AN INTERNSHIP PROJECT REPORT ON

SECURE MESSAGING SYSTEM

SUBMITTED TO THE SOHAM GLOBAL, AMRAVATI

OF

BACHELOR OF ENGINEERING
IN
COMPUTER SCIENCE & TECHNOLOGY

BY

TARUN S. GAGLANI
VANDAN P. KARWA
TEJAS R. POKALE
RUTVIK S. AGRAWAL

UNDER THE GUIDANCE OF
PROF. PRAFULL MANEKAR

FOUNDER OF SOHAM GLOBAL
SOHAM GLOBAL, RAVI NAGAR, AMRAVATI 444603
2019

CERTIFICATE OF PROJECT COMPLETION

This is to certify that
Mr. **TARUN S. GAGLANI**
Mr. **VANDAN P. KARWA**
Mr. **TEJAS R. POKALE**
Mr. **RUTVIK S. AGRAWAL**

Have worked under my guidance and supervision on the project entitled-
"SECURE MESSAGING SYSTEM"
For the purpose of their internship project as per the guidelines of
MR. PRAFULL MANEKAR and Ms. SHARAYU ZOLEKAR

While forwarding the project work and report on the mentioned topic above, I certify that the candidates have completed their project work in the prescribed period and that the project work incorporates the results of the job done by them during this period.

Guided By :
Ms. Sharayu Zolekar

Submitted By:
Mr. Tarun S. Gaglani
Mr. Vandan P. Karwa
Mr. Tejas R. Pokale
Mr. Rutvik S. Agrawal

INDEX

OBJECTIVE

Computers and people can communicate by using messaging systems to exchange messages over electronic networks. The most ubiquitous messaging system today is email, which facilitates communication among people. While email is an important human-to-human messaging system, this book is not about email. Instead, this book is concerned with messaging systems that allow different people to communicate with each other with proper security concerned. Mobile phones with SMS (Short Message Service) are getting popular day by day. SMs allow user to send brief text nearly upto 160 characters directly from their mobile phone to their friends mobile phone.

The objective of the project here was to design a software which provides same facility that of communicating with each other but with a proper security.

INTRODUCTION

This software provides an environment where different users can login and can chat with each other through the text messages. Beside this they can also create a group where the members can chat in a group all at once. All this work is done with proper security provided by the java, java beans and their class files.

This project is a Enterprise java module which is written in JAVA using STRUTS mvc framework. Beside these various technologies like HTML, JSP, AJAX, MySQL 8.0 database, Tomcat server and at last for user friendly interface Bootstrap is used.

The messages that are sent from one user to another user are stored in an encrypted form using AES ENCRYPT technology and are decrypted by using AES decrypt technology as per requirement. This technology help us to keep data safe and away from the unauthorized users with a proper security.

DATABASE SCHEMA

This projects uses the **MySQL 8.0** database which provides a space where all the data gets stored and can be retrived from it as per requirement. The Database named **SECUREMSG** contains all the data. Data gets stored in the form of tables which are described as per the need of storage. This database consist of 7 tables…..

1. Login table :

```
mysql> desc login;
+--------+-------------+------+-----+---------+-------+
| Field  | Type        | Null | Key | Default | Extra |
+--------+-------------+------+-----+---------+-------+
| mobno  | varchar(10) | YES  |     | NULL    |       |
| pass   | varchar(30) | YES  |     | NULL    |       |
| status | varchar(8)  | YES  |     | NULL    |       |
| Ques   | varchar(50) | YES  |     | NULL    |       |
| Ans    | varchar(50) | YES  |     | NULL    |       |
+--------+-------------+------+-----+---------+-------+
```

The above table stores the login information which is mainly required to validate when a user gets logged in to the software.

2. Profile table :

```
mysql> desc profile;
+---------+-------------+------+-----+---------+-------+
| Field   | Type        | Null | Key | Default | Extra |
+---------+-------------+------+-----+---------+-------+
| name    | varchar(30) | YES  |     | NULL    |       |
| surname | varchar(30) | YES  |     | NULL    |       |
| dobirth | varchar(30) | YES  |     | NULL    |       |
| mobno   | varchar(10) | NO   | PRI | NULL    |       |
| mail    | varchar(30) | YES  |     | NULL    |       |
| state   | varchar(30) | YES  |     | NULL    |       |
| city    | varchar(50) | YES  |     | NULL    |       |
| img     | varchar(50) | YES  |     | NULL    |       |
+---------+-------------+------+-----+---------+-------+
```

The above table stores the information which describes the general information about the user.

3. Addcontact :

```
mysql> desc addcontact;
+-------+-------------+------+-----+---------+-------+
| Field | Type        | Null | Key | Default | Extra |
+-------+-------------+------+-----+---------+-------+
| adder | varchar(10) | YES  |     | NULL    |       |
| mobno | varchar(10) | YES  |     | NULL    |       |
| name  | varchar(30) | YES  |     | NULL    |       |
+-------+-------------+------+-----+---------+-------+
```

The above table shows contacts which are been added by the user as his/her friend while using the system.

4. Addgroup :

```
mysql> desc addgroup;
+---------+-------------+------+-----+---------+----------------+
| Field   | Type        | Null | Key | Default | Extra          |
+---------+-------------+------+-----+---------+----------------+
| groupid | int(11)     | NO   | PRI | NULL    | auto_increment |
| grpname | varchar(50) | YES  |     | NULL    |                |
| adminn  | varchar(10) | YES  |     | NULL    |                |
| status  | varchar(10) | YES  |     | NULL    |                |
+---------+-------------+------+-----+---------+----------------+
```

The above table store the data about the groups which have been made by the various admins which are the user of the application system. All the group id are unique.

5. Groupinfo :

```
mysql> desc groupinfo;
+-----------+----------------+------+-----+---------+----------------+
| Field     | Type           | Null | Key | Default | Extra          |
+-----------+----------------+------+-----+---------+----------------+
| msgno     | int(11)        | NO   | PRI | NULL    | auto_increment |
| groupname | varchar(50)    | YES  |     | NULL    |                |
| sender    | varchar(10)    | YES  |     | NULL    |                |
| datee     | varchar(15)    | YES  |     | NULL    |                |
| time      | varchar(15)    | YES  |     | NULL    |                |
| message   | varbinary(500) | YES  |     | NULL    |                |
| groupid   | int(11)        | YES  |     | NULL    |                |
+-----------+----------------+------+-----+---------+----------------+
```

The above table stores the data related with the groups and their chats.

6. Info :

```
mysql> desc info;
+----------+---------------+------+-----+---------+----------------+
| Field    | Type          | Null | Key | Default | Extra          |
+----------+---------------+------+-----+---------+----------------+
| msgno    | int(11)       | NO   | PRI | NULL    | auto_increment |
| sender   | varchar(10)   | YES  |     | NULL    |                |
| receiver | varchar(10)   | YES  |     | NULL    |                |
| datee    | varchar(15)   | YES  |     | NULL    |                |
| time     | varchar(15)   | YES  |     | NULL    |                |
| message  | varbinary(500)| YES  |     | NULL    |                |
+----------+---------------+------+-----+---------+----------------+
```

The above table stores the data of the chats and much more about the sender and receiver. Here messages are stored in an encrypted form which are not readable by any unauthorized person.

