: Model class	38
Figure 4.2.5: Controller class (Servlet controller).....	39
Figure 4.2.6: AES encryption and decryption flow chart	41

Figure 5.1.1.1: Secure password manager database normal form 44
Figure 5.1.1.2: Secure password manager database relationship form 45
Figure 5.1.2: Secure password manager database 46

CHAPTER 1

Introduction

1.1 Introduction

Day by day increasing use of information technology in our daily lives, with corresponding also increasing number of user accounts. Therefore, users sign up many accounts and it is necessary to give password. It is important to sign up with a strong password by mixing letters, numbers, and special characters but who can remember such passwords in long time or short time. It is very risking, if writing them down on a piece of paper that others will see them. As a result, maximum people often using easy passwords to remember like their name or birthday and sometime people are used same password that are already used in other apps those are very insecure. Therefore, at the end up users got too many accounts that having many passwords, so it is very difficult to remember that entire password. If users use secure password manager then only users have to remember one single master password.

Nowadays, many security attacks on the internet increase day by day and password-based authentication on the web is insecure. It also provides some protection against hackers. In secure password manager have been used many security question for password saving and used encryption algorithm. Password is saved to entering many encryption layers for better security.

Secure password managers will not allow you to auto fill forms, you need to sign up here and after login you can keep your all password, keep secret notes. Secure password manager provide you with encrypted online storage for storing. It provide to the all users best security for saving password. Secure password manager manage your all passwords is like having your own personal assistant to remember.

It is the time for you to start thinking passwords and find easier path to manage those passwords. A secure password manager can be a lifesaver for getting that task done and saves from serious difficulty.

1.2 Motivation

Nowadays all of us are known that security has become the biggest issues to consider in computers. Everyday new tools are developed to prevent the security issues of the users, at the same time new techniques are also developed to reduce that security. The most common way to provide security for all users that is the user authentication, which is only possible for giving by strong password and which is unique for every user. Strong password acts as defense against unauthorized access. Every day we would be logging into email, social media and banking accounts, and also student may need to access into student portal, so it's our daily basis, we monitoring and count that the majority of us have need to have tens or more unique passwords for the sites we frequently visit. Consequently, it would be impossible to remember that password on the daily basis. This kind of problem that we faced daily that motivated us. Another thoughtful topic is the weakest password, Maximum people chooses weak password and does not follow proper password policy. This behavior also motivated us to understand the user's password security and management.

1.3 Objectives

Passwords are the most usable form of authentication for accessing a computing resource or information technology. The purpose of this secure password manager is to establish a standard for the creation of strong passwords for user, the protection of those passwords. It provides guidance on keeping and retrieving passwords in ways that maximize security of the password and minimize misuse of the password.

- The purpose of this project is to manage your password in secure way.
- The secure password manager competently manage a strong and effective keeping password security system with include to protecting personal data.
- It keeps your passwords safe and gives you to the benefits of make complex passwords without the trouble of remembering this password.
- To improve your password security with multiple unique passwords, it used encrypted and managed securely through a complex master password with security question.

- It makes easy to manage passwords, providing security question and automatic code generator.
- Secure Password Manager will take a load off your mind, freeing up brainpower for doing productive things rather than remembering a long list of passwords.
- Secure password manager helps users store, manage, and protect their passwords and sticky note.
- Password managers provide oversight, user management and security controls at the personal and the organizational level.
- These solutions goal to remove the disappointment, solving reset problem, and security risk connected with poorly managed passwords in the workplace.
- You can put your entire password in one database, which is encrypted.
- If someone hack your database even he/she do not able to see your actual value. Therefore, all your information is more secure than others are.

1.4 Expected Outcome

- Provide better user password security service.
- Secure password manager encrypt/decrypt password using Classical Encryption Techniques and Advanced Encryption Standard algorithm. These ciphers algorithms are consider as being very secure.
- Saving user all passwords in encrypted way in database.
- User can search password by specified URL from the databases.
- User can save, editing, searching, deleting and viewing user password information.
- Use can see its saved password by answering of its security question or security code.
- User can also saving, editing, deleting and viewing his/her personal details or basic information.
- User can set update, delete his/her profile picture
- User can keep, delete & view short note of their daily activities
- User can recover his/her own password by answering security question or entering security code, which is sent to be user's cell phone.

- Help user to remember password with security questions and automatic code generator.
- Users do not waste time with login problems.
- Stop worrying about remembering & keeping password secure.

1.5 Report Layout

Chapter 1: Introduction

In this chapter, we have discussed about the introduction, motivation, objectives and expected outcome of the project.

Chapter 2: Background

Here, we discuss about the background circumstances of our project. We also discuss about the related works, comparison to other candidate systems with our application, the scope of the problem and challenges of the project.

Chapter 3: Requirement Specification

In this chapter, we have discussed about the requirements such as business process modeling, the requirement collection and analysis, the use case model of the project and their description, the logical data model and the design requirements.

Chapter 4: Design Specification

In this chapter all the designs of the project. Front-end design, back-end design, interaction design, UX and the implementation requirements.

Chapter 5: Implementation and Testing

This chapter contains the implementation of database, front-end designs, interactions, test implementation and the test results of the project. Here we design normal and relationship from of database.

Chapter 6: Conclusion and Future Scope

This is the last chapter of our project report. In here, we discussed about the conclusion and the scope for further developments.

CHAPTER 2

Background

2.1 Introduction

One of the most crucial components of staying secure online is making sure that your account passwords do not fall into the wrong hands. Now there are available password manager on online so how user can understand which one is better for them and which will provide better security. This section describes about similar existing work of password manager and their methodology, limitation, etc.

2.2 Related Works

In this short section, we briefly introduce different available password manager application. There are the different types of password management software available now but we merely consider of password manager is a Web application that you can use from any Internet-connected device. We considered only real systems that already usable to all users.

Some of existing applications are [11]:

- LastPass
- 1Password
- KeePass
- Dashlane
- Keeper

2.3 Comparative Studies

In this section, we would try to provide a basic overview of different kind of password manager. Password managers differ in many aspects, including database format, functionality, supported platforms, availability, user-friendly, reliability, security etc.

Table 2.3 represents the comparative studies between existing application and our project. The basic comparison table 2.3 uses columns for password manager's name, methodology, and limitation the application, and rows for the attributes. In this table, it

allows for quick and easy comparison between each offering's features and characteristics.

Table 2.3 Comparative studies

SL	Name	Methodology	Limitation
1	LastPass [9]	<ul style="list-style-type: none"> → Syncs with multiple devices and platforms. → Works with many browsers. → Notifications appear in toolbar to save new usernames and passwords. → Unlimited stored logins. → The basic version of Lastpass is free but the Premium version of Lastpass is \$12 per year and Lastpass Enterprise is also available for businesses. 	<ul style="list-style-type: none"> → Tries to save passwords multiple times which results in duplicate entries or outdated entries → Hacked in 2015 → Live chat would be helpful for support → It's not offline base
2	1Password [9]	<ul style="list-style-type: none"> → Syncs with Dropbox → App integrations for mobile → Compatible with Chrome, Firefox, Internet Explorer, Opera, Safari, Android, iOS, Mac, Windows → Free Version 	<ul style="list-style-type: none"> → Doesn't keep you logged in → Asks to save a password that's already been save → Pro Pricing is high → Recently 1Password moved from a one-time purchase to a subscription based business model (\$2.99 per month for an individual account, \$4.99 per month for a family account supporting five people[1]) → Performance is not

			<p>consistent</p> <ul style="list-style-type: none"> → Search bar to find saved passwords doesn't work well
3	KeePass [9]	<ul style="list-style-type: none"> → 100% free → Performs well on Windows → Password strength report → Great reputation 	<ul style="list-style-type: none"> → Downloading the Mac version was confusing and once it was downloaded it wouldn't open → Wasn't able to use this password manager due to the inability to open after download → Difficult to keep synced between devices → Outdated looking site
4	Dashlane [9]	<ul style="list-style-type: none"> → Password sharing → Password Changer, automatically changes all or a selected set of passwords with one click → Compatible with: Chrome, Firefox, Internet Explorer, Opera, Safari, Android, iOS, Mac, Windows 	<ul style="list-style-type: none"> → Expensive → Not the best email support → Setting up 2FA required research, it wasn't self-explanatory
5	Keeper [9]	<ul style="list-style-type: none"> → Free 30 day trial → Ability to import/export stored data → Find duplicates feature → Pre-loaded onto AT&T devices → Secure file storage 	<ul style="list-style-type: none"> → Form fills are more difficult to use → No password strength report → Expensive → Didn't simplify the login process → Outdated interface
6	Our Project	<ul style="list-style-type: none"> → Totally free → Password does not change automatically. It depends on user. → Secure data storage. → Works with many browsers 	<ul style="list-style-type: none"> → Don't provide auto form fills service. → It's not offline base → It's not for available device

		(Chrome, Firefox, Internet Explorer and Safari etc.) → Don't need to installing any software. Only having any browser user can access it. → It is online base → Users love it → Simplify the login process → User friendly UI → Easy to understand → Easy to manage	
--	--	--	--

2.4 Scope of the Problem

We are decided to develop an application for the users so that user can store password in secure place in easy way. Because there are some existing or related solution are already having, but there are much more limitation and problems of that existing application. Many of them are expensive and critical to use and did not provide better security of database. Therefore, user's data is not safe there. We provide security of user data by using different layer of security with encryption algorithm also provide user friendly UI.

2.5 Challenges

We used the model-view-controller pattern in our project. Java frameworks come with a lot more built in for things deployment and java has the tools to do this built in. so we have to learn the tools and to do things that make Java hard to start.

User may think two types, one, if the same password used for accessing all systems that is very insecure. On the other hand, when different passwords are used for different systems, users may have the tendency to choose easy password to remember or weak passwords that is jeopardize the security of the systems concerned. There is also a higher chance of users forgetting their passwords to update in password manager, which has reset. It is also challenging.

Secure password managers handle sensitive data like user password that is save into database passing four encryption layer and same layer also be used in decryption that was also challenge for us.

CHAPTER 3

Requirement Specification

3.1 Business Process Modeling

Mainly business process modeling allow you to represent your process in a digital way and it's gives everyone a clear understanding of how the process works and you can analyze it. Usage of diagram that helps you to visualize this process and make better decisions. In this section, we represent our business model by using data flow diagram (DFD). DFD is a one kind of technique that shows the flow of data from one site to another. It represents how the processes link together through data stores and how the processes relate to the users and the outside world. Figure 3.1 shows the Data flow diagram of the system.

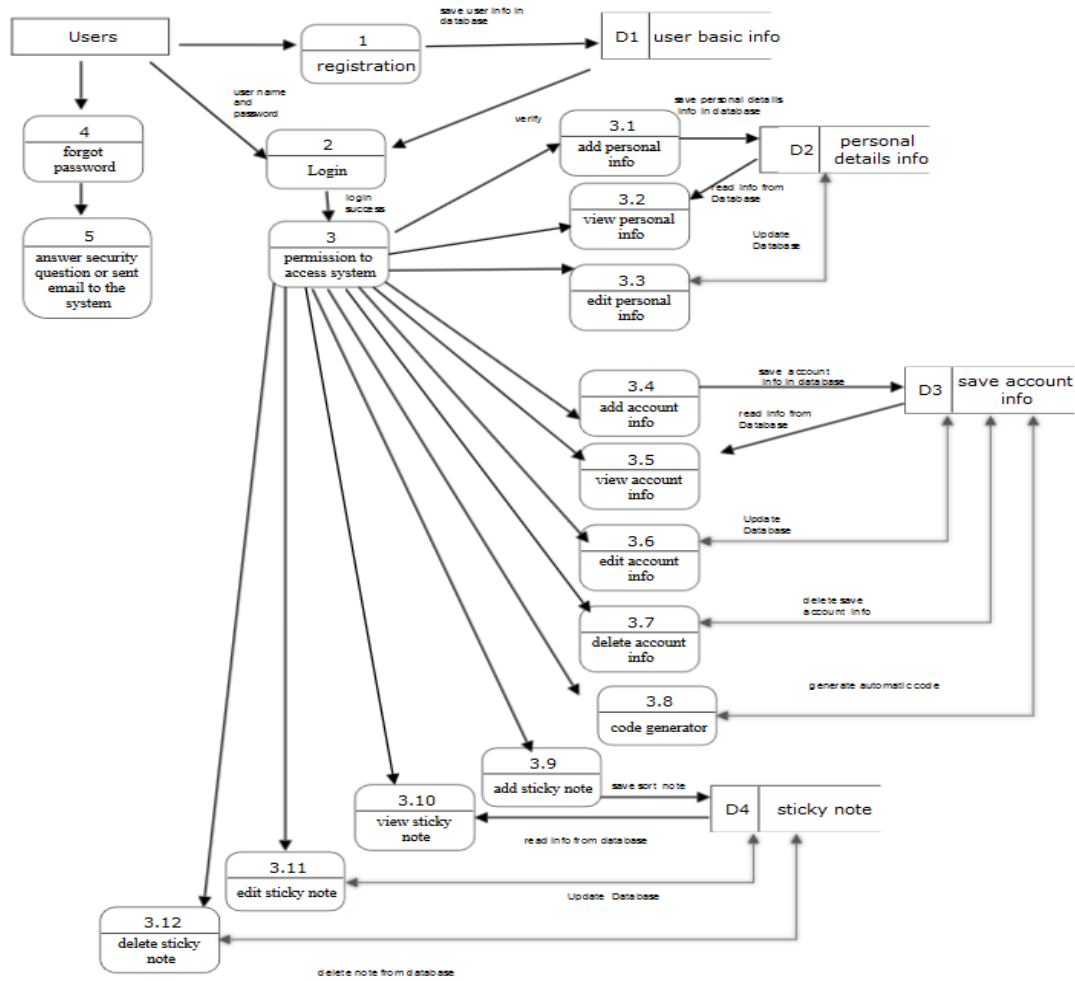


Figure 3.1 Data flow diagram of the system

Waterfall model

Waterfall Model illustrates the software development process in a linear sequential flow. It is very simple to understand and use. In a Waterfall model, each phase must be completed before the next phase can begin and there is no overlapping in the phases. In “The Waterfall” approach, the whole process of software development is divided into separate phases. The waterfall model is a sequential design process in which progress is seen as flowing steadily downwards through the phases of requirements, design, implementation, verification and maintenance. [2]



