ONLINE BANKING FRAUD PREVENTION USING MULTICONTEXTUAL BEHAVIOUR PROFILING

A MINI PROJECT REPORT

Submitted by

Mr. CHANDRU.G (410819104003)

Mr. RONALD ISSAC.B J (410819104023)

of

BACHELOR OF ENGINEERING

in

COMPUTER SCIENCE AND ENGINEERING

GKM COLLEGE OF ENGINEERING AND TECHNOLOGY

AFFLICTED TO ANNA UNIVERSITY

CHENNAI-600 025

DEPARTMENT OF COMPUTER SCIENCE ENGINEERING

JUNE-2022

ANNA UNIVERSITY:: CHENNAI – 600025

BONAFIDE CERTIFICATE

Certified that this Mini project report "**ONLINE BANKING FRAUD PREVENTION USING MULTICONTEXTUAL BEHAVIOUR PROFILING**" is the bonafide work of "**Mr.CHANDRU.G,Mr.RONALD ISSAC.B J**" who carried out the project work under my supervision.

SIGNATURE

Mrs.R AISWARYA,M.E,
SUPERVISOR

Department of Computer Science and Engineering

GKM College of Engineering and Technology
GKM Nagar
New Perungalathur
Chennai-600063.

SIGNATURE

Dr.M.BABU Ph.D
HEAD OF THE DEPARTMENT

Department of Computer Science and Engineering

GKM College of Engineering and Technology
GKM Nagar
New Perungalathur
Chennai-600063.

GKM COLLEGE OF ENGINEERING AND TECHNOLOGY

CHENNAI-600 063

ANNA UNIVERSITY :: CHENNAI 600 025

MINI PROJECT VIVA-VOCE EXAMINATION

The viva-voice Examination of the mini project work submitted by,

Mr. CHANDRU.G (410819104003)

Mr. RONALD ISSAC.B J (410819104023)

Is to be held on………… at Computer Science and Engineering Department

INTERNAL EXAMINER **EXTERNAL EXAMINER**

ACKNOWLEDGEMENT

We thank God Almighty for enabling us to complete our project. We express our deep sense of gratitude and thanks to our respected **CEO**, **Dr.SUJATHA BALASUBRAMANIAN,** G.K.M. Group of Educational institutions for her constant support and educating us in her prestigious institution. Also, we take this opportunity to thank our Managing Director Mr. **C. BALASUBRAMANIAN**, for his extended support to complete the project work.

We express our sincere thanks to our Principal, **Dr**. **N. S. BHUVANESWARI** for her continuous motivation, kind support and guidance throughout the project.

We feel immense pleasure in thanking our Head of the Department **Dr**.**M.BABU**, **Professor** and our project coordinator **Mrs**.**R.AISWARYA**, Asst. Prof., for the continuous motivation, support and making us to complete the project in time. Also, We express our gratitude to our Project guide, **Mrs.R.AISWARYA**, **Asst. Prof.**, for giving innovative ideas and for the valuable guidance and the support that have added a great deal to the substance of this report.

We also extend our thanks to all our **FACULTIES** of the **department of Computer Science and Engineering** for helping us throughout the project work. Further the acknowledgement would be incomplete if we would not mention a word of thanks to our beloved family and friends whose continuous support to complete the project.

ABSTRACT:

Many consumers today are turning to the ease and convenience of Internet banking to take care of their financial needs. With the new levels of access made possible by the Internet, people can now check the status of their finances with the click of a button. This occurs with text based and graphical passwords. There are two types of difficulties of remembering text passwords. They are easy to remember and hard to guess. If the password is easy to remember, it will be easy to guess. On the other hand, if the password is hard to guess, it will be hard to remember also Users tend to write passwords down or use the same passwords for different accounts. People always select predictable passwords. To create more unforgettable passwords, graphical password systems have been devised. Graphical password authentication is based on clicking on the image rather than typing alphanumeric strings. we proposed a new click-based graphical password scheme called Cued Click Points. A password consists of one click-point per image for a sequence of images. This enhances security greatly than using conventional login methods.

The main purpose that banks have been serving since their inception is keeping our money safe for us. While keeping our money safe, they also let us earn a certain amount of interest on the money deposited with them. Traditional banks have been doing this, and internet banks continue the same function. The only difference is in the way the transactions are made. We all know about internet banking and most of us use it quite often as well, but few of us actually understand about the history of internet banking and how it all came out. Knowing the history of internet banking can be incredibly useful, especially since it will allow us to have more respect for the little things that we take for granted

LIST OF FIGURES

LIST OF TABLES:

LIST OF SYSMBOLS, ABBREVIATIONS AND NOMENCLATURE

- CCP – Cued Click Point.
- SOM – Self organizing Map.
- ANN - Artificial Neural Network.
- UML – Unified Modeling Language.

CHAPTER 1 - INTRODUCTION

1.INTRODUCTION

Online banking has been around for quite a few years. In fact, it was introduced in the 1980s and has come a long way since then. The last decade has seen a profuse growth in internet banking transactions. Several pieces of legislation have also been introduced in this area. Though it began in the 1980s, it was only in the mid-nineties that internet banking really caught on. What attracts customers to internet banking is the round the clock availability and ease of transactions. Studies estimate that internet banking still has a long way to go.

There are several banks that have customers who prefer banking in the traditional ways. Some customers have been known to turn to internet banking due to dissatisfaction with standard procedures and practices. The total absence of human interaction appeals to some people. Some customers turn to internet banking facilities for security reasons. This is mainly because of customers being assured of banks' ability to keep transactions safe and secured.

Banks usually have a traditional login system where the user inputs registered username, followed by the registered password. If the login details are to be leaked/stolen then the account would be compromised. Here we implement another layer of security using image verification which incorporates pixel identification at its core for added security. Here along with the traditional login and password, the user also has to set-up image verification where the user has to first predefine a specific point on the image which will be used as the password for the image. Upon attempting login after setting up the image verification system the user logs into the account as usual but after the login page the image verification will be promoted. By failing this the user will be automatically redirected back to the login page. By this way even if the user account details are compromised the account is still protected because of this added security layer.