7. Grpcontact :

```
mysql> desc grpcontact;
+--------------+-------------+------+-----+---------+-------+
| Field        | Type        | Null | Key | Default | Extra |
+--------------+-------------+------+-----+---------+-------+
| groupid      | int(11)     | YES  |     | NULL    |       |
| addedbyadmin | varchar(10) | YES  |     | NULL    |       |
| adder        | varchar(10) | YES  |     | NULL    |       |
+--------------+-------------+------+-----+---------+-------+
```

The above table describes the number of groups and their admins.

Beside these tables our database contains **views** which plays an important role in our project. These views help system to decrypt the data which has been stored in an encrypted form. View stores that data temporarily which again is shown only to the authorized user without any leaks.

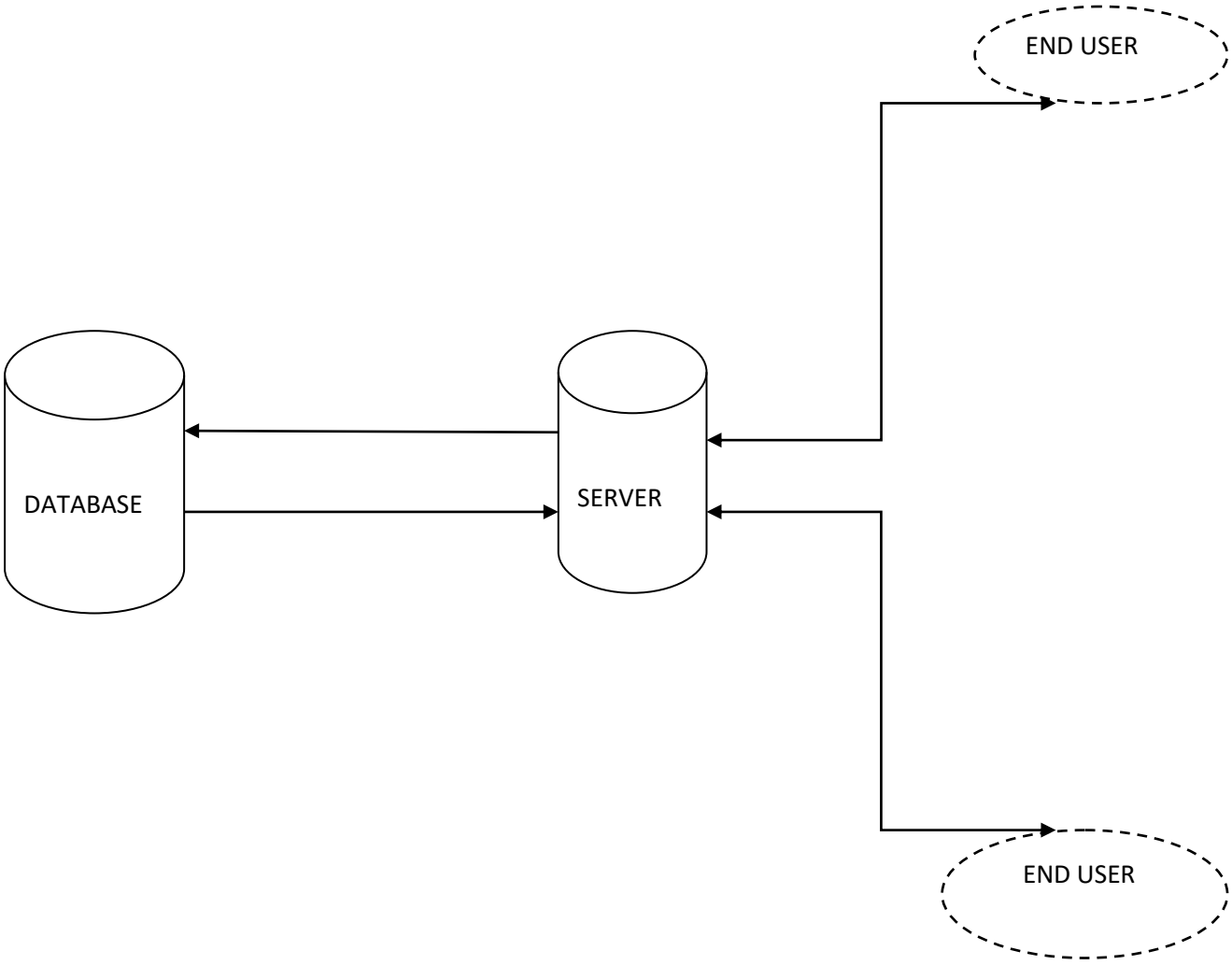
1. Testdecrypt :

```
mysql> desc testdecrypt;
+----------+----------------+------+-----+---------+-------+
| Field    | Type           | Null | Key | Default | Extra |
+----------+----------------+------+-----+---------+-------+
| sender   | varchar(10)    | YES  |     | NULL    |       |
| receiver | varchar(10)    | YES  |     | NULL    |       |
| message  | varbinary(500) | YES  |     | NULL    |       |
+----------+----------------+------+-----+---------+-------+
```

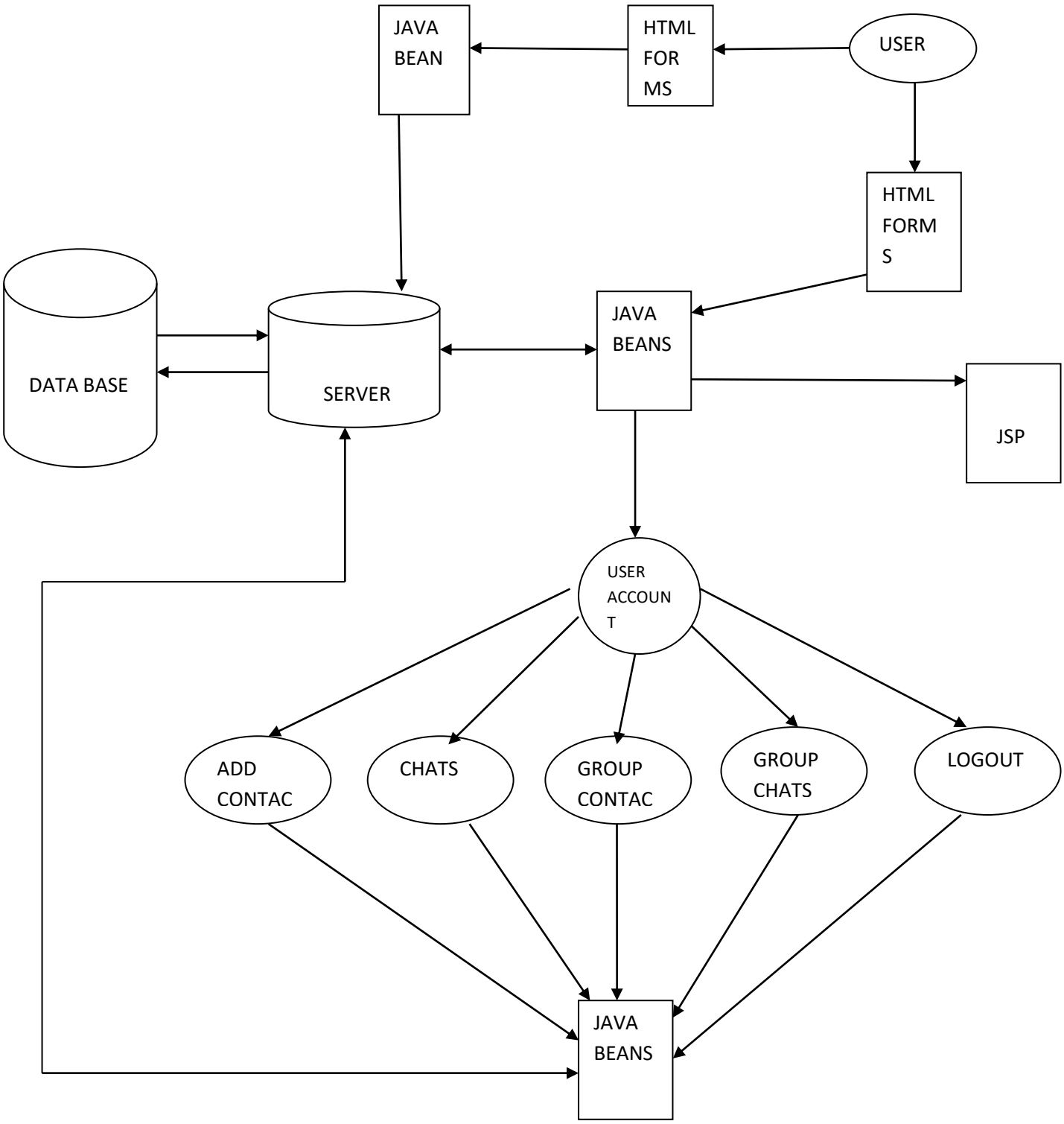
2. Testdecrypt1 :

```
mysql> desc testdecrypt1;
+-----------+----------------+------+-----+---------+-------+
| Field     | Type           | Null | Key | Default | Extra |
+-----------+----------------+------+-----+---------+-------+
| groupname | varchar(50)    | YES  |     | NULL    |       |
| sender    | varchar(10)    | YES  |     | NULL    |       |
| message   | varbinary(500) | YES  |     | NULL    |       |
+-----------+----------------+------+-----+---------+-------+
```