Figure 3.2: Waterfall Model [2]

3.2 Requirement Collection and Analysis

The requirement collection and analysis process is the most important phase of any project. The system development life cycle (SDLC) first phase is the requirements gathering and analysis. Collecting requirements for the project is the most important part. When collecting the requirements; it must notice that the requirements are realistic, specific and measurable.

After collecting requirements for the system, the project team begins to analyze the requirements. Then, analyze each requirement to ensure the requirement can be included in the software without causing problems with system functionality.

There are four types of requirements, those are

- a) User requirements
- b) System requirements
- c) Functional requirements
- d) Nonfunctional requirements

3.2.1 User requirements

In user requirements, consider the users expectations, including who will use the system, how the users will use the system etc. In our project, we consider user requirements from user's point of view.

3.2.2 System requirements

System requirements are one kind of documentation that represent the features and behavior of a system. It is the configuration of a system that must have in order for a hardware or software application to run smoothly and efficiently. Our system is online base so user must have internet connection it is one of the example of our system requirements.

3.2.3 Functional requirements

Functional requirement mean what system must do. It defines the system functionality .in functional requirements take care to be precise & unambiguous. In our system contain many functional requirement like if any user want to access our system at first they have to registration and then login after that they are allow to access to our system.

3.2.4 Nonfunctional requirements

Nonfunctional requirements mean a quality that the system must have liked as secure, reliable, quickly, easy to use, compliant with Data Protection legislation etc. In our system we provide better security, user-friendly user interface and easy to access.

3.3 Use Case Modeling and Description

Generally, a use case diagram is a graphical representation of the interactions among the elements of a system. It is used to describe a set of actions means use cases that some system with one or more external users of the system means actors and it is also used in system analysis to identify, clarify, and organize system requirements.

Below all tables, show the Use Case Modeling.

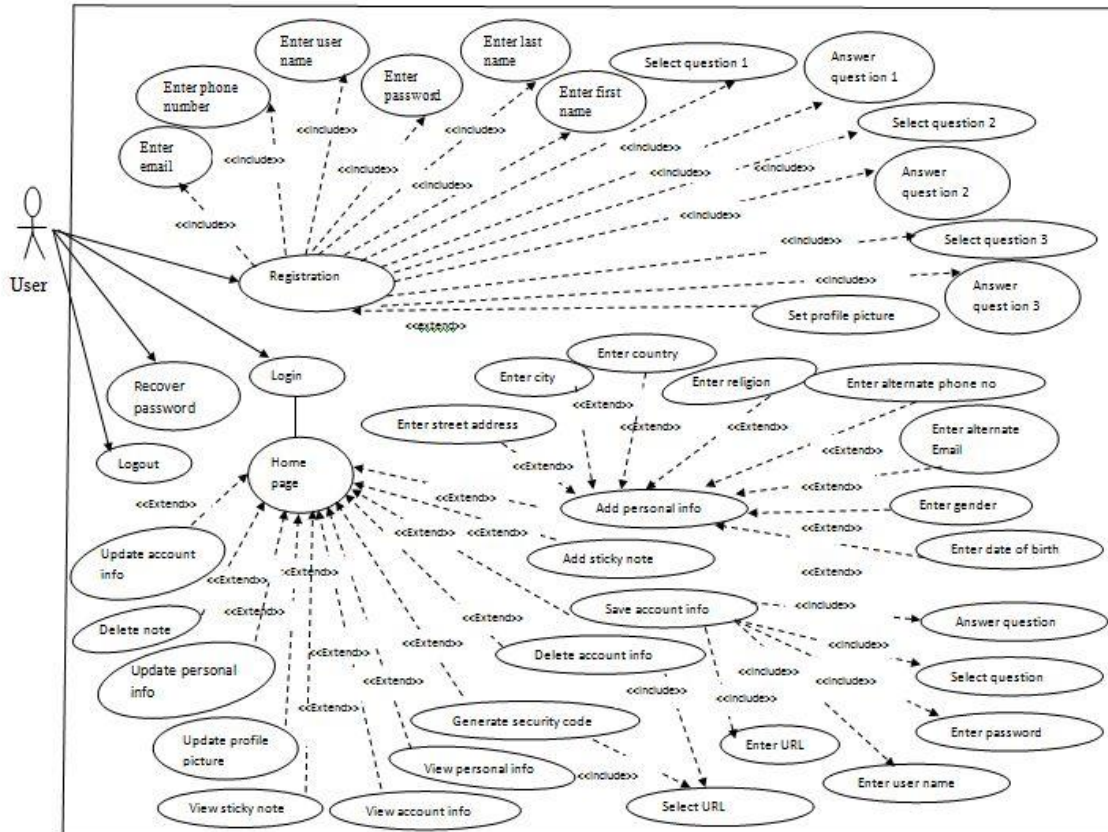


Figure: 3.3 use case model

Table 3.3.1: Use case description of registration

Use case #01	Registration
Actors	User
Type	Primary
Description	Here, registration process is divided into to two steps. First is the basic information and another is security question. In first step, basic information is first name, last name, email, phone number and password is required. In second step user must select three questions and answer those questions. If user wants, user may add extra question and answer but this is not mandatory to do.

Uses	First name, Last name, Email, Phone number and password, question 1, answer 1, question 2, answer 2, question 3, answer 3.
Extended by	Set profile picture
Extends	None

Table 3.3.2: Use case description of login

Use case #02	Login
Actors	User
Type	Primary
Description	User must enter correct user name and password. Valid username and password allow user to access the user home page.
Uses	None
Extended by	None
Extends	None

Table 3.3.3: Use case description of homepage

Use case #03	Homepage
Actors	User
Type	Primary
Description	<ul style="list-style-type: none"> • User able to save different account such as Face book, Gmail etc. • User able to add personal info, add sticky note, update personal information, update account information, delete account

	<p>information, update profile picture and user can reset username and password.</p> <ul style="list-style-type: none"> • User can view his /her saved account information by answering security question or generate secure code and view personal information, sticky note. After viewing sticky note user can delete saved note.
Uses	None
Extended by	Add personal info, save account info, delete account info, generate security code, view personal info, view account info, update profile picture, update personal info, and update account info.
Extends	None

Table 3.3.4: Use case description of add personal info

Use case #04	Add personal info
Actors	User
Type	Primary
Description	User can able to save his/her personal information here such as street address, city, country, religion, alternative email, alternative cell phone number and date of birth. This not mandatory but user can do if user want.
Uses	None
Extended by	Street address, city, country, religion, alternative email, alternative phone number and date of birth
Extends	None

Table 3.3.5: Use case description of add sticky note

Use case #05	Add sticky note
Actors	User
Type	Primary
Description	User can able to save short note or sticky note. When users want to save sticky note, user must fill two fields this are title and description. Here have automatic date and time that is saved with each note.
Uses	None
Extended by	None
Extends	None

Table 3.3.6: Use case description of save account info

Use case #06	Save account info
Actors	User
Type	Primary
Description	User can save different kind of account here with better security. When saving account user must be filled up URL, username, password and a security question. Then user may able to save information.
Uses	None
Extended by	Street address, city, country, religion, alternative email, alternative phone number and date of birth
Extends	None

Table 3.3.7: Use case description of delete account info

Use case #07	Delete account info
Actors	User
Type	Primary
Description	If user want to delete his/her saved account information. Users have to select URL then confirm delete button.
Uses	None
Extended by	Select URL
Extends	None

Table 3.3.8: Use case description of generate security code

Use case #08	Generate security code
Actors	User
Type	Primary
Description	When user forgot to security question answer, here has an option to recovery this kind of situation. When user select ULR system generate a code that is send to the user's phone.
Uses	None
Extended by	Select URL
Extends	None

Table 3.3.9: Use case description of view personal info

Use case #09	View personal info
--------------	--------------------

Actors	User
Type	Primary
Description	User can able to view his/her personal information that is provided to the system.
Uses	None
Extended by	None
Extends	None

Table 3.3.10: Use case description of view account info

Use case #10	View account info
Actors	User
Type	Primary
Description	Mainly user can view his/her saved different account information in two way one is answering security question another is entering security code.
Uses	None
Extended by	None
Extends	None

Table 3.3.11: Use case description of view sticky note

Use case #11	View sticky note
Actors	User

Type	Primary
Description	User can view sticky note with list according to save date and time.
Uses	None
Extended by	None
Extends	None

Table 3.3.12: Use case description of update profile picture

Use case #12	Update profile picture
Actors	User
Type	Primary
Description	While user are doing registration to our system by default a picture is set if user do skip. After login user can update his/her profile picture.
Uses	None
Extended by	None
Extends	None

Table 3.3.13: Use case description of update personal info

Use case #13	Update personal info
Actors	User
Type	Primary
Description	User able to change personal info.
Uses	None

Extended by	None
Extends	None

Table 3.3.14: Use case description of delete note

Use case #14	delete note
Actors	User
Type	Primary
Description	From list of note user can delete note.
Uses	None
Extended by	None
Extends	None

Table 3.3.15: Use case description of update account info

Use case #15	Update account info
Actors	User
Type	Primary
Description	User can edit saved account information by answering security question or entering code.
Uses	None
Extended by	None
Extends	None

Table 3.3.16: Use case description of logout

Use case #16	Logout
Actors	User
Type	Primary
Description	Users can logout from this system.
Uses	None
Extended by	None
Extends	None

Table 3.3.17: Use case description password recovery

Use case #17	Password recovery
Actors	User
Type	Primary
Description	If user forgot password, then user can recover its password. For recovering password user, have to enter email address into the system.
Uses	None
Extended by	None
Extends	None

3.4 Logical Data Model

The logical architecture or logical data model describes how users perceive data in the database. Logical data model is not concerned with how the data is handled and processed by the DBMS. It is concerned with how it looks.

In this method data, storage is not published only the users can manipulate the data without worrying about where it is located or how it is actually stored. Database has different levels of abstraction. Database architecture has main tree level.

- External level
- Conceptual level or logical level
- Physical level

External level

This is the view of the relational database that end users can see. An external level specifies a view of the data in terms of the conceptual level.

Conceptual level or logical level

The conceptual level or logical level where designers work. In this section, we describe of complex objects in terms of simpler ones. Here we represent logical database design.

Physical level

In physical level, we maintain a database on a hardware system.