CHAPTER 2 –LITERATURE SURVEY

2. LITERATURE SURVEY

TITLE 1: New Physical Layer Key Generation Dimensions: Subcarrier Indices/Positions-Based Key Generation

AUTHOR : Haji M. Furqan, Jehad M. Hamamreh, and Huseyin Arslan, Fellow,IEEE.

YEAR : 2020

DESCRIPTION

In this paper, novel algorithms for secret key generation from the wireless channel in multi-carrier systems are proposed for ensuring the confidentiality and authentication in wireless communication systems. The novelty of the proposed algorithms lies in the generation of random secret bits not just from the magnitudes of orthogonal frequency division multiplexing (OFDM) subchannels as it has conventionally been done in the literature, but also from the indices/positions of the subchannels corresponding to highest gains. Thus, the proposed algorithms provide additional dimensions for enhancing overall key rates. The efficiency of the proposed algorithms is evaluated in terms of key mismatch rate (KMR) and key generation rate (KGR). Simulation results showed that the proposed algorithms can enhance the overall performance of physical layer keybased algorithms by providing extra dimensions for secret key generation.

ADVANTAGES

The proposed novel dimensions for secret key generation results in the enhancement of overall KGR without degrading overall performance as shown by simulation results.There is a 50 % increase in key rate as shown by JKG performance compared to the CKG approach due to the involvement of the proposed dimensions of key generation.The secret key generation can be extended to other domains such as time, space, and code domains

DISADVANTAGES

The broadcast nature of wireless communication makes it vulnerable to adversarial eavesdropping and intervention.to ensure confidentiality, integrity, and authentication of wireless communication, classic encryption-based techniques are employed at the upper layers.

TITLE 2: Authentication by Encrypted Negative Password

AUTHOR : Wenjian Luo, Senior Member, IEEE, Yamin Hu, Hao Jiang, and Junteng Wang

YEAR : 2018

DESCRIPTION

Secure password storage is a vital aspect in systems based on password authentication, which is still the most widely used authentication technique, despite its some security flaws. In this paper, we propose a password authentication framework that is designed for secure password storage and could be easily integrated into existing authentication systems. In our framework, first, the received plain password from a client is hashed through a cryptographic hash function (e.g., SHA-256). Then, the hashed password is converted into a negative password. Finally, the negative password is encrypted into an Encrypted Negative Password (abbreviated as ENP) using a symmetric-key algorithm (e.g., AES), and multi-iteration encryption could be employed to further improve security. The cryptographic hash function and symmetric encryption make it difficult to crack passwords from ENPs. Moreover, there are lots of corresponding ENPs for a given plain password, which makes precomputation attacks (e.g., lookup table attack and rainbow table attack) infeasible. The algorithm complexity analyses and comparisons show that the

ENP could resist lookup table attack and provide stronger password protection under dictionary attack. It is worth mentioning that the ENP does not introduce extra elements (e.g., salt); besides this, the ENP could still resist precomputation attacks. Most importantly, the ENP is the first password protection scheme that combines the cryptographic hash function, the negative password and the symmetric-key algorithm, without the need for additional information except the plain password.

ADVANTAGES

The lookup table could be quickly constructed, and the size of the lookup table could be sufficiently large, which results in a high success rate of cracking hashed passwords.

stretching schemes provide stronger password protection than salted password under dictionary attack, they impose an extra burden on programmers for configuring more parameters.

DISADVANTAGES

system problems may cause password compromises.

It is very difficult to obtain passwords from high security systems.stealing authentication data tables (containing usernames and passwords) in high security systems is difficult.

TITLE 3: Exploiting Mapping Diversity for Enhancing Security at Physical Layer in the Internet of Things

AUTHOR: Sasi Vinay Pechetti, Student Member, IEEE, Abhishek Jindal, Member

YEAR : 2018

DESCRIPTION

In health, defense, banking and other confidential information transfer urges the need for secure . As most of the devices are resource-limited (antennas, bandwidth, energy), securing the information transfer has always been a challenge. Looking at a solution for enhancing the security of single antenna, single carrier, energy efficient devices, we propose a novel scheme, channel-based mapping diversity (CBMD). This scheme uses the inherent randomness of the wireless channel and multiple mappings available for an M-ary phase shift keying (M-PSK) constellation in confusing an eavesdropper. When the legitimate and the eavesdropper channels are independent of each other, it is shown that a symbol error rate (SER) of M−1 M is induced at the eavesdropper. Whereas, when the channels are correlated, optimal and sub-optimal strategies at source and eavesdropper are derived for their respective optimal performances. Further, a closed-form expression for a lower-bound on the SER at the eavesdropper is derived. Simulation results show that for the correlated case, as SNR at the eavesdropper increases, SER initially decreases, later saturates to a relatively high SER, hence making the job of the eavesdropper difficult in getting the legitimate data. Furthermore, the effect of the correlation is more pronounced on SER at higher levels of correlation. This indicates that for practical correlation scenarios, SER is high enough to confuse the eavesdropper

ADVANTAGES

when the pattern is very long as it will skip checking character by character comparison.

The effect of the correlation is more pronounced on SER at higher levels of correlation.

DISADVANTAGES

It is possible to achieve perfect secrecy assuming that the channel from the sensor to the ally fusion center is independently fading with the channel from the sensor to the eavesdropping fusion center.

In addition, exchanging a pre-shared key securely is also an issue.

TITLE 4: An Efficient, Hybrid, Double-Hash StringMatching Algorithm

AUTHOR: Mehmet Bicer 1 and Xiaowen Zhang.

YEAR : 2019

DESCRIPTION

we show that combining some of the good features of the existing popular algorithms can be even more efficient. This new algorithm is hybrid as it employs features from Boyer-Moore-Horspool, Rabin-Karp and Raita algorithms. We compare the right most character as well as use two independent hash functions and no character by character checking - hence leaving a very small probability for a false positive result if there is any. The proposed algorithm particularly does well when the pattern is very long as it will skip checking character by character comparison.

ADVANTAGES

A very quick hash function goes through only first half of the string or pattern to create hash value 1 after the last character match hence quickly determines whether there is a mismatch or not.