DATA FLOW DIAGRAM



PROJECT WORK FLOW DIAGRAM



PROJECT WORK FLOW EXPLANATION

This module works on a simple flow which basically can be divided into two parts i.e. registration and login.

1. Registration :

   This process is very common and is a general process where user wish to create his/her account on the following application or software. This work is done using HTML forms, Java beans, JSP and database where this all the data would get stored.

   Firstly the user will fill the html form which will demand the users common information. On next, that particular data will be sent to bean where different java codes are written and class files are generated. Further going on that data is again passed onto the server which helps us to move that data into database where it gets stored in particular tables of a defined database.

2. Login :

   Once the registration process is completed the next step a user would like to do is login into that particular software or application. All the work again over here is done using html forms, JSPs, java beans, server and database playing an important role in it.

   At first the data will be inserted by the user on the html form which will ask him/her for their ID which is nothing but their registered mobile number and password which they have set at the time of their registration. This data gets passed on to java bean which does the work of validating this particular data by sending it to the server and checking it from the database. If the given data is matched with the data in that database then the user gets logged in to the application or else the message gets displayed which conveys the user that data inserted by him is incorrect. This message is displayed using JSP.

   After this process when a user gets logged into this application with his proper account, further on he gets number of options that he can

make use of it. As soon as he gets logged in the home screen would get appeared which has different options like

1. **Add Contact** : Where user can add new contacts into their friend list so that they can chat and send text to one another.
2. **My Contacts** : Here user can see his friend list that are the number of contacts he had added on to his list. Here they also get an option of chat button where using that they can can chat with one another.
3. **Create New Group** : One can create a new group if they want where they can add the members of their contact list into that particular group.
4. **My Groups :** This button shows the list of the groups a user had made or is a member of some other group.
5. **Edit profile :** The most important feature that an application provides a user is one where he/she can update their general information as per their needs. This option gets available after clicking this button.
6. **Change Password:** Here user can change its current password and can generate a new one for the login purpose.
7. **Logout :** This is again an important button which ends the session of their account and helps to exit the application.

Whole of the module is made in Java language which defines an enterprise project using STRUTS 2.5 MVC framework. The general scenario of this mvc framework is that it accepts the data from a html form, sends it to the java bean for processing it, which again gets passed on to the server and gets inserted or retrived in/from the database as per requirement. So all of the above mentioned buttons have a same work flow as described over here.

TECHNOLOGICAL DETAILS

1. JAVA :

Java is the base language in which the above particular software is written. **Java** is a general-purpose programming language that is class-based, object-oriented (although not a pure OO language, as it contains primitive types), and designed to have as few implementation dependencies as possible. It is intended to let application developers *write once, run anywhere* (WORA),meaning that compiled Java code can run on all platforms that support Java without the need for recompilation. Java applications are typically compiled to bytecode that can run on any Java virtual machine (JVM) regardless of the underlying computer architecture. The syntax of Java is similar to C and C++, but it has fewer low-level facilities than either of them. As of 2018, Java was one of the most popular programming languages in use according to GitHub, particularly for client-server web applications, with a reported 9 million developers.

2. TOMCAT SERVER :

Apache Tomcat (also referred to as **Tomcat Server**) implements several Java EE specifications including Java Servlet, JavaServer Pages (JSP), Java EL, and WebSocket, and provides a "pure Java" HTTP web serverenvironment in which Java code can run.

Tomcat is developed and maintained by an open community of developers under the auspices of the Apache Software Foundation, released under the Apache License 2.0 license, and is open-source software.

3. JSP :

JavaServer Pages (**JSP**) is a technology that helps software developers create dynamically generated web pagesbased on HTML, XML, or other document types. Released in 1999 by Sun Microsystems,JSP is similar to PHP and ASP, but it uses the Java programming language. To deploy and run JavaServer Pages, a compatible web server with a servlet container, such as Apache Tomcat or Jetty, is required.

4. **HTML :**

   Hypertext Markup Language (**HTML**) is the standard markup language for documents designed to be displayed in a web browser. It can be assisted by technologies such as Cascading Style Sheets (CSS) and scripting languages such as JavaScript. Web browsers receive HTML documents from a web server or from local storage and render the documents into multimedia web pages. HTML describes the structure of a web page semantically and originally included cues for the appearance of the document.

5. **AJAX :**

   Ajax (also **AJAX** short for asynchronous JavaScript and XML) is a set of web development techniques using many web technologies on the client side to create asynchronous web applications. With Ajax, web applications can send and retrieve data from a server asynchronously (in the background) without interfering with the display and behavior of the existing page. By decoupling the data interchange layer from the presentation layer, Ajax allows web pages and, by extension, web applications, to change content dynamically without the need to reload the entire page. In practice, modern implementations commonly utilize JSON instead of XML.

6. MySQL 8.0 :

   MySQL is an open-source relational database management system(RDBMS). Its name is a combination of "My", the name of co-founder Michael Widenius's daughter, and "SQL", the abbreviation for Structured Query Language. MySQL is free and open-source software under the terms of the GNU General Public License, and is also available under a variety of proprietary licenses. MySQL was owned and sponsored by the Swedish company MySQL AB, which was bought by Sun Microsystems (now Oracle Corporation).[8] In 2010, when Oracle acquired Sun, Widenius forked the open-source MySQL project to create MariaDB.