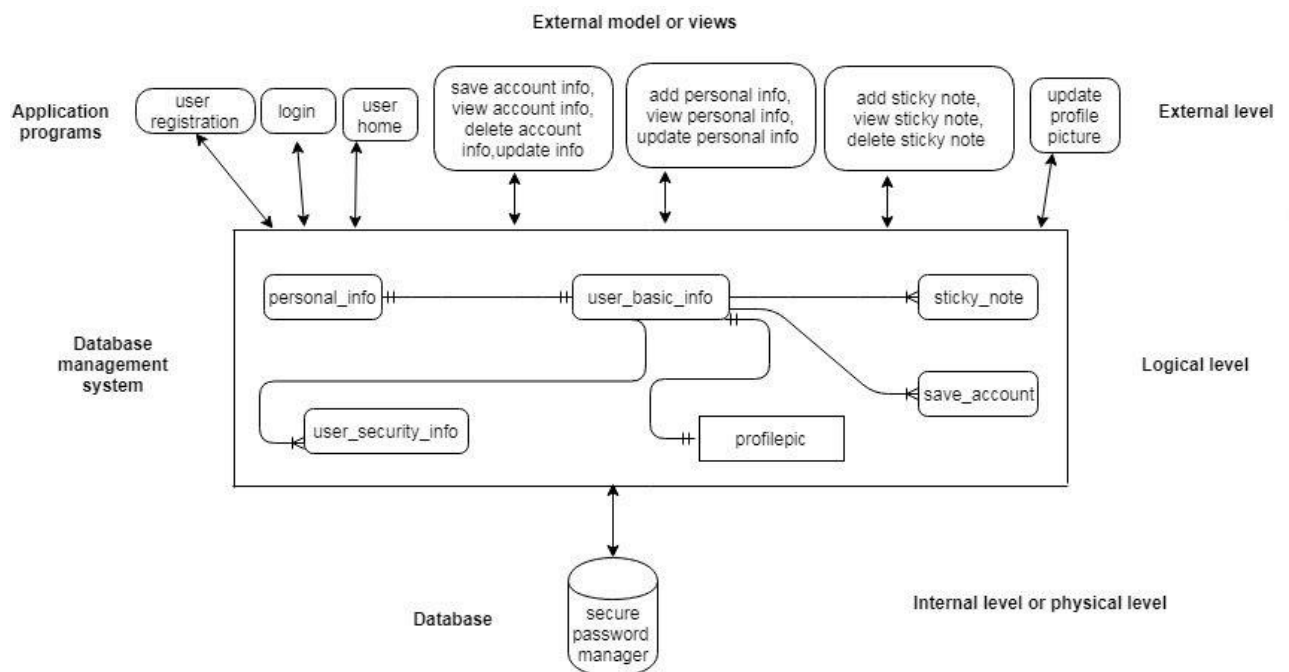


Figure: 3.4 logical data model

3.5 Design Requirements

Design requirements state the important characteristics in order to be successful. The design requirement of our project will differ from any other existing application. In our application, we mainly focused on ease of use and user friendly. We are working on our own specific problem statement and user experience. We also provide some new features by which the user can easily operate our system.

- In our application we design a registration section, In here we divide into two part first one is user personal information and second one is, select security questions and answer those questions for security purpose so any user can be registered to our application with their information.
- We design for saving different account contains multiple security question selection options.
- We design search options where user can search with specific option where after selecting option result automatic change without page reloading.
- We design an option for save sticky note here automatically date and time would be saved along with each note.
- We design a popover option, here we gather all user information together such that user can easily manage his /her information easily.

CHAPTER 4

Design Specification

4.1 Front-end Design

Front-end generally refers to the portion of an application the user will see or interact with and also referred to as the client-side and is sometimes considered "web design". Mainly the front-end defines the user interface, user interaction, and presentation of information. Front end is the essential part of any application, so it is very necessary to build up a straightforward and understandable front-end design or GUI for the user of an application. Therefore, while developing our project we tried to keep our design as simple as possible so that the user can easily access the application. We attach our application front-end design as follows:

In figure 4.1.1, shows the home screen of our application. In home page in our system, we used login process to access the application. Only authenticated person can login. For login is required to insert email and password.

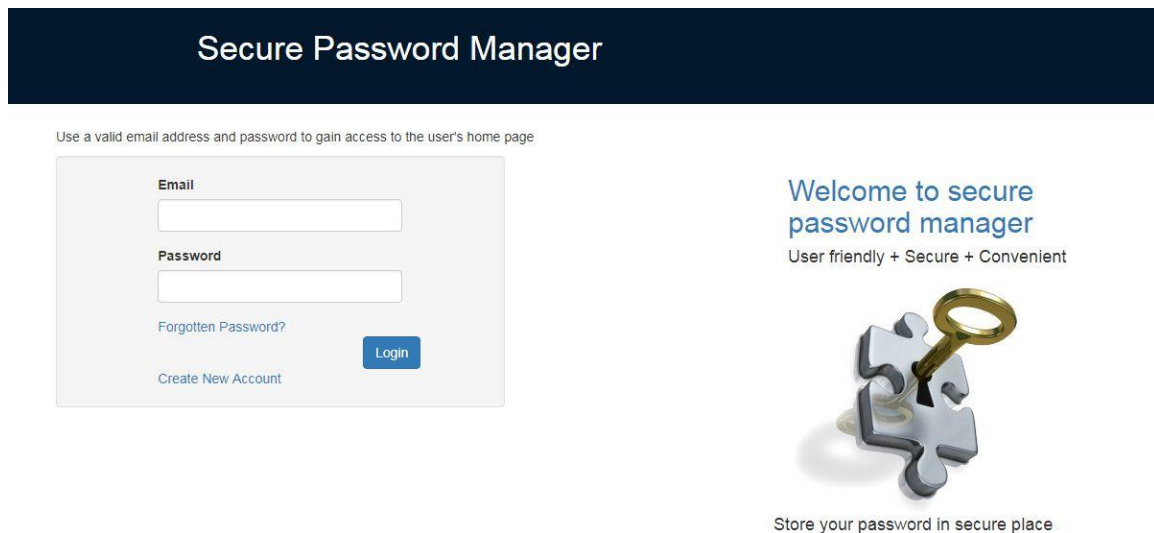
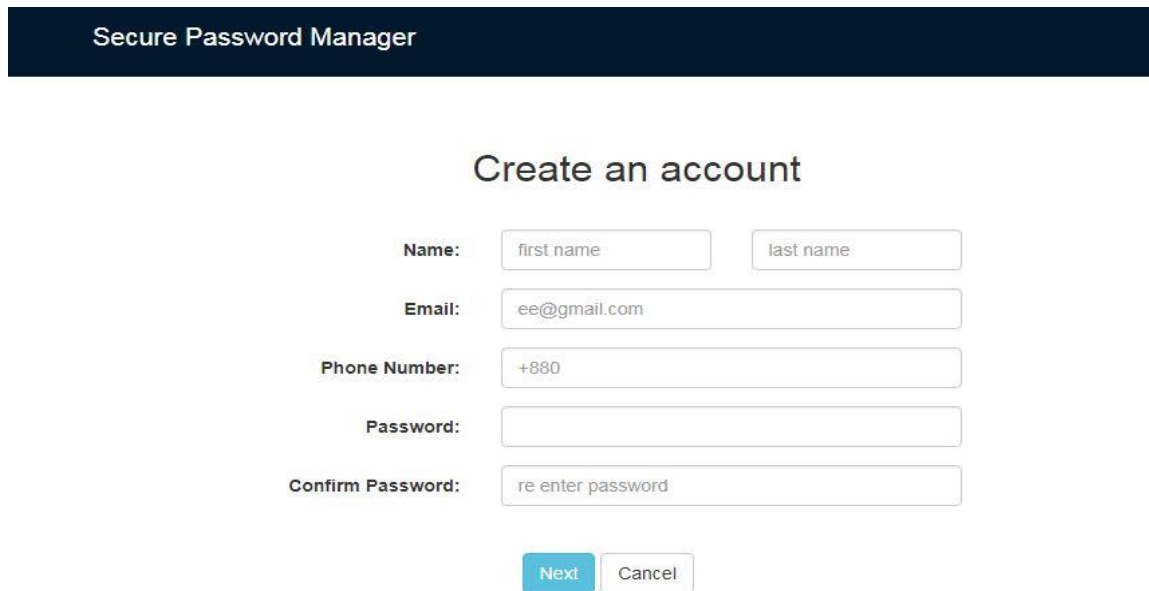


Figure 4.1.1: Home Page

Registration is provided to all the users to know whether the user is valid or not. This can be verified through several components. Three steps are required to complete registration. In figure 4.1.2, shows the registration screen of our application is the first part. If someone wants to use the application, they need to register at first by providing their name, valid email address, phone number, and password. This form requirement must be fill all objects.



The image shows a dark blue header with the text "Secure Password Manager" in white. Below the header, the title "Create an account" is centered. The registration form consists of the following fields:

- Name:** Two input fields labeled "first name" and "last name".
- Email:** One input field containing "ee@gmail.com".
- Phone Number:** One input field containing "+880".
- Password:** One empty input field.
- Confirm Password:** One input field containing "re enter password".

At the bottom of the form, there are two buttons: a blue "Next" button and a white "Cancel" button with a grey border.

Figure 4.1.2: User registration UI

In figure 4.1.3, shows the registration screen of our application is the second part. In this section user must be selected three security questions and insert those answers. If user wants, user may be able to set extra question and those answer.

Answer all security question for get better secure environment .

Security Question #1:

Answer:

Security Question #2:

Answer:

Security Question #3:

Answer:

Add New Question:

Answer:

Figure 4.1.3: User registration UI

In Figure 4.1.4, shows the registration screen of our application. It is the last part for complete registration successfully. This is not mandatory. If user want user may set profile picture or skip this.

Secure Password Manager

Set Profile Picture

No file chosen

Figure 4.1.4: User registration UI part 3

In figure 4.1.5, shows the user homepage of the application where user can keep different account information in secure way, keep short note also and manage them. User can see user's saved account information by answering security question answer or inserting security code. User can generated code with generate security code option.

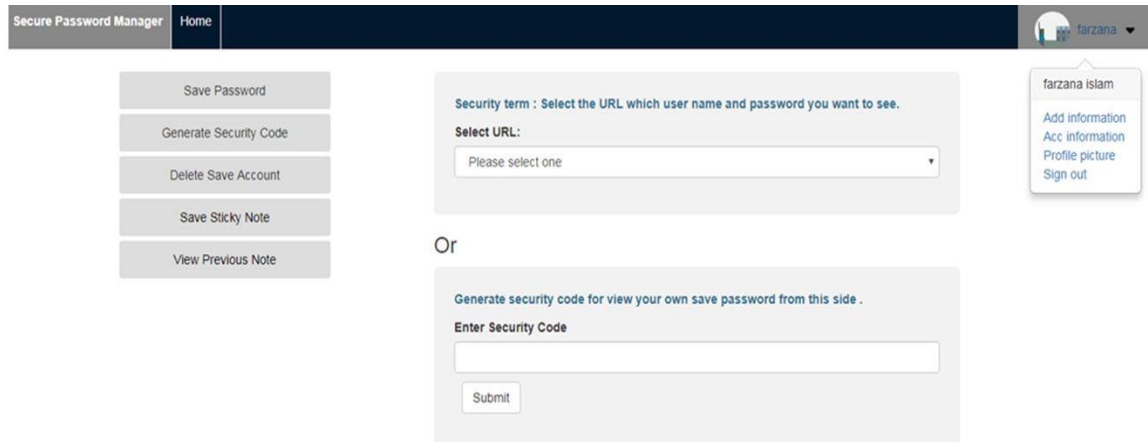


Figure 4.1.5: User home page

In figure 4.1.6 shows the save account information popup window. Here user can save account information. There all field must be filled up, those are URL, username and password. When user save this information must choose a security question and answer for getting better security.

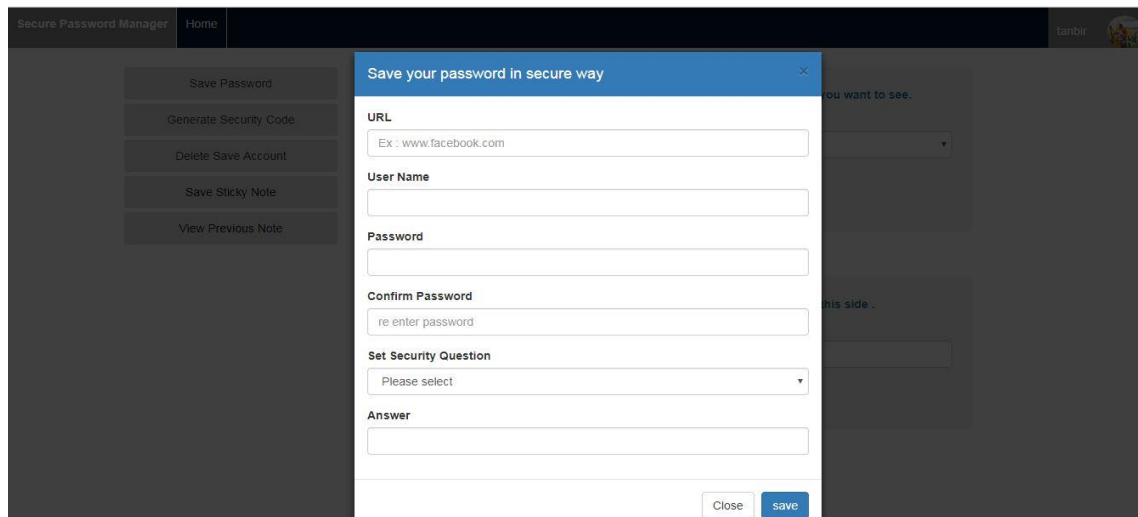


Figure 4.1.6: Save account information popup window

In figure 4.1.7, shows the view account information page where user can see account information that is saved.