Double-hash skips quickly once the last character does not match.

DISADVANTAGES

Check right most character only.

Skip based on bad-match table if right-most character does not match

Align or skip if one of the hash comparisons.

CHAPTER 3 – SYSTEM SPECIFICATIONS

3. SYSTEM SPECIFICATION

Software Requirements:

Operating System	:	Windows 7 or Higher
Languages used	:	Java (JSP, Servlet), HTML
Tools	:	visual studios code
Backend	:	PHP

Hardware Requirements:

Processor	:	Pentium Dual Core 2.3 GHz
Hard Disk	:	250 GB or Higher
Ram	:	2 GB

CHAPTER 4 – SYSTEM ANALYSIS

4. SYSTEM ANALYSIS

4.1 EXISTING SYSTEM

- In existing framework, same clients have the various online records they are utilizing comparable passwords for those records.
- In that time the programmers where an enemy may assault a record of a client utilizing the same or comparable passwords of his/her different less delicate records.
- It is secure against secret word related assaults, as well as can oppose replay assaults, bear surfing assaults, phishing assaults, and information break episodes.
- The above process is just used to keep up the amount of sum is exchanged from every single record this idea will be commendable if there should arise an occurrence of client see yet not to lessen the dark cash in the perspective of government.
- Different from existing works, we misuse dynamic verification accreditations alongside client driven access control to tackle the static qualification issue.
- In ordinary strategy in the event that you need to open one record implies we will give the username and give the watchword. So if it's conceivable someone else might be track our record detail.

DISADVANTAGES

- The security level of the current framework is low, so there might be shot of programmers may hacked our keeping money framework and gather the information.
- Difficult to keep up private subtle elements from programmer.

4.2 PROPOSED SYSTEM

- Here, we utilize progressed graphical verification strategy so it is exceptionally tough to crack.
- Data will be put away in encoded design so the security level turned out to be high.
- In the present framework, we keep up one of a kind code foe each exchange.
- The persuasive cued clicks help the users to choose more random positions for the increase of security.
- The advantages of the Graphical Password Scheme are the easy usability and greater security.

ADVANTAGES

- Here, we utilize progressed graphical verification strategy so it is exceptionally troublesome for other client to hacking.
- Data will be put away in encoded design so the security level turned out to be high.
- The persuasive cued clicks help the users to choose more random positions for the increase of security.

CHAPTER 5 – SYSTEM DESCRIPTION

5.1 ARCHITECTURE DIAGRAM

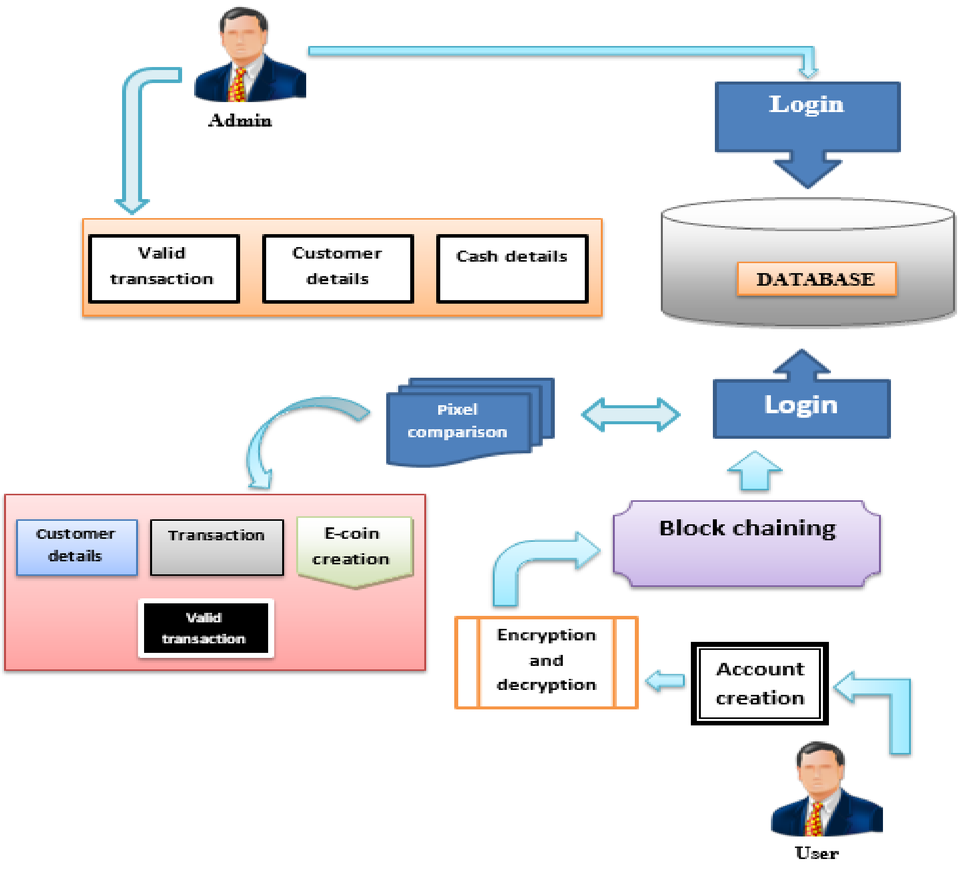


Figure 5.1

Here we have provided a clear architecture for our proposed system. Here the system works on two phase one is admin part and the user part. Admin can check the transaction, customer details and cash details. In the user part we stats with the creation of an individual bank account user data will be encrypted for security and before logging in the blocking chain is implemented for pixel comparisons. If the selected pixel matched then used is allowed to login. User can do transaction and while making money transfer an E-coin is generated randomly according to the note and amount is deposited to the account in the form of that e-coin key.