7. STRUTS 2.5 :

Apache Struts 2 is an open-source web application framework for developing Java EE web applications. It uses and extends the Java Servlet API to encourage developers to adopt a model–view–controller (MVC) architecture. The WebWork framework spun off from Apache Struts aiming to offer enhancements and refinements while retaining the same general architecture of the original Struts framework. In December 2005, it was announced that WebWork 2.2 was adopted as Apache Struts 2, which reached its first full release in February 2007.

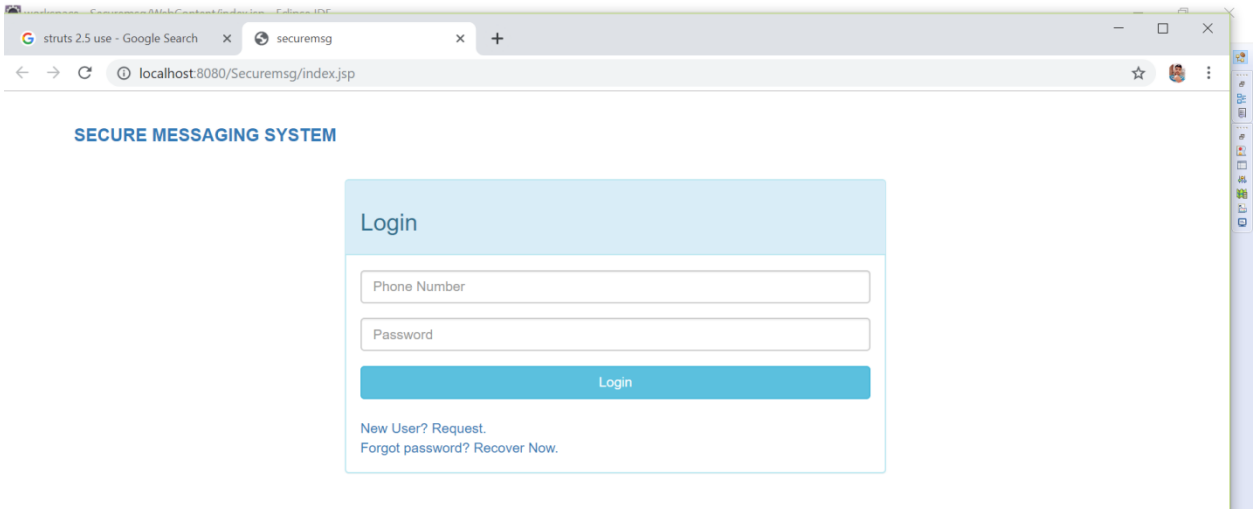
8. **AES Encryption & Decryption:**

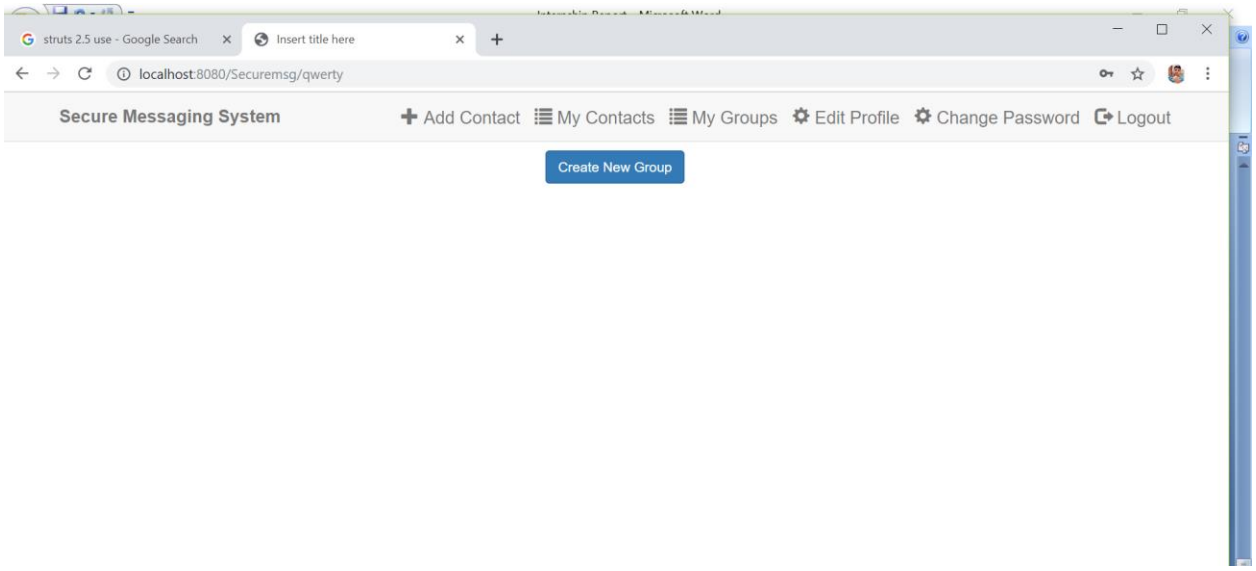
AES is based on a design principle known as a substitution–permutation network, and is efficient in both software and hardware. Unlike its predecessor DES, AES does not use a Feistel network. AES is a variant of Rijndael which has a fixed block size of 128 bits, and a key size of 128, 192, or 256 bits. By contrast, Rijndael *per se*is specified with block and key sizes that may be any multiple of 32 bits, with a minimum of 128 and a maximum of 256 bits.

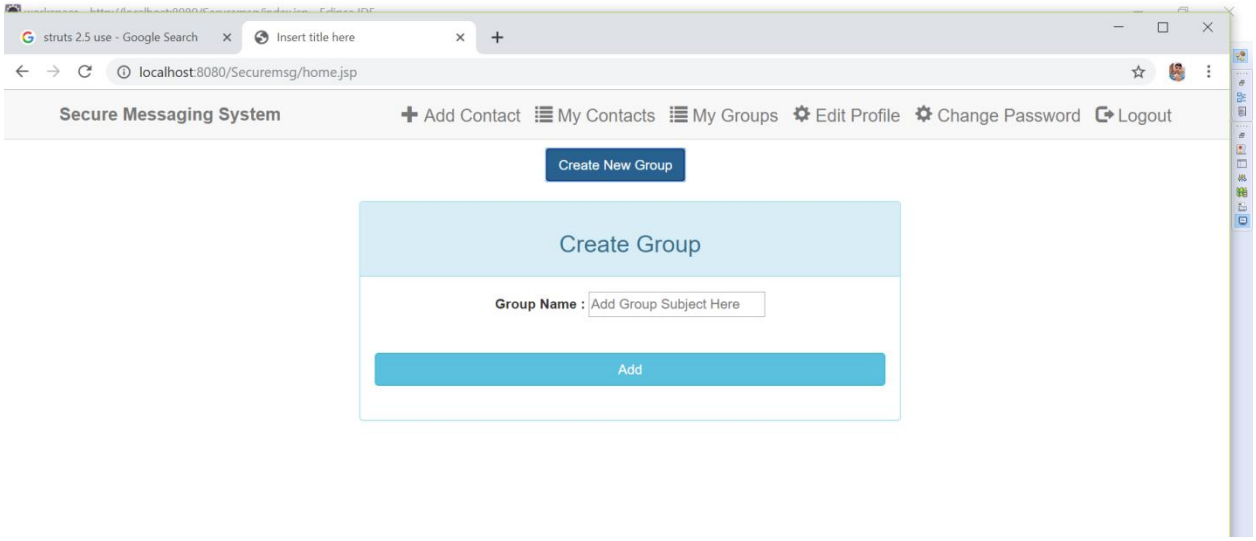
9. Bootstrap :