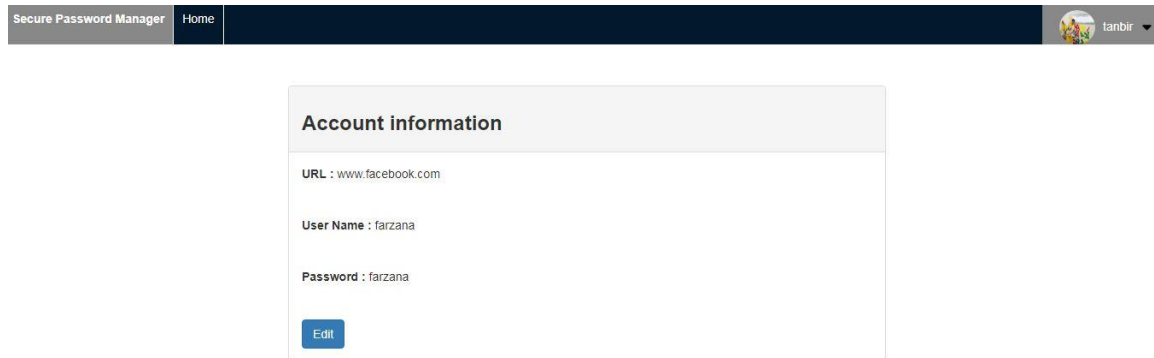


Figure 4.1.7: View account information page

There are two ways user can view the information. One is the answering security question. In figure 4.1.8, shows the user is selected a URL and then show a security question in base on selected URL.

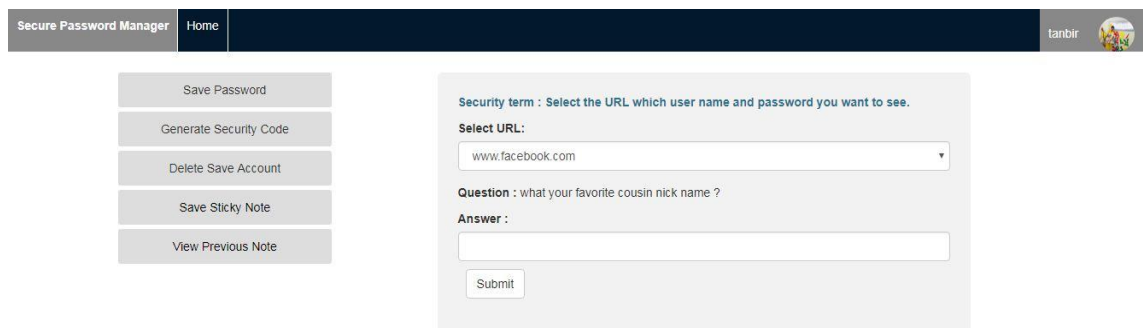


Figure 4.1.8: Selecting URL for seeing account information

Second is the generate security code. It is the optional for user. Sometimes user may forget its security question answer or may be confused spelling or else. It would be backup way for user.

In figure 4.1.9 shows a popup window, in here the user is selected a URL for generate a code that would be sent to user phone number. After getting code user insert it and can able to see the account information.

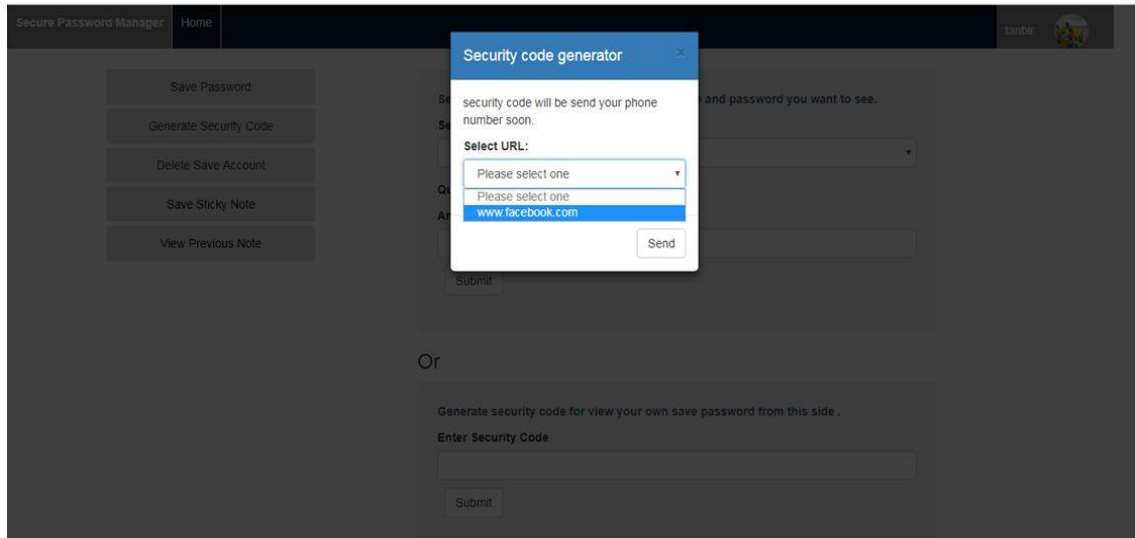


Figure 4.1.9: Generating code for seeing account information

In figure 4.1.10 shows, the edit account information page where user can edit his/her account information. Here also user can change security question and answer.

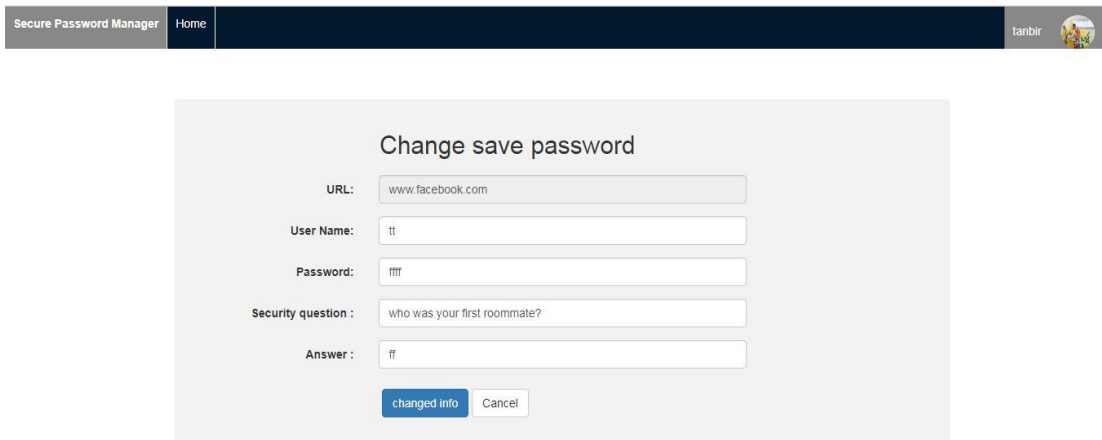


Figure 4.1.10: Edit account information page

In figure 4.1.11, shows the delete account information popup window. User can permanently delete his/her account information from the application. For deleting information user must be select a URL, which wan to delete.

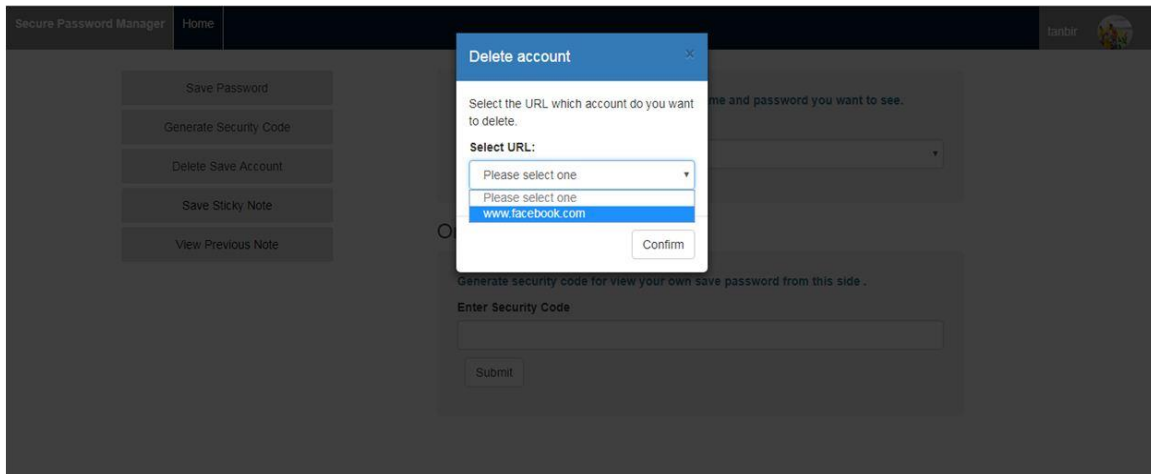


Figure 4.1.11: Delete account information popup window

In figure 4.1.12 shows the save sticky note page. User can save his/ her short note here. While saving any short note user need to set title of note, note description and auto date and time are saved with them.

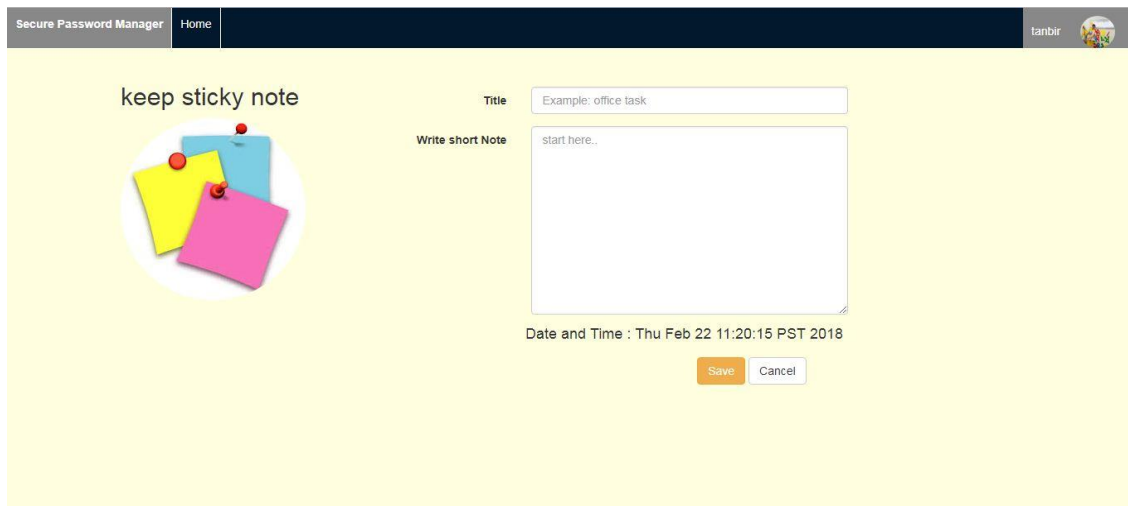


Figure 4.1.12: Sticky note page

In figure 4.1.13, shows the saved all previous notes like as list. Here have two options. One is edited and another is delete option. In delete option, notes are permanently deleted from the user account.

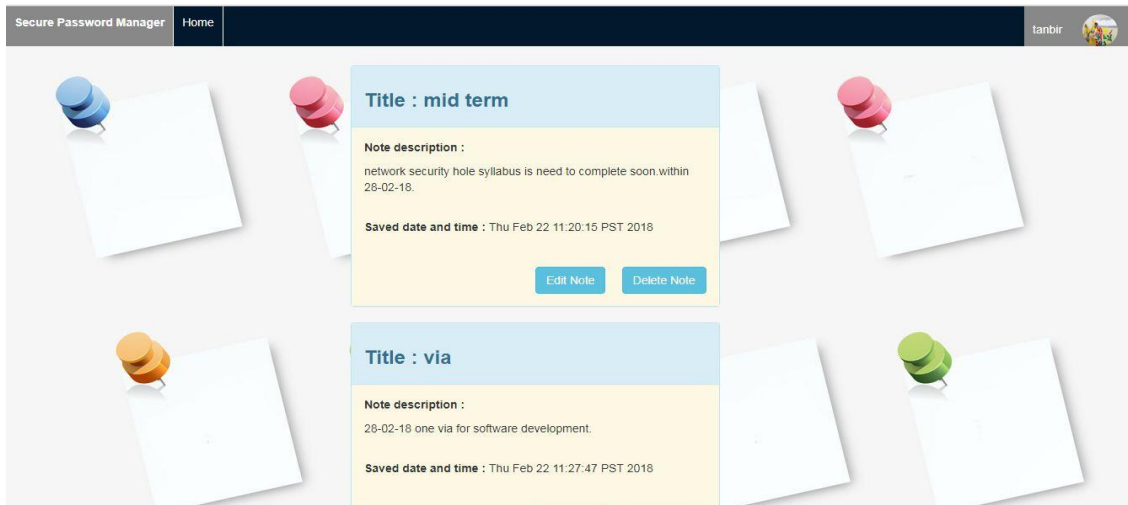


Figure 4.1.13: View sticky note page

In figure 4.1.14, shows edit sticky note page. Here user can update note title, note description and date & time.