5.2 MODULES DESCRIPTION

Modules:

- **5.2.1 User Authentication**
- **5.2.2 Secured login**
- **5.2.3 Graphical Password**
- **5.2.4 Cued Recall Technique**

5.2.1 User Authentication:

Every last client login the page at that point makes the exchange and utilize this application. Validness is confirmation that a message, exchange, or other trade of data is from the source it cases to be from. Validness includes verification of character. We can check validness through confirmation. Enroll and login choice in landing page. Every single client needs to enlist as the new client for login. Client need to Fill the all prerequisite for security reason just, so fill the all subtle elements unique points of interest. Every one of the subtle elements spared in various ways. Make new table for every client and spare points of interest in like manner table. Those qualities utilized standardize and check for cash transmission preparing. Here to confirm the client points of interest for one time secret key sent to your enlisted mail id. At that point enter the way to confirm your subtle elements and can get to the page. Client accessible to see the adjust, see exchange history and make exchange of its own and client likewise see the what number of cash they have.

5.2.2 Secured login:

An effective and handy client confirmation conspire utilizing individual gadgets that use distinctive cryptographic natives, for example, encryption, advanced mark, pixel determination. The strategy profits by the broad utilization of figuring and different smart convenient gadgets that can empower clients to execute a safe verification convention. It keep up static username and secret key tables for distinguishing and confirming the authenticity of the login clients. Furthermore the picture pixel utilizing for to open the record. In the event that we are not pick amend point picture implies the record won't open. It is secure technique.

5.2.3 Graphical Password:

A graphical password is an authentication technique which asks the user to select details from images displayed on a Graphical User Interface.It may be selection of many details that has to be selected in a specific order which will increase the security. The password is set by the user initially and his knowledge and memory for remembering it will be the key to access the information from a system. This is why it is under the category of Knowledge based. As a graphical password is used on graphical user interface, the techniques are also called as Graphical User Authentication.

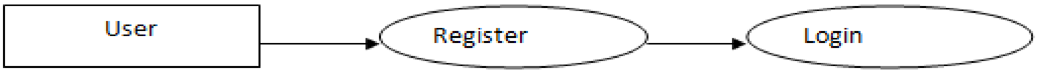
5.2.4 Cued Recall Technique:

In this technique the user has to select a specific points or locations on an image while registering. For logging in to the system, user has to click on same points that selected during the registration. This will increase the security by avoiding many attacks by intruders.