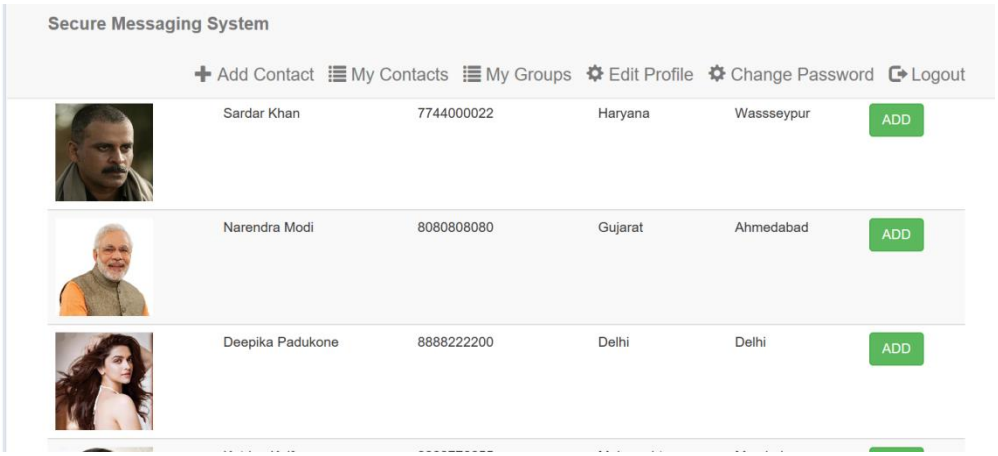
Bootstrap is a free and open-source CSS framework directed at responsive, mobile-first front-end web development. It contains CSS- and (optionally) JavaScript-based design templates for typography, forms, buttons, navigation and other interface components.