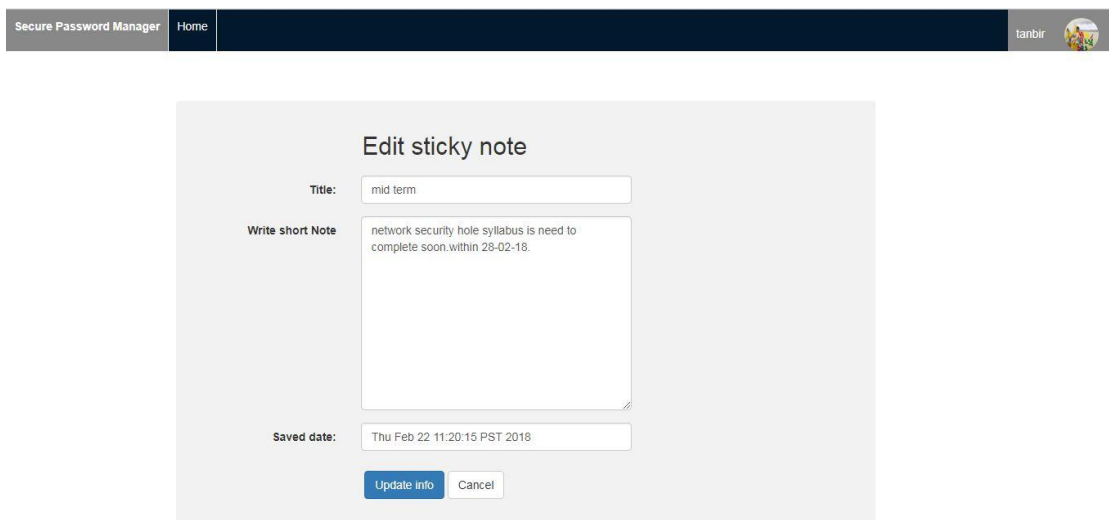


Figure 4.1.14: Edit sticky note page

In figure 4.1.15, shows add personal information page. If user wants, user can save personal information here. User can save his/her street address, city, country, and religion, date of birth, alternative email, alternative phone number and gender. All fields are optional for user.

Personal Information

Street Address:

City:

Country:

Religion:

Date Of Birth:

Alternate Email:

Alternate Phone Number:

Gender: Male Female

Figure 4.1.15: Personal information page

In figure 4.1.16 shows the account all information such as basic account information means which information user are provided when registered to the application site and personal information also user can be seen here and can to go to the edit option from here. Here have another option that is change password option.

Change Password

Basic Account Information

First Name : farzana

Last Name : islam

Email : farzana11@gmail.com

Phone Number : 57y5675

Personal Details Information

Street Address : b/0

City : meherpur

Country : bangladesh

Religion : islam

Date Of Birth : 1994-08-19

Alternate Email : farzana@gmail.com

Alternate Phone Number:

Gender : female

Figure 4.1.16: Account all information page

In figure 4.1.17, shows the edit option of the basic information to the user. User can update his/her first name, last name email and phone number.

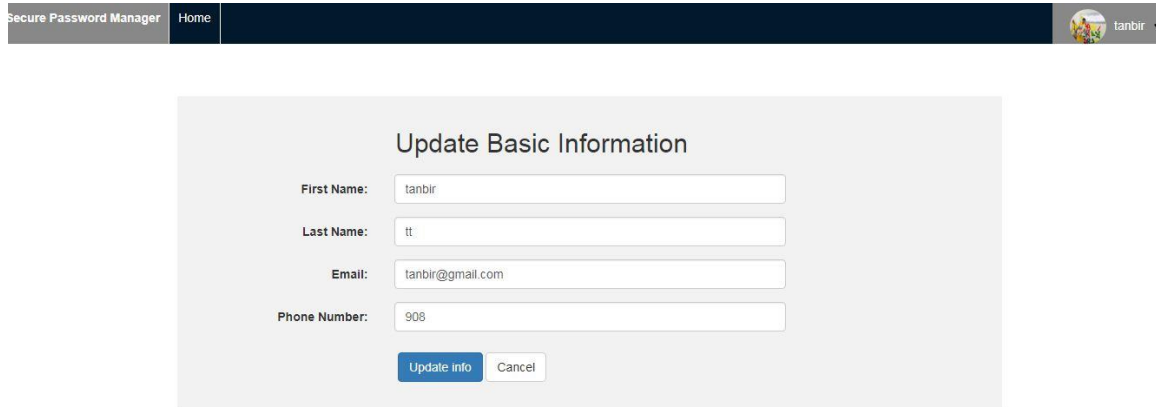


Figure 4.1.17: Edit basic information page

In figure 4.1.18, shows the edit option of the personal information to the user. User can update his/her personal information from here.

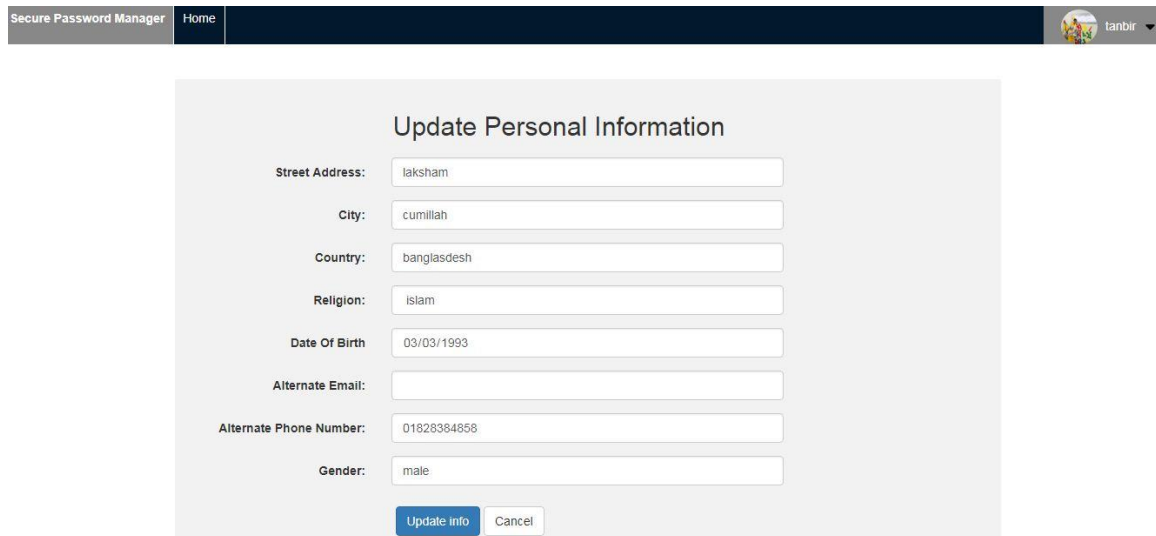


Figure 4.1.18: Edit personal information page

In figure 4.1.19, shows the password reset option. For changing password user must need to enter current password and then set the new password.

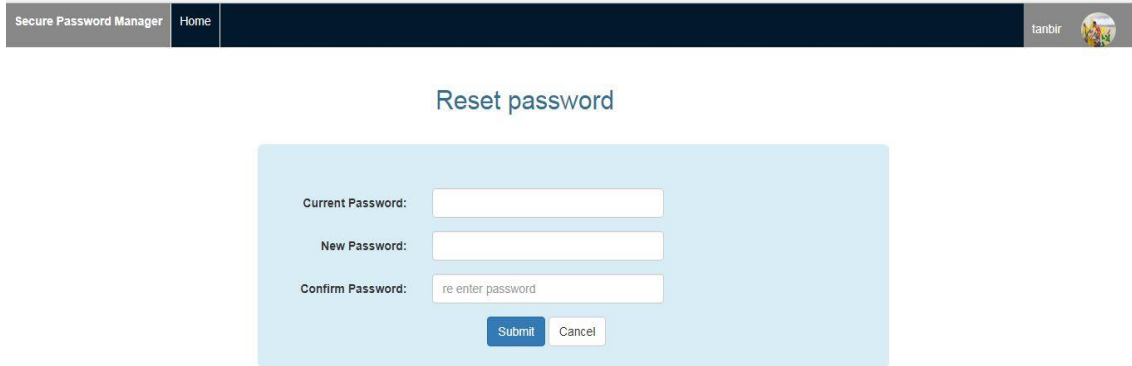


Figure 4.1.19: Reset password page

In figure 4.1.20, shows the profile picture of user. User can see the current profile picture and go to the update profile picture option from here.



Figure 4.1.20: View profile picture page

In figure 4.1.21, shows the update profile picture page. In here user can update his/her profile picture.



Figure 4.1.21: Update profile picture page

We always think of user side and think how we provide better service in easy way. On thinking of user side, in this application we have been keep recovery option for forgotten password. User must be passed two steps for recover password. In figure 4.1.22, shows the first step of recovery password.

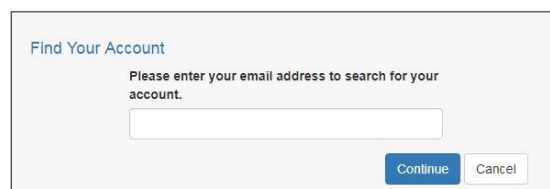


Figure 4.1.22: Recovery password step one

In figure 4.1.23, shows the second step of recovery password. Here user must be answer some questions that he/she set for security when registered to the application.

The screenshot shows a dark blue header with the text "Secure Password Manager". Below it are three light blue question boxes, each with an "Answer:" label and a text input field. The questions are:

- Question 1 : what was your favorite food as a child?
- question 2 : what your favorite cousin nick name ?
- question 3: what was your favorite food as a child?

 At the bottom right of the form area are two buttons: "Continue" and "Cancel".

Figure 4.1.23: Recovery password second step

Some user may forget its security questions answer. In this case, we have another option for password recovery. Here user must fill out a field with primary contract number. In figure 4.1.24, shows the optional step of recovery password.

The screenshot shows a password recovery interface. A "Security code generator" popup is open, displaying the text: "security code will be send your phone number soon." with a "close" button. The background interface includes a "Continue" and "Cancel" button at the top right, a heading "Did you forget your security questions answer?", and a form with a "Please enter your phone number" label, a text input field containing "0173483493", and a "send code" button. Below the form is a three-step process diagram:

- Step 1: A computer monitor icon with a hand pointing to it, labeled "1" and "ENTER YOUR PHONE NUMBER XXX XXXX XXXX".
- Step 2: A speech bubble icon labeled "2" and "YOUR PIN IS 5555".
- Step 3: A computer monitor icon with a checkmark, labeled "3" and "ENTER YOUR PIN 5555 CONFIRMED".

 Arrows connect the steps from left to right.

Figure 4.1.24: Recovery password Optional step

4.2 Back-end Design

The Back-end design is the behind part of the application. User cannot see the back-end part that handles the logic, data storage, user security, server configuration etc. The users are send all requests to the back-end and the back-end into process the incoming request, generate, and send the response to the users.

The back-end is typically includes three major parts. This is a server, an application, and a database. The server is the computer that receives requests. An application is running on the server that listens for requests, retrieves information from the database, and sends a response and Databases are used to organize and persist data. We tried to complete our project on back-end part as possible as simple way.

In our application, we worked on java web application with MVC pattern. MVC means model view controller. Model represents an object that carrying data and can have logic to update controller if its data changes. Model part only interacts with controller about data related. View represents the visualization of the data that model contains and interact with controller. It does not any direct connection to the model class. Controller works on both Model and view. It controls the data flow into model object and updates the view whenever data changes. It keeps View and Model separate.

Figure 4.2.1 shows the diagram of MVC pattern.