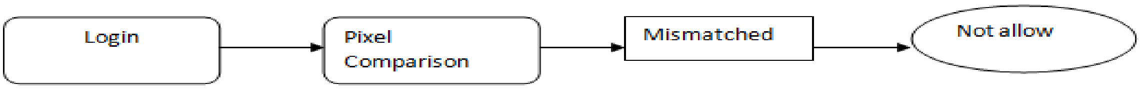
CHAPTER 6– SYSTEM DESIGN

6.1 Data flow diagram

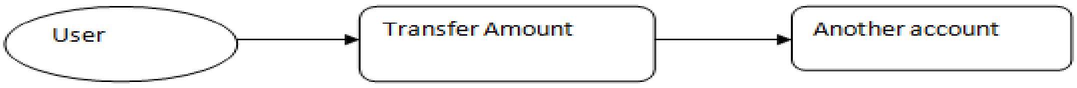
Level 0



Level 1



Level 2



Level 3

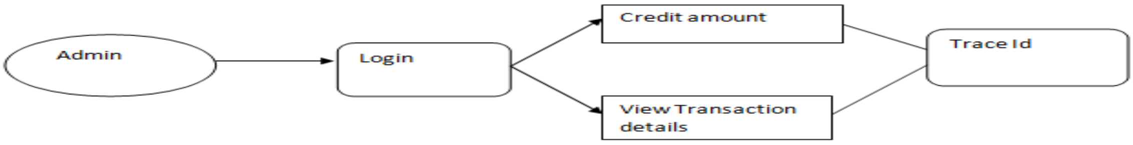


Figure 6.1

6.2 ER diagram

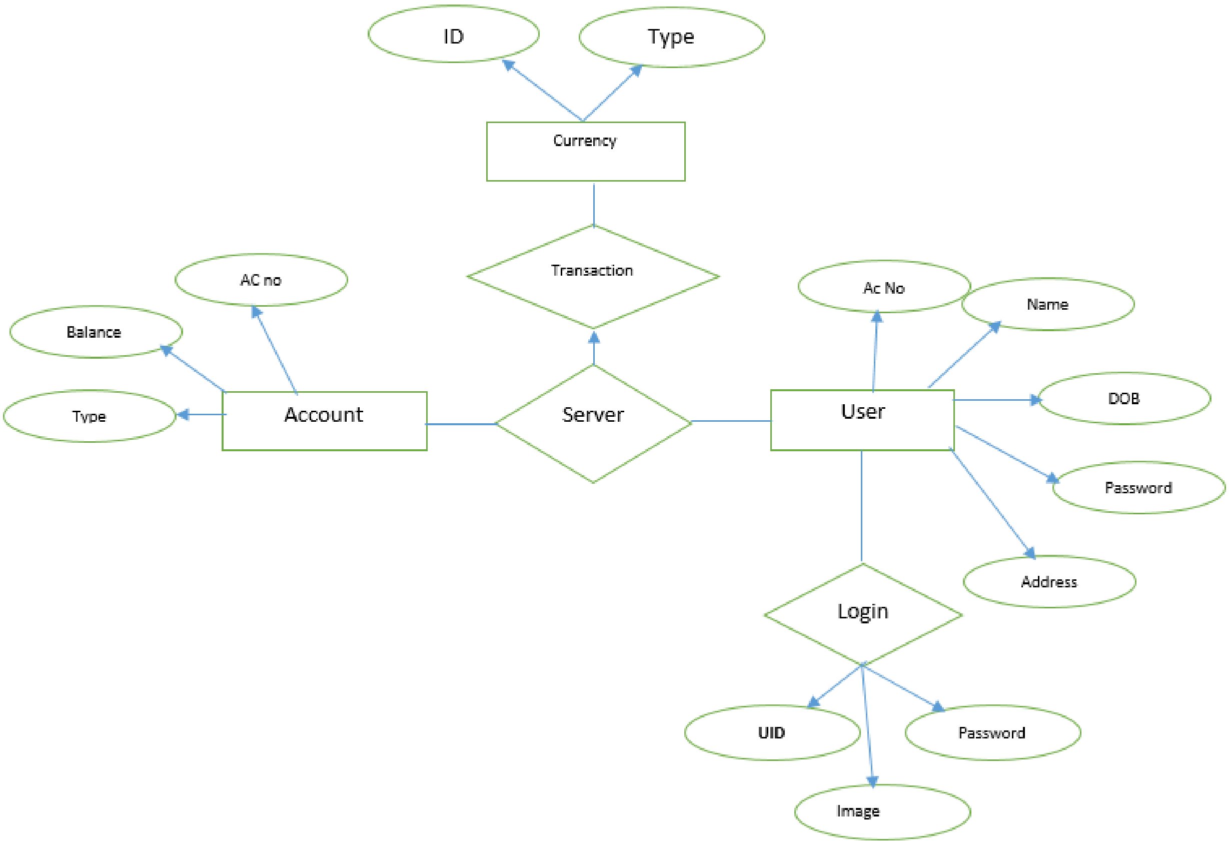


Figure 6.2

6.3 Class diagram

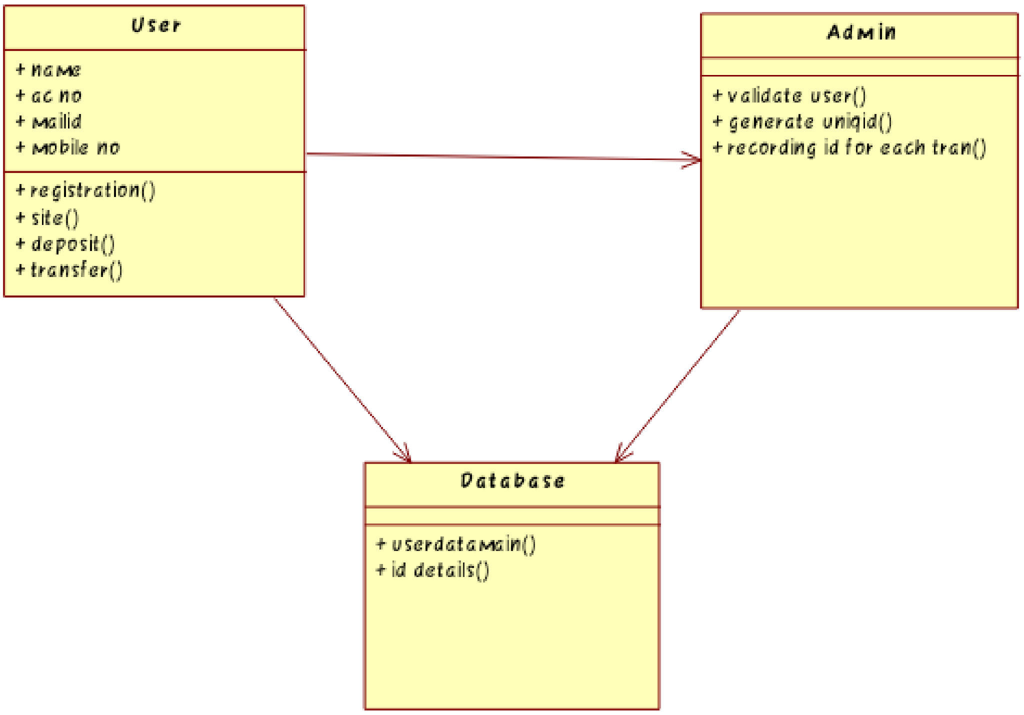


Figure 6.3

The class diagram is a static diagram. It represents the static view of an application. Class diagram is not only used for visualizing, describing and documenting different aspects of a system but also for constructin executable code of the software application. The class diagram describes the attributes and operations of a class and also the constraints imposed on the system. The class diagrams are widely used in the modelling of object oriented systems because they are the only UML diagrams which can be mapped directly with object oriented languages. The class diagram shows a collection of classes, interfaces, associations, collaborations and constraints. It is also known as a structural diagram. The purpose of the class diagram is to model the static view of an application. The class diagrams are the only diagrams which can be directly mapped with object oriented languages and thus widely used at the time of construction. The UML diagrams like activity diagram, sequence diagram can only give the sequence flow of the application but class diagram is a bit different. So it is the most popular UML diagram in the coder community.

So the purpose of the class diagram can be summarized as:

- Analysis and design of the static view of an application.
- Describe responsibilities of a system.
- Base for component and deployment diagrams.
- Forward and reverse engineering.

6.4 Use case diagram

In software and systems engineering, a use case is a list of steps, typically defining interactions between a role (known in UML as an "actor") and a system, to achieve a goal. The actor can be a human or an external system. In systems engineering, use cases are used at a higher level than within software engineering, often representing missions or stakeholder goals. The detailed requirements may then be captured is php or as contractual statements.