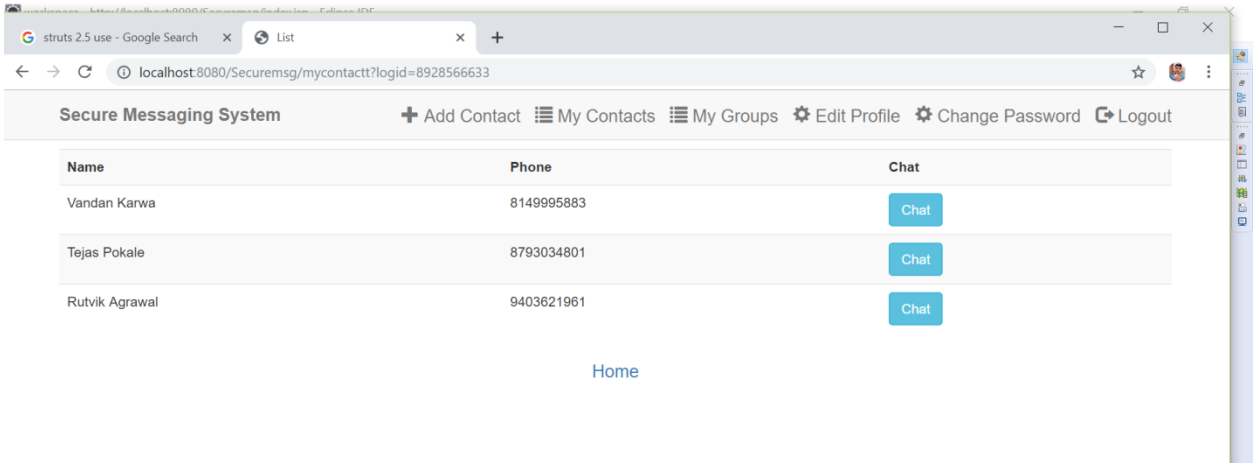
SCREENSHOTS

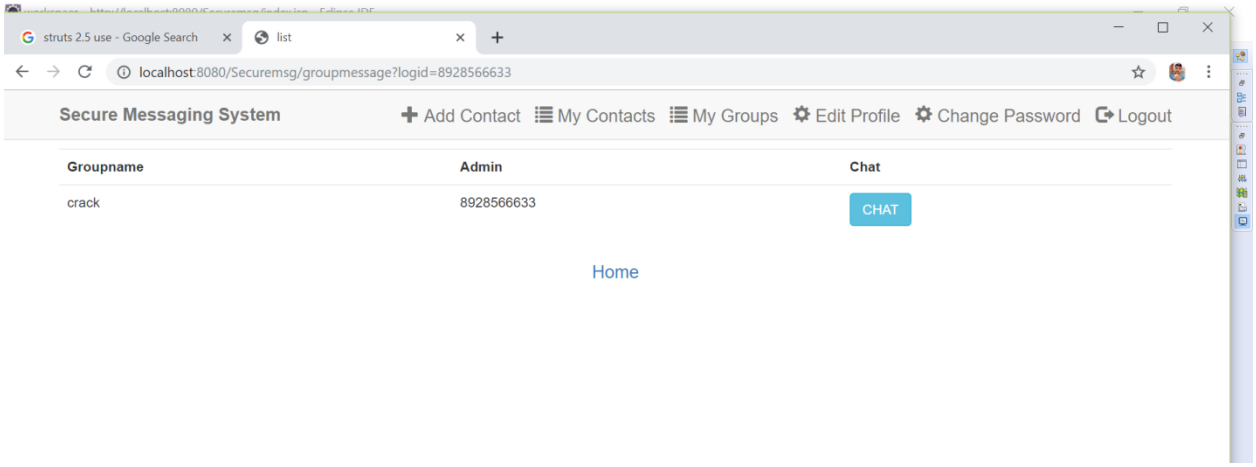


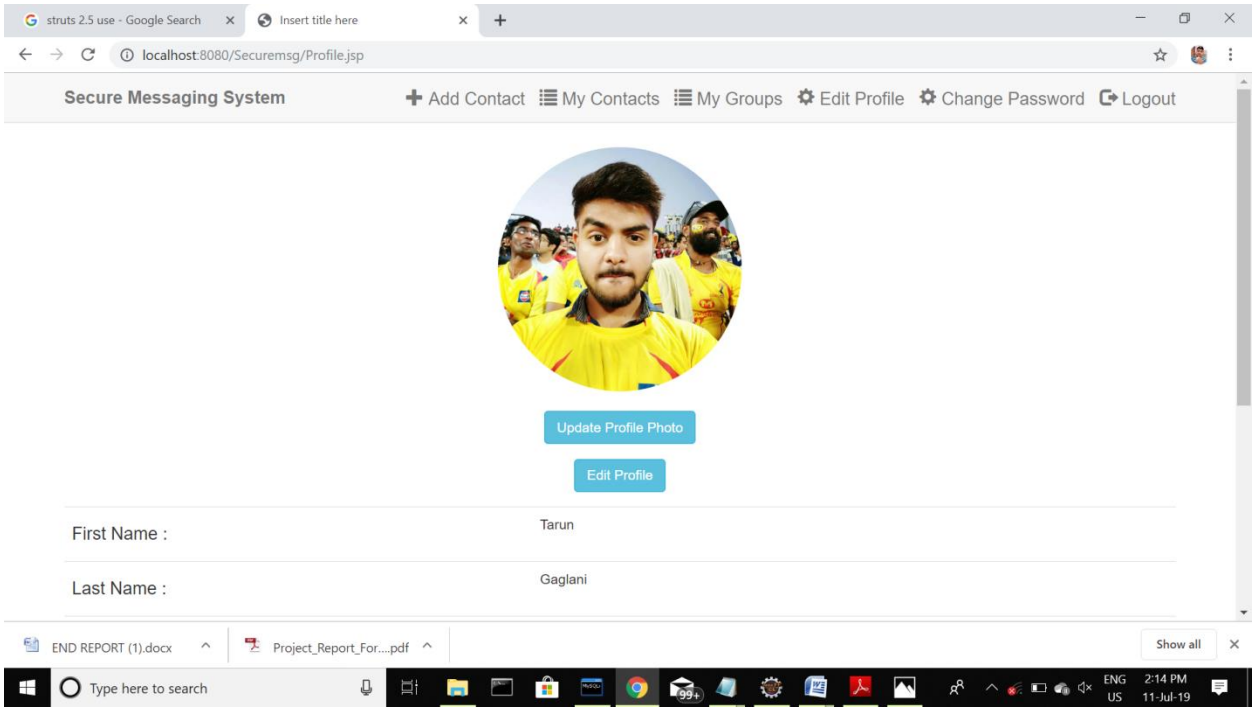


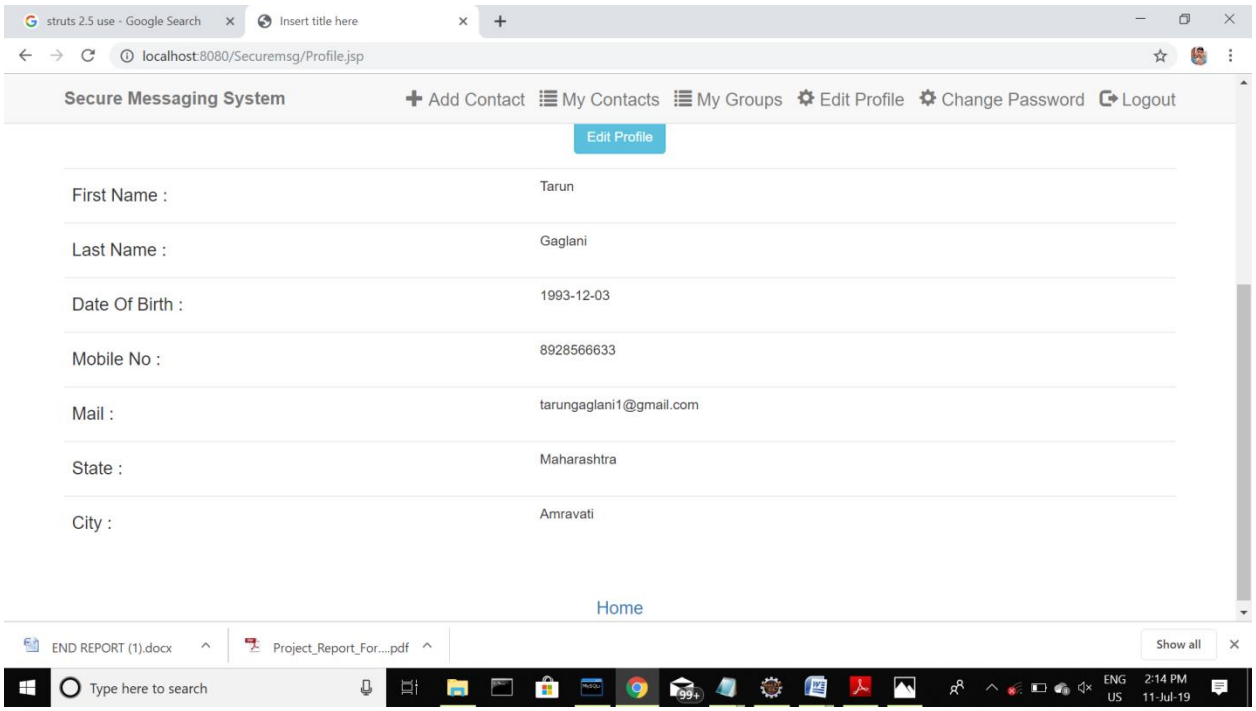

struts 2.5 use - Google Search
Insert title here
localhost:8080/Securemsg/home.jsp
Secure Messaging System
Add Contact
My Contacts
My Groups
Edit Profile
Change Password
Logout
Create New Group
Create Group
Group Name :
Add Group Subject Here
Add

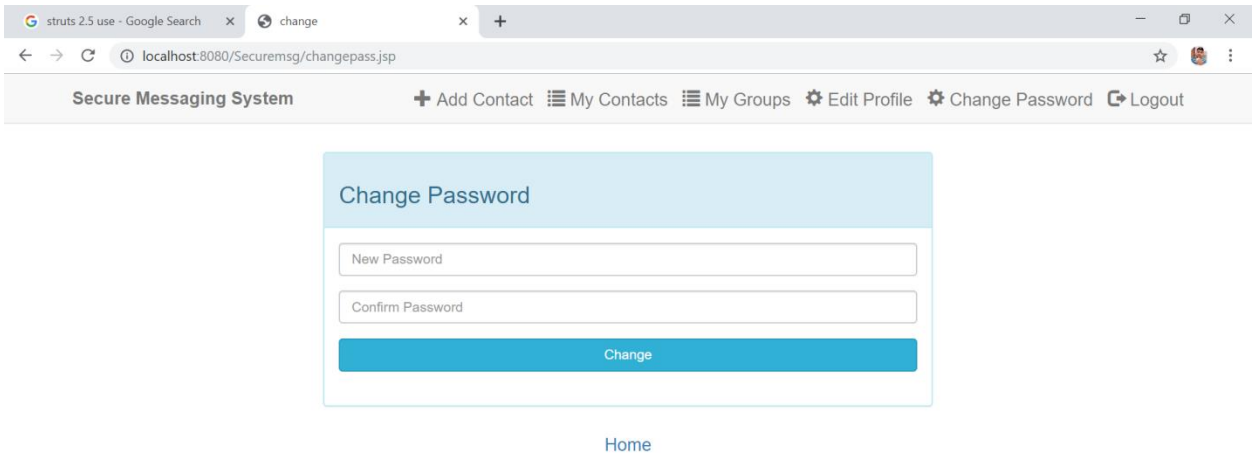

Secure Messaging System
Add Contact
My Contacts
My Groups
Edit Profile
Change Password
Logout
Sardar Khan
7744000022
Haryana
Wassseypur
ADD
Narendra Modi
8080808080
Gujarat
Ahmedabad
ADD
Deepika Padukone
8888222200
Delhi
Delhi
ADD