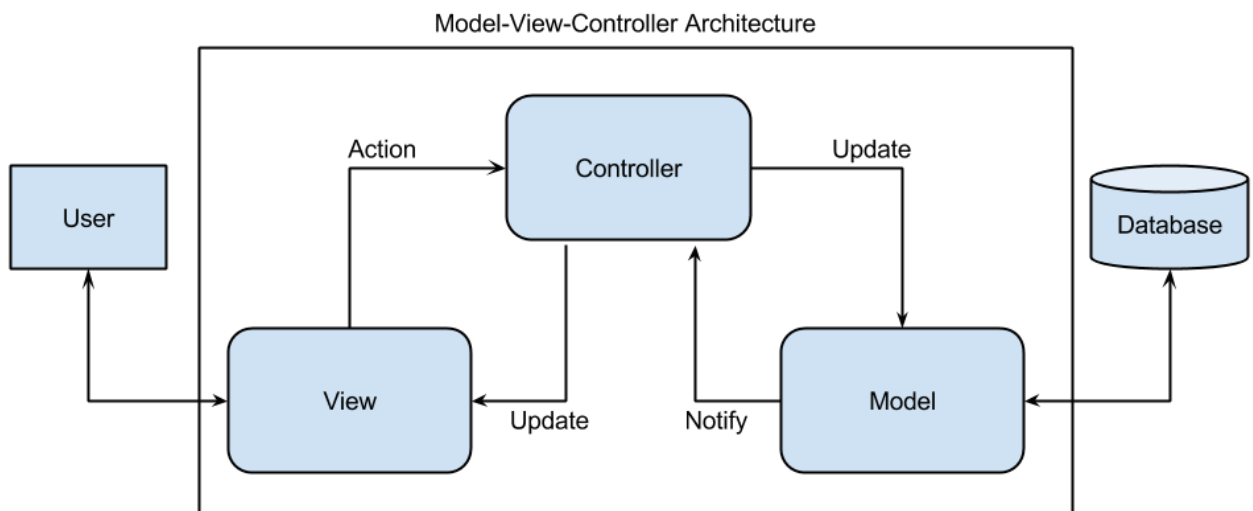


Figure 4.2.1: Model view controller diagram [3]

To developing and maintaining the back-end section, we use MySQL Database on our application. Our application's back-end design as follows:

Figure 4.2.3 shows the view class of our project. Dot jsp(.jsp) extension class the our view page. In here, we managed all view pages.

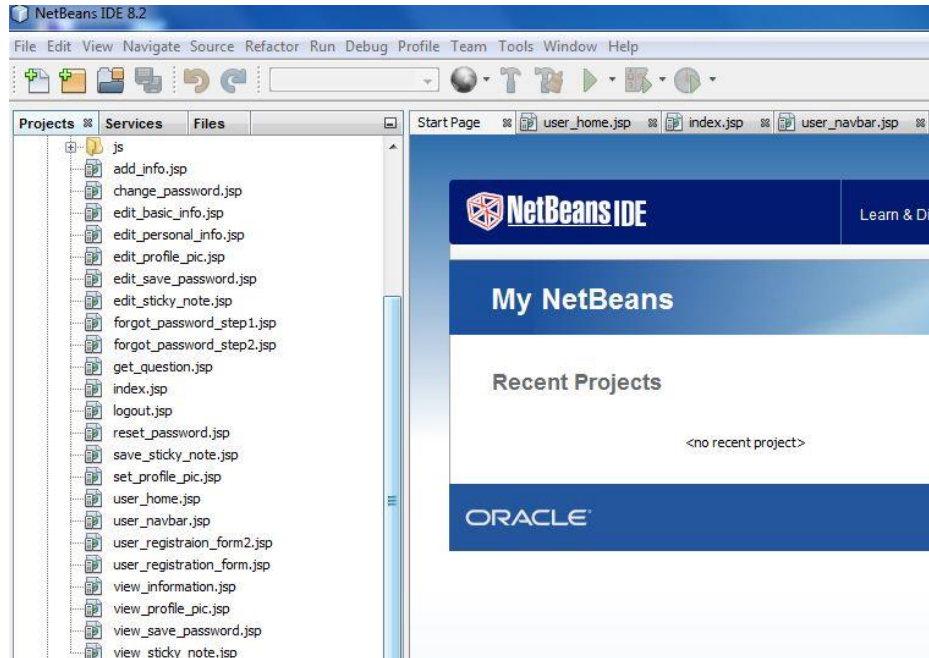


Figure 4.2.3: View class

Figure 4.2.4 shows the model class of our project. Dot java extension class the our model class within model class package

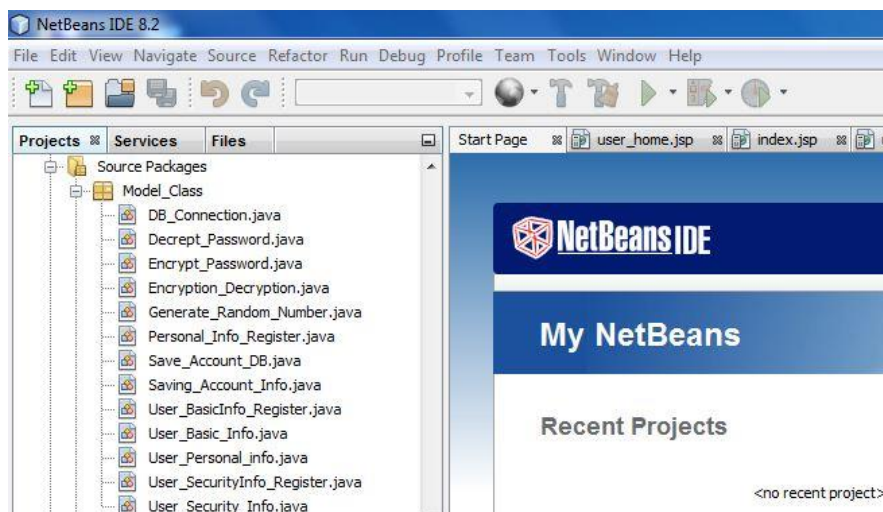


Figure 4.2.4: model class

Figure 4.2.5 shows the controller class of our project. Dot java extension class is the controller our project within the Servlet controller package. Controller controls the model class and view page. Servlet controller is the controller of our project that receives the request from user and then process with model class and sends result to the user view page.

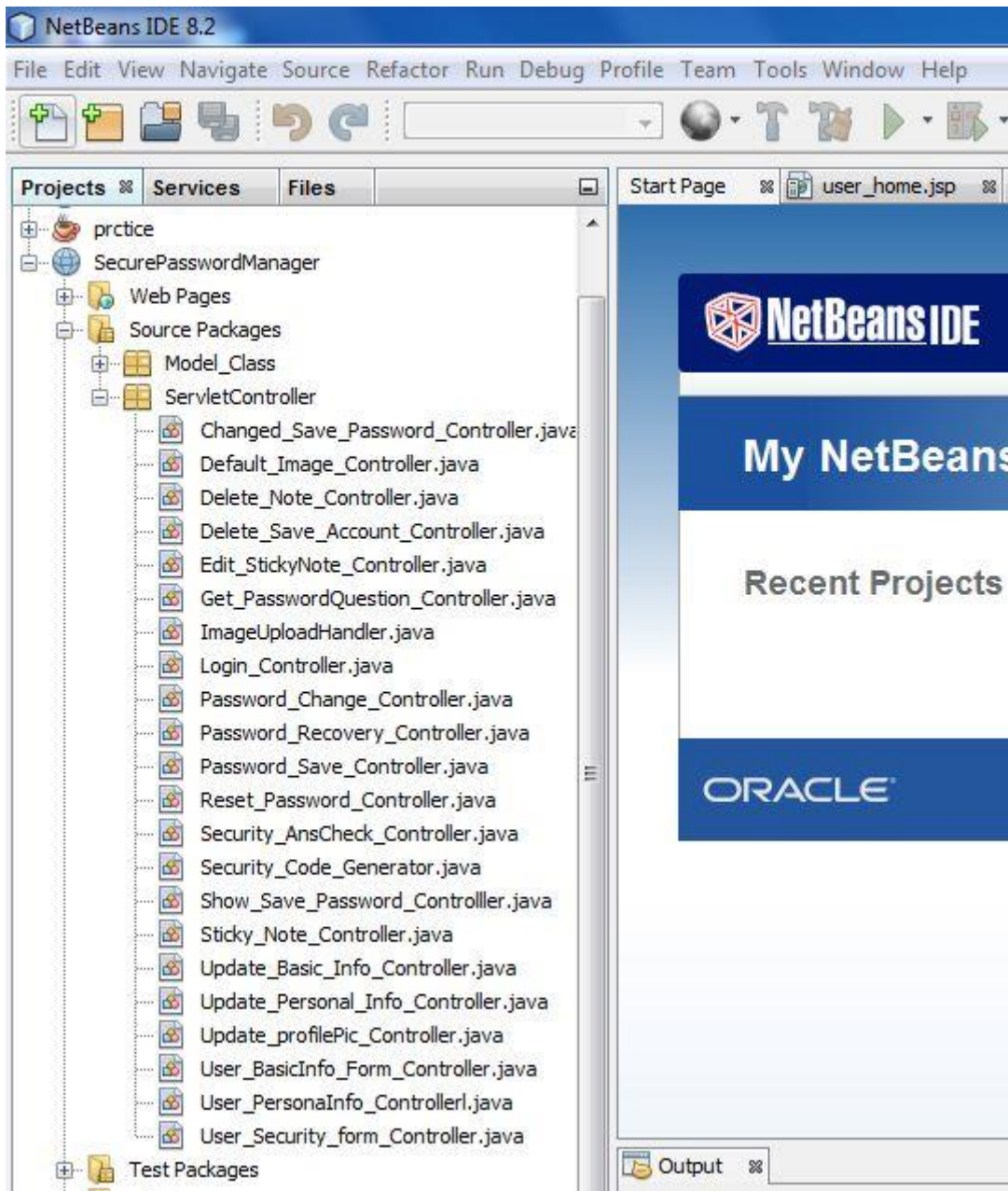


Figure 4.2.5: controller class (Servlet Controller)

In our project, we used some native and advanced encryption algorithm for user security.

Caesar Cipher 4.2.1

The Caesar Cipher technique is one of the earliest and simplest techniques of encryption. It is simply a type of substitution cipher. In here, each letter of a given text is replaced by a letter some fixed number of positions down the alphabet.

a	b	c	d	e	f	g	h	i	J	k	l	m	n	o	p	q	R	s	t	u	v	w	x	y	z
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

So, if the string is “secure password manager”. Then we convert the lowercase to uppercase then the string is “SECURE PASSWORD MANAGER”. After that If the shift value is (2) then string becomes “ UGEWTG RCUUYQTF OCPCIGT”. In this example with a shift of 2, s would be replaced by U, E would become G and so on [12].

Advanced Encryption Standard (AES) 4.2.2

AES stands for advanced encryption standard. It is a strong symmetric encryption algorithm. AES algorithm is three types. These are AES-128, AES-192 and AES-256. A secret key is used for the both encryption and decryption of data. This classification is done on the bases of the key used in the algorithm for encryption and decryption process. The numbers represent the size of key in bits. This key size determines the security level as the size of key increases the level of security increases. Only someone who has access to the same secret key can decrypt data. AES encryption provides strong protection to your data.

AES-128, AES-192 and AES-256 are similar algorithms, but with distinct numbers of rounds. AES is described as a sequence of elementary operations called rounds; rounds are (mostly) identical except that they use distinct sub keys (extracted from the main encryption key), and they are successive (each round takes as input the output of the previous round). AES-128 has 10 rounds, AES-192 has 12 rounds, and AES-256 has 14 rounds. The computation of sub keys, called the key schedule or the key expansion, also differs a bit between the three variants: with a larger key, the key schedule must work

over, indeed, a larger key, and must output more sub keys since there are more rounds to feed [4].

Encryption process rounds consist of Substitute byte, Shift row, Mix columns and Add round key while the decryption process is the reverse process of the encryption, which consists of Inverse shift row, Inverse substitute byte, Add round key and inverse mix columns. The operation of AES algorithm is shown in figure 4.2.6.