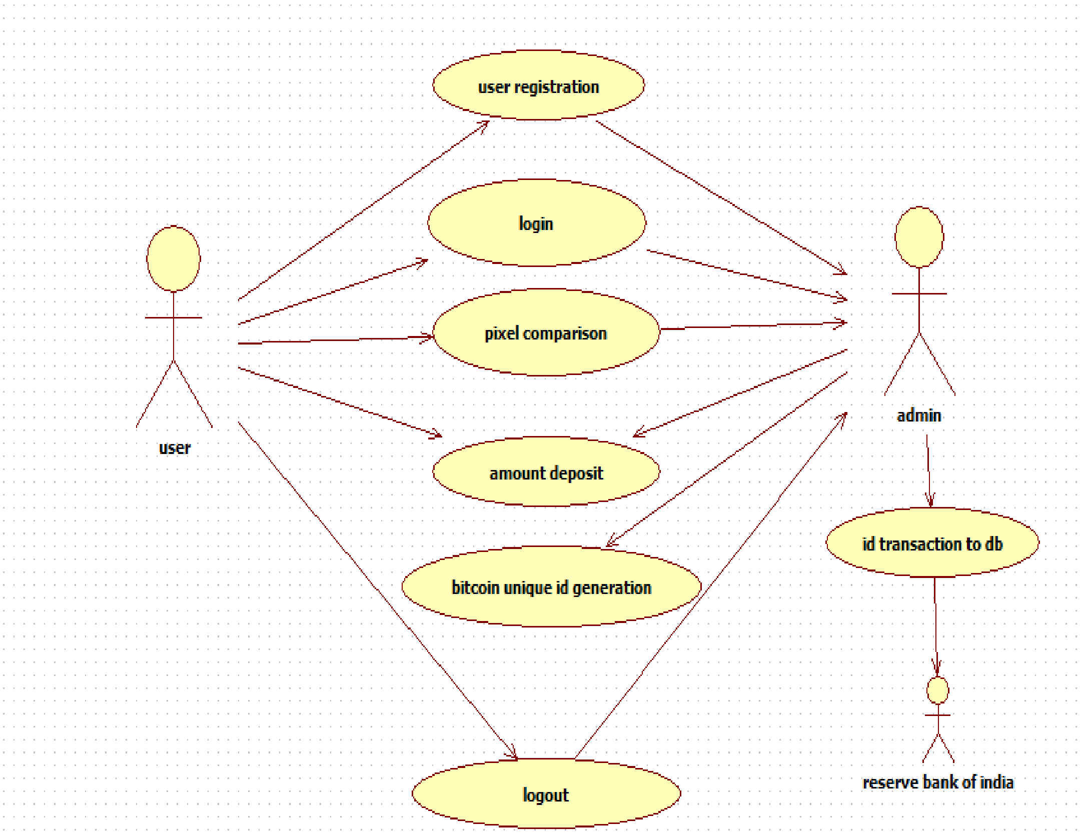


Figure 6.4

6.5 Activity Diagram

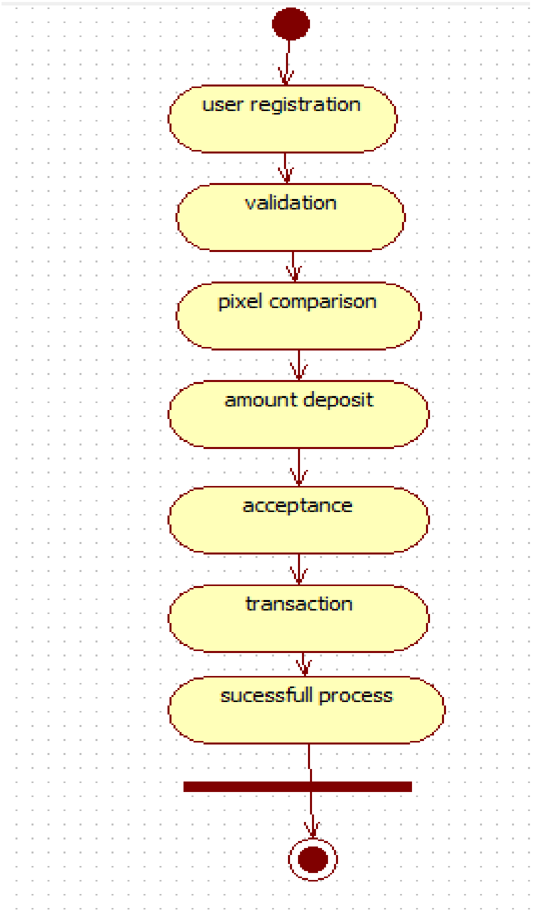


Figure 6.5

Activity diagram is another important diagram in UML to describe dynamic aspects of the system. Activity diagram is basically a flow chart to represent the flow form one activity to another activity. The activity can be described as an operation of the system. So the control flow is drawn from one operation to another. This flow can be sequential, branched or concurrent. Activity diagrams deals with all type of flow control by using different elements like fork, join etc. The basic purposes of activity diagrams are similar to other four diagrams. It captures the dynamic behavior of the system. Other four diagrams are used to show the message flow from one object to another but activity diagram is used to show message flow from one activity to another. Activity is a particular operation of the system. Activity diagrams are not only used for visualizing dynamic nature of a system but they are also used to construct the executable system by using forward and reverse.

engineering techniques. The only missing thing in activity diagram is the message part. It does not show any message flow from one activity to another. Activity diagram is some time considered as the flow chart. Although the diagrams looks like a flow chart but it is not. It shows different flow like parallel, branched, concurrent and single.

So the purposes can be described as:

- Draw the activity flow of a system.
- Describe the sequence from one activity to another.
- Describe the parallel, branched and concurrent flow of the system**.**

6.6 Sequence Diagram

A sequence diagram in a Unified Modeling Language (UML) is a kind of interaction diagram that shows how processes operate with one another and in what order. It is a construct of a Message Sequence Chart. A sequence diagram shows object interactions arranged in time sequence. It depicts the objects and classes involved in the scenario and the sequence of messages exchanged between the objects needed to carry out the functionality of the scenario. Sequence diagrams typically are associated with use case realizations in the Logical View of the system under development. Sequence diagrams are sometimes called event diagrams, event scenarios, and timing diagrams.