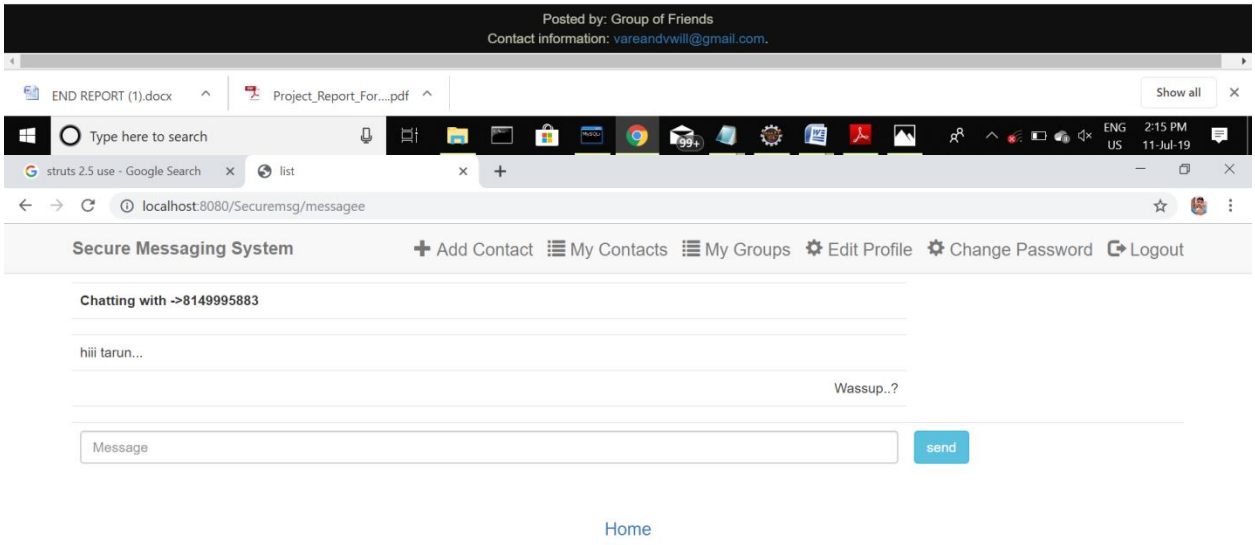

struts 2.5 use - Google Search
List
localhost:8080/Securemsg/mycontactt?logid=8928566633
Secure Messaging System
Add Contact
My Contacts
My Groups
Edit Profile
Change Password
Logout
Name
Phone
Chat
Vandan Karwa
8149995883
Chat
Tejas Pokale
8793034801
Chat
Rutvik Agrawal
9403621961
Chat
Home

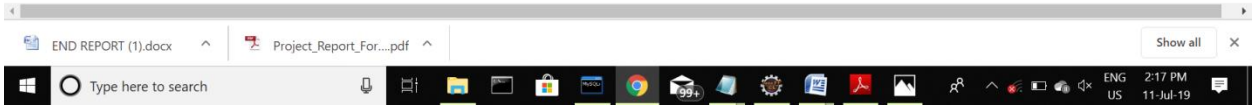

struts 2.5 use - Google Search
list
localhost:8080/Securemsg/groupmessage?logid=8928566633
Secure Messaging System
Add Contact
My Contacts
My Groups
Edit Profile
Change Password
Logout
Groupname
Admin
Chat
crack
8928566633
CHAT
Home

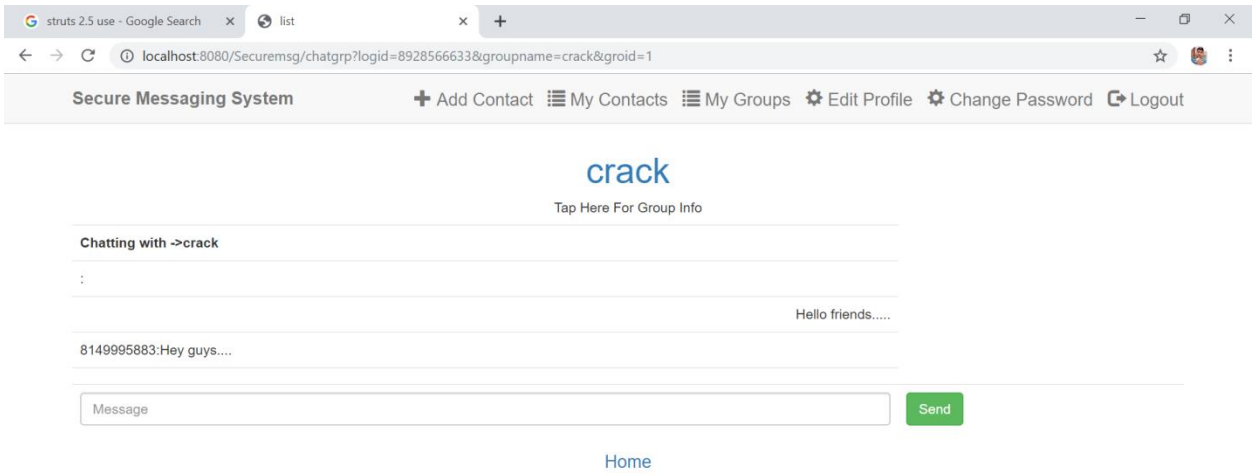

struts 2.5 use - Google Search
Insert title here
localhost:8080/Securemsg/Profile.jsp
Secure Messaging System
Add Contact
My Contacts
My Groups
Edit Profile
Change Password
Logout
Update Profile Photo
Edit Profile
First Name :
Tarun
Last Name :
Gaglani
END REPORT (1).docx
Project_Report_For....pdf
Show all
Type here to search
ENG
US
2:14 PM
11-Jul-19