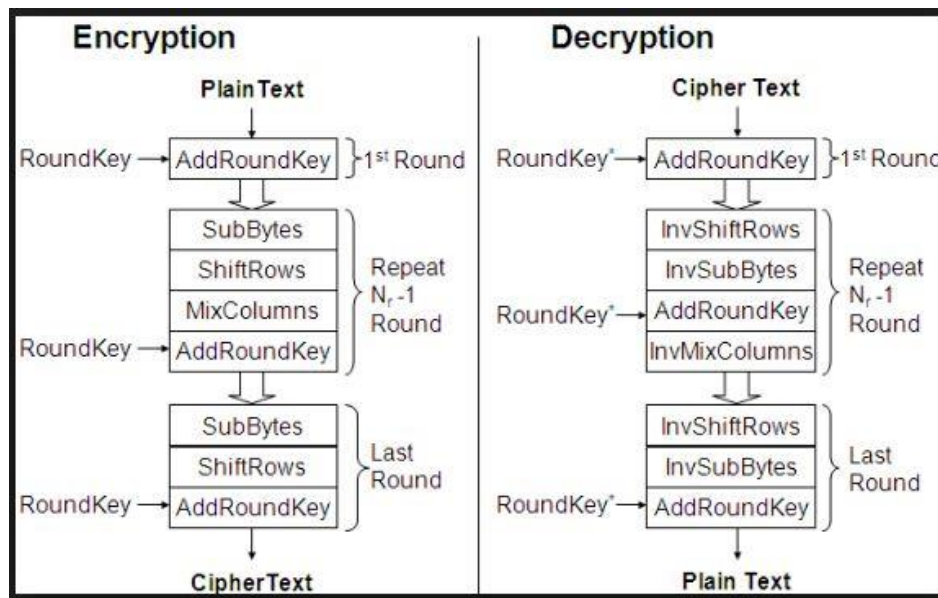


Figure 4.2.6: AES encryption and decryption flow chart [5]

4.3 Interaction Design and UX

Interaction design is specifically a methodology that represents the interaction between a system and its user. I design is just a part which is responsible for visual part and comfort of our project. It focused on how information should be presented within a system to enable the user to best understand that information.

UX is the fundament for all sides of web or application design. User experience design focuses on the overall experience between a user and application such as system response time or user support. It is not just concerned with the interactive elements but also the way that certain elements look, feels or contrive to deliver certain outputs. We have added some new feature so that user can get better experience.

4.4 Implementation Requirements

To develop a web applications are need to combine with server side programming which provide functionalities such as interacting with users, connecting to back-end databases and generating results to browsers. Therefore, our project also on web application so we worked with server side programming and used different type of tools, components those help us to developed our project successfully. In the Implementation Requirement section, we discussed about all the tools and components that we have used to develop our project.

4.4.1 Development Platform

We worked our project on NetBeans IDE 8.2. NetBeans IDE 8.2 (Integrated Development Environment) delivers excellent support for developing Web and server side applications and a Java web application generates interactive web pages containing various types of markup language and dynamic content that utilize the Java EE application framework. NetBeans IDE 8.2 is the best way to quickly learn and become productive in Java EE programming [13].

We used in our project of web components are Java Server Pages (JSP), Servlets and JavaBeans that is used to modify & temporarily store data, interact with databases and web services, and give satisfaction in response to user requests.

4.4.2 Java version

We used our project Java version jdk-8. The Java Development Kit (JDK) is required if you want to use any of the Java features. JDK is required to install with NetBeans IDE to building a Java application so JDK 8 is required to use Web and server side applications in NetBeans IDE 8.2. The JDK is a software development environment used for developing Java applications. It is the combination of the Java Runtime Environment (JRE), Java Virtual Machine (JVM), set of libraries such as jar and other files and development tools such as java, javac, javac and javaw[10].

4.4.3 Database server

We used mysql-essential-5.1 for database server. MySQL Essential is a powerful database manager that is similar in many ways to Oracle and SQL Server. MySQL Essential is a complete solution for MySQL database administration and development. MySQL Essential provides you with must have tools for administering MySQL databases, managing database schema and objects as well as for MySQL database design, migration, extraction, MySQL query building, data import, and export and database comparison [14].

4.4.4 MySQL GUI Tools

MySQL GUI Tools are used for MySQL database design, SQL development, administration and migration. In our project, we used MySQL Query Browser as GUI tools and version is mysql-gui-tools-5.0. MySQL Query Browser is a digital utility for creating, executing, and optimizing SQL queries. With using MySQL Query Browser our MySQL database environment is easy to use [15].

4.4.5 Web server

Apache Tomcat is our application web server that version is apache-tomcat-7.0.73. Basically, Tomcat acts as a development server. It used to deploy your Java Servlets and JSPs, JSF 2, or other Java-based dynamic Web technologies. In our project implements the Java Servlet and the Java Server Pages (JSP) specifications by Apache Tomcat. It is an open source web server and Servlet container developed by the Apache Software Foundation. It provided simplest configuration and runs in a single operating system process. Every single HTTP request from a browser to Tomcat is processed in the Tomcat process in a separate thread and the process runs a Java virtual machine. Apache Tomcat includes tools for configuration and management and can also be configured by editing XML configuration files [16].

CHAPTER 5

Implementation and Testing

5.1 Implementation of Database

We already mentioned earlier for our project we used MySQL database and MySQL Query Browser as GUI Tools. In this chapter focused on how we implement our database.

5.1.1 Database Design

Database design is part of system development. The main objectives of database designing are to produce logical and physical designs models of our database system. In our project, we have tried to provide users with access to up to date, accurate information. Because a correct design is essential to achieving our goals. Database design largely implements are two form.

1. Relationships and
2. Normal forms.

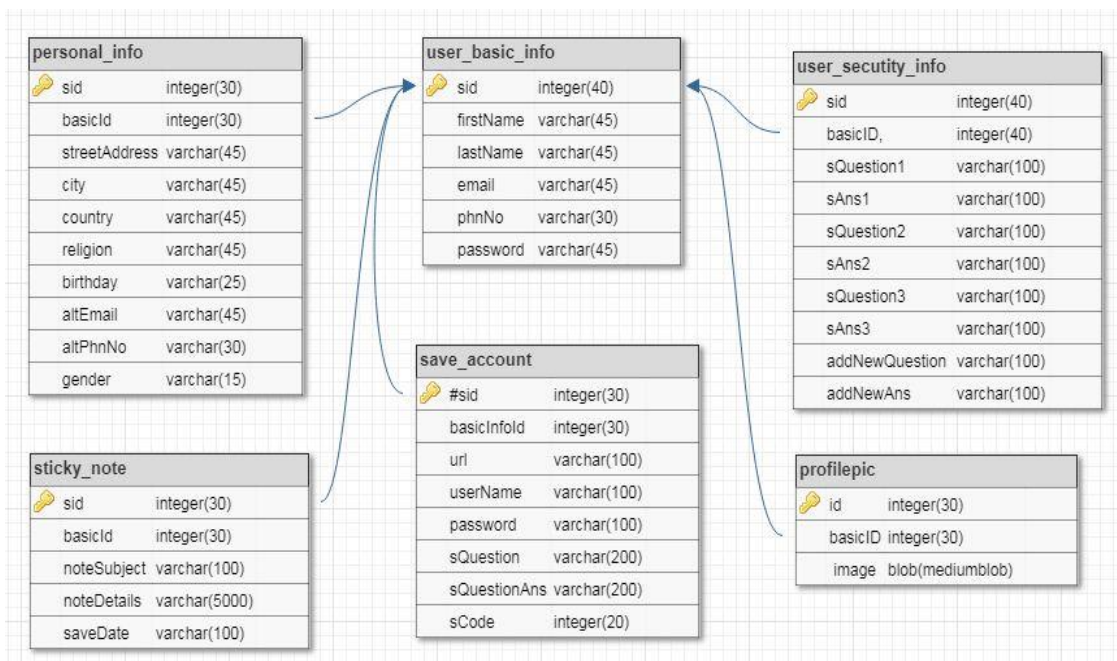


Figure 5.1.1.1: Secure password manager database normal form

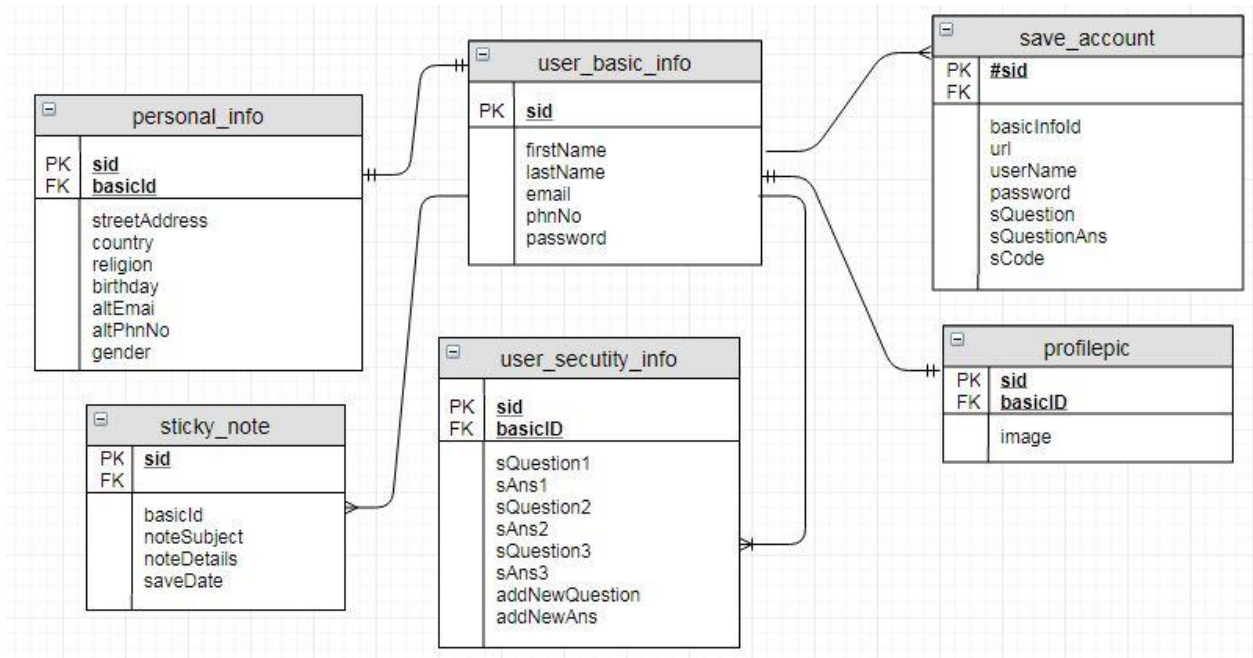


Figure 5.1.1.2: Secure password manager database relationships form

5.1.2 Storing Process of Data

All registered user's identification is stored in our database. Only authorized user can access our system. If any user gives any email and password, which are not store in our database, they cannot log in to our system. MYSQL provided authentication rules, to find if a user gives correct login account or not.

Figure 5.1.2 shows the Database and its table. Database name is the "secure_password_manager" and its authorized table are personal_info, pofilepic, save_account, sticky_note, user_basic_info and user_security_info.

- Personal_info table contains the user personal information who are registered into our system.
- Profile pic table contains the authorized user profile picture.
- Save_account contains the different website's account information such as URL, username, password etc.
- Sticky_note contains the short note of authorized user.
- User_basic_info contains the user registration information of this application when register into our application.

- User-security_info contains the security questions and answer when register into the application.

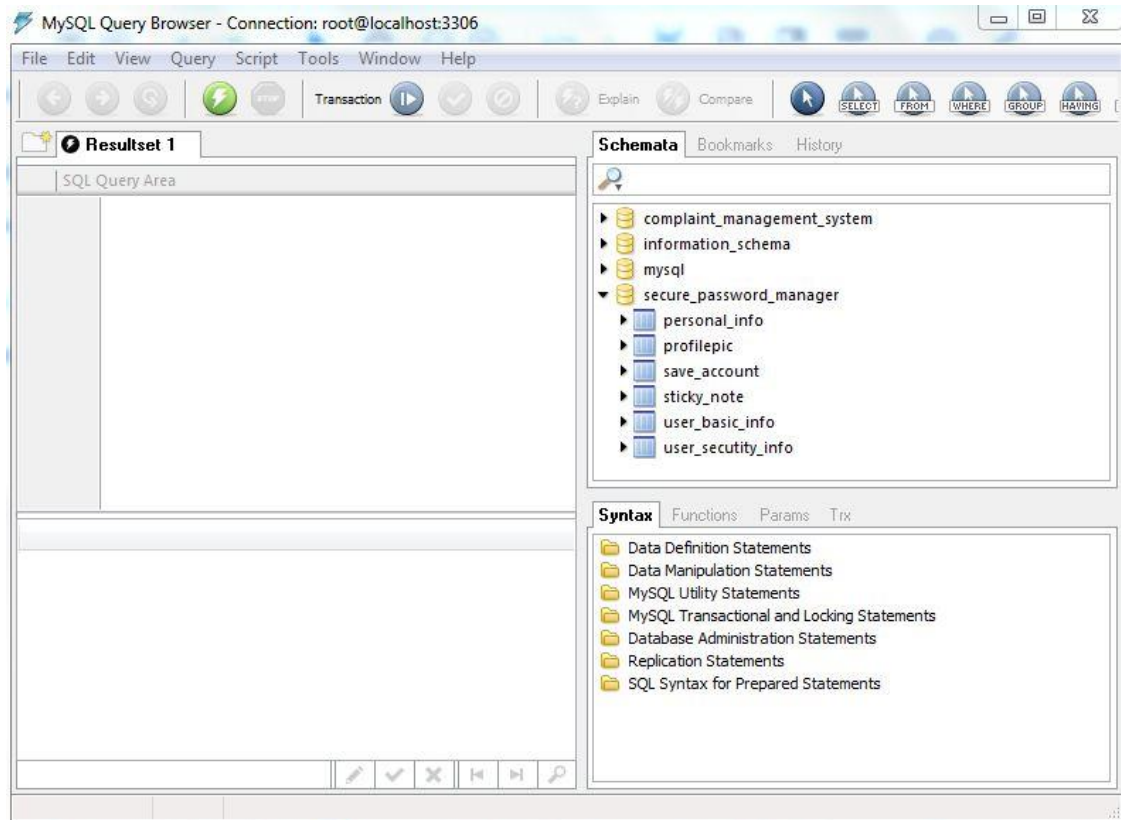


Figure 5.1.2: Secure password manager database

5.2 Implementation of front-end design

In Front end, we used HTML, CSS, JavaScript, Bootstrap, Ajax and jQuery to code the web app designs.