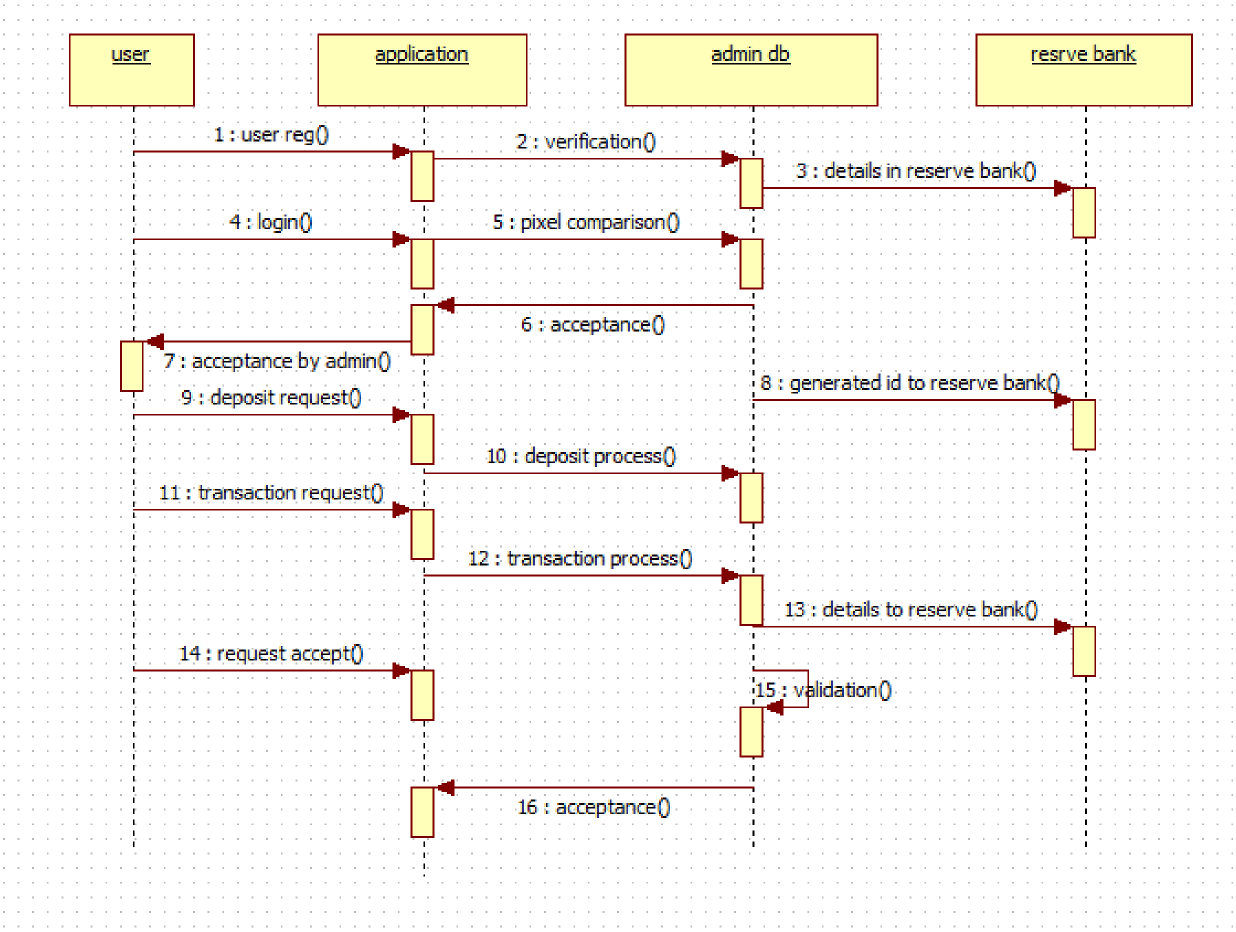


Figure 6.6

6.7 COLLABORATION DIAGRAM

A collaboration diagram, also called a communication diagram or interaction diagram, is an illustration of the relationships and interactions among software objects in the Unified Modeling Language (UML). The concept is more than a decade old although it has been refined as modeling paradigms have evolved. A collaboration diagram resembles a flowchartthat portrays the roles, functionality and behavior of individual objects as well as the overall operation of the system in real time. Objects are shown as rectangles with naming labels inside. These labels are preceded by colons and may be underlined. The relationships between the objects are shown as lines connecting the rectangles.