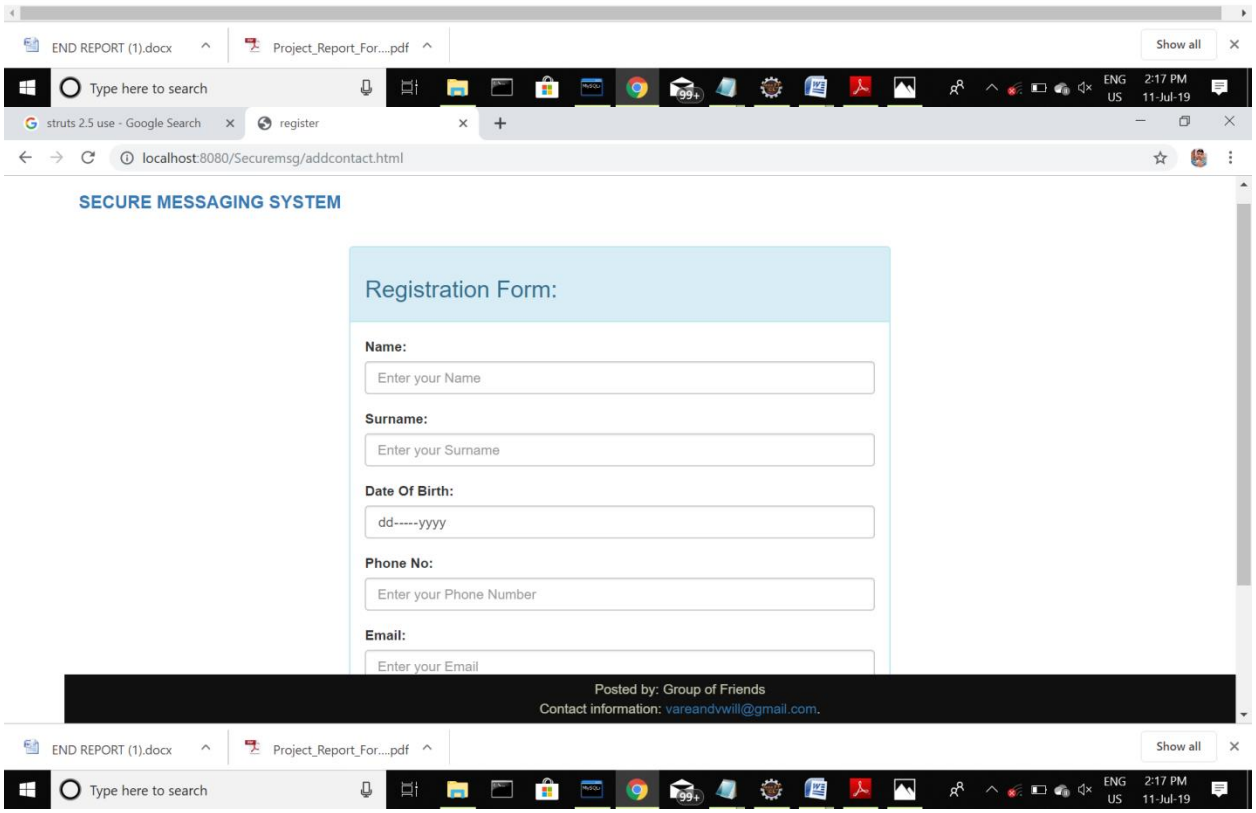

struts 2.5 use - Google Search
Insert title here
localhost:8080/Securemsg/Profile.jsp
Secure Messaging System
Add Contact
My Contacts
My Groups
Edit Profile
Change Password
Logout
Edit Profile
First Name :
Tarun
Last Name :
Gaglani
Date Of Birth :
1993-12-03
Mobile No :
8928566633
Mail :
tarungaglani1@gmail.com
State :
Maharashtra
City :
Amravati
Home
END REPORT (1).docx
Project_Report_For....pdf
Show all
Type here to search
ENG
US
2:14 PM
11-Jul-19

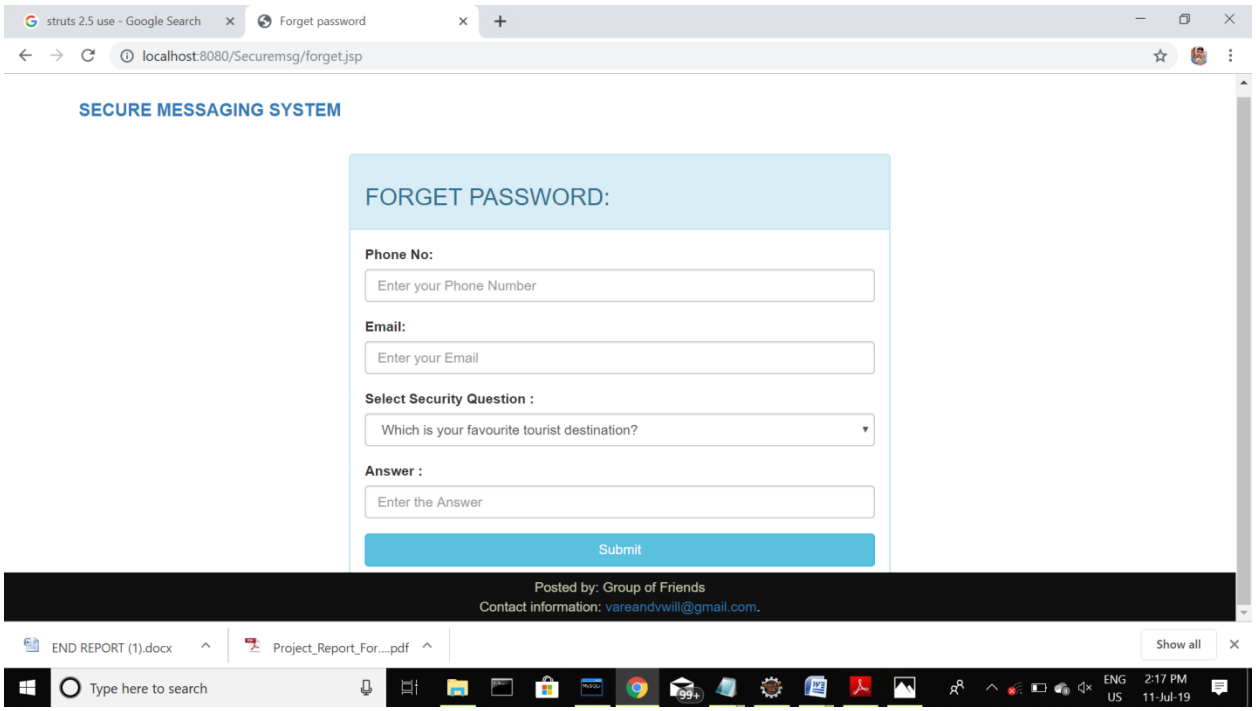

struts 2.5 use - Google Search
change
localhost:8080/Securemsg/changepass.jsp
Secure Messaging System
Add Contact
My Contacts
My Groups
Edit Profile
Change Password
Logout
Change Password
New Password
Confirm Password
Change
Home


Posted by: Group of Friends
Contact information: vareandvwill@gmail.com.
END REPORT (1).docx
Project_Report_For....pdf
Show all
Type here to search
ENG
US
2:15 PM
11-Jul-19
struts 2.5 use - Google Search
list
localhost:8080/Securemsg/messagee
Secure Messaging System
Add Contact
My Contacts
My Groups
Edit Profile
Change Password
Logout
Chatting with ->8149995883
hiii tarun...
Wassup..?
Message
send
Home


END REPORT (1).docx
Project_Report_For....pdf
Show all
Type here to search
ENG
US
2:17 PM
11-Jul-19


struct 2.5 use - Google Search
list
localhost:8080/Securemsg/chatgrp?logid=8928566633&groupname=crack&groid=1
Secure Messaging System
Add Contact
My Contacts
My Groups
Edit Profile
Change Password
Logout
crack
Tap Here For Group Info
Chatting with ->crack
:
Hello friends.....
8149995883:Hey guys....
Message
Send
Home


END REPORT (1).docx
Project_Report_For....pdf
Show all
Type here to search
struct 2.5 use - Google Search
register
localhost:8080/Securemsg/addcontact.html
SECURE MESSAGING SYSTEM
Registration Form:
Name:
Enter your Name
Surname:
Enter your Surname
Date Of Birth:
dd-----yyyy
Phone No:
Enter your Phone Number
Email:
Enter your Email
Posted by: Group of Friends
Contact information: vareandvwill@gmail.com.


struts 2.5 use - Google Search
Forget password
localhost:8080/Securemsg/forget.jsp
SECURE MESSAGING SYSTEM
FORGET PASSWORD:
Phone No:
Enter your Phone Number
Email:
Enter your Email
Select Security Question :
Which is your favourite tourist destination?
Answer :
Enter the Answer
Submit
Posted by: Group of Friends
Contact information: vareandvwill@gmail.com.
END REPORT (1).docx
Project_Report_For....pdf
Show all
Type here to search
ENG
US
2:17 PM
11-Jul-19

CONCLUSION

The era of technologies have have opened the windows for various communication applications and softwares which increase the speed and ease the way of communication. So all these technologies have become a part of our daily routine and here we introduce our software SECURE MESSAGING SYSTEM which will work for a chatting purpose with keeping an eye on proper security regarding with the whole module.