5.2.1 HTML & CSS

HTML means Hyper Text Markup Language and CSS means Cascading Style Sheets. Both are the most basic building blocks of web coding. Without these two things, you cannot create a website design. Even we cannot add images to a page without HTML. Before you get started on any web development, you will have to master coding with HTML and CSS. Mainly HTML use to structure and give meaning to our web content and CSS use to apply styling to our HTML content [17].

5.2.2 JavaScript

JavaScript is a scripting language that allows you to implement complex things on web pages. HTML pages are fine for displaying static content. Nowadays most of the pages are rarely static. Many of today's pages have menus, forms, slideshows and even images that provide user interaction. In our project, we used JavaScript for password matching and auto reloading data from database. JavaScript provided more interaction. JavaScript enables you to create dynamically updating content, control multimedia, animate images, and pretty much everything else [18].

5.2.3 Bootstrap

We used in our project of Bootstrap v3.3.7. Bootstrap is an HTML, CSS, JavaScript framework that you can use as a basis for creating web applications. The main reasons to use of Bootstrap Framework are the easier and faster. It also Save Time, Customizable, Core Factors, grid system, JavaScript, Consistency, Updates, Integration, Responsiveness and Future Compatibility [19].

5.2.4 JQuery

We used in our project of jquery-3.2.1.min.jQuery is a fast and small JavaScript library included in a single .jsfile. JQuery makes our project easier. It provides many built in functions using which you can perform various tasks easily and quickly [20].

5.2.5 Ajax

AJAX means Asynchronous JavaScript and XML. It is the combination of old technologies such as HTML and CSS, JavaScript, XML and XSLT, XMLHttpRequest. Ajax is a client side script that communicates to and from a server or database without the need for a complete page refresh. In our project, when user choose question then page is refreshed from database. It can display web pages with interactive and efficient [21].

5.3 Implementation of Interactions

System interaction is very important part to achieve system goal. Interactions can be found almost everywhere in the real world. Interaction makes a system popular and attractive. We tried to create our system user friendly and easy for users. Because of, to achieve the desired aim of a system depend on the interaction with the user. So we tried

to provide some unique feature to interact our system with user like page refresh without refresh icon, auto password matching when user enter password or used popup dialogue box. We implement our system with responsive UI for better user experience. For this, we use easy icon, text link, button and some places given hints. Therefore, the system is totally user friendly and user can easily interact with our system.

5.4 Testing Implementation

Testing implementation is process of testing the implementation of a system. It is defining how the information system should be built, ensuring that the information system is operational and used, and ensuring that the information system meets quality standard.

Table 5.4: Testing Implementation

Test Case	Test Input	Expected Outcome	Actual Outcome	Status	Tested On
1. Registration	Without registration	Access to the system features	Restricted to access to the system features.	Fail	20/03/18
2. Registration	With registration	Access to the system features	User can access to the system features.	pass	20/03/18
3. Email or password	Blank or incorrect email or password	Can be gone to next step for completing registration.	For email, showed a warning that please fill out this field and if user didn't enter '@' then show please include an '@' in the email address. For password, showed a message that password does not match.	Fail	20/03/18
4. Email or Password	correct email or password	Can be gone to next step for complete registration.	Did not show warning for email and for password, showed a message that password matched and Can be gone to next step for complete registration.	Pass	20/03/18

5. Login	incorrect email or password	Login should be successful	User cannot login and cannot show the homepage.	Fail	20/03/18
6. Login	correct email or password	Login should be successful	User cannot login and Showed the homepage. Therefore, User permitted fully to access the system.	Pass	20/03/18
7. Logout	Don't click the logout button	Logout should be successful	Did not logout and user are staying login	Fail	20/03/18
8. Logout	After clicking logout button	Logout should be successful	Logout was successful and did not show the secure pages.	Pass	20/03/18

5.5 Test Results and Reports

Reporting test execution results is very important part of testing, whenever test execution cycle is complete, tester should make a complete test results report which includes the Test Pass/Fail status of the test cycle [6].

In chapter 5.4, we showed the test case, test input, expected outcome, actual outcome and status. Status is the result of our system testing. Finally, we find out our results and the test result of this application was successful.

We perform usability testing. Usability testing is to check if the user interface is easy to use and understand. It is concerned mainly with the use of the application [7]. Usability test check the user satisfaction such as how much easy to use application. or how much convenient to end-user ?. Benefits of Usability Testing are that Usability testing lets identify problems before they are coded. The earlier issues were identified and fixed. During a usability test, you will [8]:

- Learn if participants are able to complete specific tasks successfully and
- Identify how long it takes to complete specific tasks

- Find out how satisfied participants are with your Web site.
- Identify changes required to improve user performance and satisfaction
- And analyze the performance to see if it meets your usability objectives

As per of users perspective, we can get result of usability test on our application that is application is easy to use, easy to learn, easy to manage, user acceptance, user interaction and user satisfaction.

CHAPTER 6

Conclusion and Future Scope

6.1 Discussion and Conclusion

In these day, many security attack on the internet increase rapidly for that reason authentication based on passwords has become insecure. Easy password cannot protect from harm or risk on the other hand complex password is hard to remember. To resolve these problems there are secure password manager. Secure password manager will be effective for the people who are want to store password in secure place. It also provides some protection against hackers and protects user's online information including emails, Facebook, Instagram records and more.

6.2 Scope for Further Developments

- We will allow you to auto fill forms.
- We will add SMS or email notification system, when user wants to recover password with entering code.
- We will make this application available for all platforms such as android.

REFERENCES

- [1] “1Password” Internet: <https://lifehacker.com/5529133/five-best-password-managers>
[last accessed: April 1, 2018]
- [2] “waterfall model” Internet: <http://toolsqa.com/software-testing/waterfall-model/> [last accessed: Feb 2, 2018]
- [3] “MVC diagram” Internet: <http://csilnmiit.com/mvc-model-view-controller/> [last accessed: March 20, 2018]
- [4] “AES algorithm” Internet: <https://security.stackexchange.com/questions/103541/how-does-aes-encryptions-algorithm-actually-work> [last accessed: March 21, 2018]
- [5] “AES Encryption & Decryption” Internet: https://www.researchgate.net/figure/AES-Encryption-Decryption-Flowchart_fig2_221958203 [last accessed: March 21, 2018]
- [6] “Test reports” Internet: <http://www.softwaretestingmentor.com/test-results/> [last accessed: March 25, 2018]
- [7] “System testing” Internet: https://en.wikipedia.org/wiki/Software_testing [last accessed: March 25, 2018]
- [8] “Usability Testing” Internet: <https://www.usability.gov/how-to-and-tools/methods/usability-testing.html> [last accessed: April 1, 2018]
- [9] “Comparison study” Internet: <https://www.asecurelife.com/dashlane-vs-lastpass-vs-1password-vs-roboform-vs-keepass/#1password> [last accessed: March 31, 2018]
- [10] “Java version” Internet: <https://www.techopedia.com/definition/5594/java-development-kit-jdk> [last accessed: March 31, 2018]
- [11] “List of password managers” Internet: https://en.wikipedia.org/wiki/List_of_password_managers [last accessed: March 31, 2018]
- [12] “Classical Encryption Techniques” Internet: <https://www.codeproject.com/Articles/63432/Classical-Encryption-Techniques> [last accessed: April 10, 2018]
- [13] “NetBeans IDE” Internet: <https://netbeans.org/features/> [last accessed: April 10, 2018]
- [14] “MySQL Installation” Internet: <http://download.nust.na/pub6/mysql/doc/refman/5.1/en/windows-install-wizard.html> [last accessed: April 10, 2018]
- [15] “MySQL GUI tools” Internet: <http://www.webdesigndev.com/best-mysql-gui-tools/> [last accessed: April 10, 2018]
- [16] “Apache Tomcat” Internet: <http://tomcat.apache.org/> [last accessed: April 10, 2018]
- [17] “HTML & CSS” Internet: <https://learn.shayhowe.com/html-css/> [last accessed: April 20, 2018]

- [18] “JavaScript” Internet: <https://www.tutorialspoint.com/javascript/index.htm> [last accessed: April 20, 2018]
- [19] “Bootstrap” Internet: <https://www.w3schools.com/bootstrap/default.asp> [last accessed: April 20, 2018]
- [20] “jQuery” Internet: <https://www.w3schools.com/jquery/default.asp> [last accessed: April 21, 2018]
- [21] “AJAX” Internet: https://www.w3schools.com/js/js_ajax_intro.asp [last accessed: April 21, 2018]
- [22] “Pseudo code for encryption and decryption” [http://imps.mcmaster.ca/courses/SE-4C03-07/wiki/siaa/se4c03_aes_wiki\(7\).html](http://imps.mcmaster.ca/courses/SE-4C03-07/wiki/siaa/se4c03_aes_wiki(7).html) [last accessed: May 1, 2018]

APPENDIX

The final year project is a great opportunity for us to learning valuable practical skills. Our project is created on Model View Controller (MVC) pattern. Here, we understood that how MVC pattern used in web applications to separate the application logic from the user interface. Our project we also learnt some classical and advanced encryption & decryption techniques. Classical encryption techniques such as Caesar Cipher Mono Alphabetic Cipher etc. Advanced algorithm is the Advanced Encryption Standard (AES) is a symmetric block cipher.

Pseudo code for Caesar Cipher encryption:

```
begin
    encryptPassword (String password)
    passwordUpr=password.toUpperCase() // convert lower case to Upper case
    passwordArray=passwordUpr.toCharArray() // take upper case string in an array
    for i=0 step 0 to password.length()
        passwordArray[i]=(char) (passwordArray[i]+15)
    end for
    passwordChyper=String.valueOf(passwordArray)
    passwordChyperConcat=passwordChyper.concat(passwordChyper)
end
```

Pseudo code for Caesar Cipher decryption:

```
begin
    decryptPassword(String password)
    lenHalf=password.length()/2
    passwordChyperSub=password.substring(0, lenHalf)
    passwordCiperArray=passwordChyperSub.toCharArray()
    for i=0 step 0 to passwordChyperSub.length
        passwordCiperArray[i]=(char) (passwordCiperArray[i]-25)
    end for
```



```

passwordDecipher=String.valueOf(passwordCiperArray)
passwordLower=passwordDecipher.toLowerCase()
end

```

Pseudo code for AES encryption [22]:

Cipher(byte in[4*Nb], byte out[4*Nb], word w[Nb*(Nr+1)], //Nb = block size

```

begin
    byte state[4,Nb]
    state = in
    AddRoundKey(state, w[0, Nb-1])
    for round = 1 step 1 to Nr-1
        SubBytes(state)
        ShiftRows(state)
        MixColumns(state)
        AddRoundKey(state, w[round*Nb, (round+1)*Nb-1])
    end for
    SubBytes(state)
    ShiftRows(state)
    AddRoundKey(state, w[Nr*Nb, (Nr+1)*Nb-1])
    out = state
end

```

Pseudo code for AES decryption [22]:

InvCipher(byte in[4*Nb], byte out[4*Nb], word w[Nb*(Nr+1)])

```

begin
    byte state[4,Nb]
    state = in
    AddRoundKey(state, w[Nr*Nb, (Nr+1)*Nb-1])
    for round = Nr-1 step -1 downto 1
        InvShiftRows(state)
        InvSubBytes(state)
    end for
end

```

```
        AddRoundKey(state, w[round*Nb, (round+1)*Nb-1])
        InvMixColumns(state)
    end for
    InvShiftRows(state)
    InvSubBytes(state)
    AddRoundKey(state, w[0, Nb-1])
    out = state
end
```

PLAGIARISM REPORT