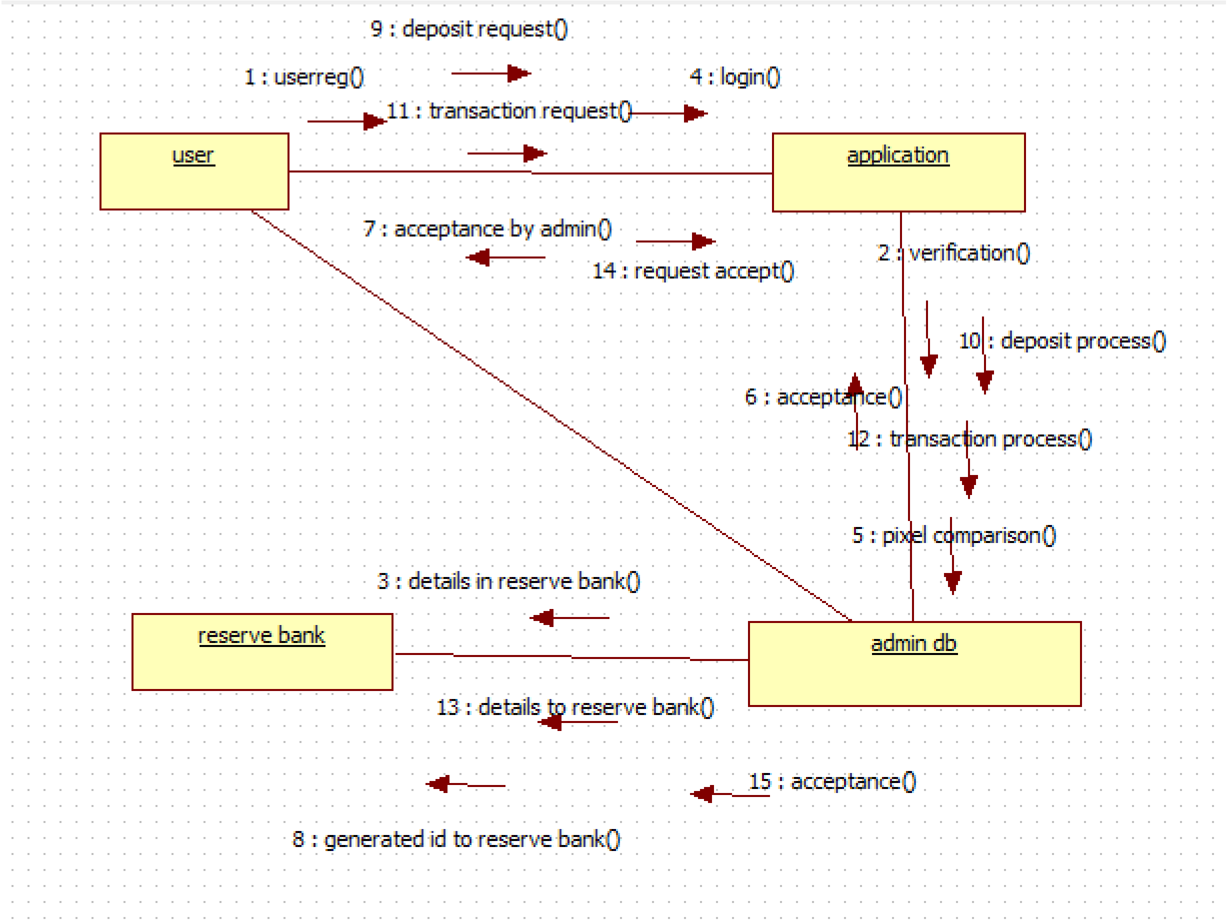


Figure 6.7

CHAPTER 7– SYSTEM IMPLEMENTATION AND TESTING

7.1 IMPLEMENTATION

System implementation projects are long difficult journeys by which organisations move from an old set of technology/methods/procedures to a new one. A software implementation method is a systematic structured approach to effectively integrate software based service or component into the workflow of an organizational structure or an individual end-user. The complexity of implementing product software differs on several issues. Examples are: the number of end users that will use the product software, the effects that the implementation has on changes of tasks and responsibilities for the end user, the culture and the integrity of the organization where the software is going to be used and the budget available. It is vital to select the right strategy for implementing the application to assure successful results.

7.1.1 Direct Implementation

With this method of implementation the users stop using the manual system and start using the computer system from a given date. The advantage of this method is that it is less costly in effort and time than any other method of implementation. The disadvantage of this method is that if problems occur the users do not have any alternative apart from returning to a manual system which may prove difficult if it has been discontinued.

7.1.2 Phased Implementation

The phased implementation method enables us to break our project in to smaller milestones. Major disadvantage is difficult to achieve due to interdependencies between modules.

7.1.3 Implementation Strategy

Since the software application consists of three modules as per in the high level architectural design, the implementation was done using iterative, incremental approach. Phase wise implementation process enables to execute by incrementally aligning the product with the end-user.

7.2 TESTING

Software Testing is the process of executing a program or system with the intent of finding errors. The scope of software testing often includes examination of code as well as execution of that code in various environments and conditions.

7.2.1 Black Box Testing

Black Box Testing is testing without the knowledge of the internal workings of the item being tested. When black box testing is applied to software engineering, the tester selects valid and invalid input and what the expected outputs should be, but not how the program actually arrives at those outputs.Black box testing methods include equivalence partitioning, boundary value analysis, all-pairs testing, fuzz testing, model-based testing, traceability matrix, exploratory testing and specification-based testing. This method of test design is applicable to all levels of software testing: unit, integration, functional testing, system and acceptance.

7.2.2 White Box Testing

White box testing (glass box testing) strategy deals with the internal data structures and algorithms. The tests written based on the white box testing strategy incorporate coverage of the code written, branches, paths, statements and internal logic of the code etc. These testers require programming skills to identify all paths through the software.

7.2.3 Test Case

Test Case ID: 1

Test Type : Software

Operation : System Login

ACTION	INPUT	EXPECTED OUTPUT	STATUS
Input Correct user ID and correct password.	2549532555 demo	Proceed to image verification page.	pass
Type invalid User ID and keep password empty then click log in button	3489515515 -	Display Login failed!!! under login field.	pass
Type invalid User ID and type correct password then click log in button.	8449651644 demo	Display Login failed!!! under login field.	pass
Type valid User ID and keep password empty then click log in button.	2549532555 -	Display Login failed!!! under login field.	pass

Type valid User ID and invalid password then click login button.	2549532555 memo	Display Login failed!!! under login field.	pass
Keep both user ID and password empty and click login button.	- -	Display Login failed!!! under login field.	pass
Type both user ID and password invalid and click login button.	84364984 memo	Display Login failed!!! under login field.	pass
Keep user ID blank and type correct password and click login button.	- demo	Display Login failed!!! under login field.	pass

Table 7.1 Test Case Login

Test Case ID: 2

Test Type : Software

Operation : Registration

ACTION	**INPUT**	**EXPECTED OUTPUT**	**STATUS**
Leave one or more fields empty	Roy - -	Please fill out the field	pass
Input all the field	Roy 2549532555	Registration completed	pass

Enter alphabet in account number field	yvbn	Display must input number	pass
Enter less than 10 mobile numbers in field	854156 35	Display please enter valid mobile number	pass

Table 7.2 Test Case Registration

Test Case ID: 3

Test Type : Software

Operation : Transaction

	INPUT	**EXPECTED OUTPUT**	**STATUS**
Enter valid account number and empty account name	5268486324 -	Display please enter the account name	pass
Enter invalid account number and valid account name	545632632 Raja	Display sorry account number is not valid	pass
Enter account name and account number is correct but	5268486324 Raja -	Display total amount is can not be empty	pass

amount field is empty			
Enter account name, account number is correct and fill amount field	5268486324 Raja 5000	Display amount can be transferred successfully	pass

Table 7.3 Test Case Transaction

7.2.4 Test Report

Test case ID	Actual Output	Status
1	● Login to the image pin when user id and password is correct. ● Display error message ”Login failed!!!” under login field when the user id or password is incorrect. ● Display error message ”Login failed!!!” under login field when user is correct and password is incorrect. ● When user id and password is correct, proceed to image verification page.	Pass Pass Pass Pass Pass

	● Login to the system dashboard when user id, password and image pin is correct.	
2	● Completing the registration format process it is successfully completed.	Pass
3	● Completing the transaction format process it is successfully completed	

Table 7.4 Test Report

CHAPTER 8 – CONCLUSION

8. CONCLUSION

This is the undertaking which can change the fiscal status of our country if it is executed by the banks and the significant research is going in light of the bit coin so our thought will be important for the pros. As an issue of first significance, we should need to inspect using lightweight cryptographic frameworks in our diagram. Second, we plan to analyze the blueprint of different customer driven access control models. Our proposed plan is definitely not hard to-learn and easy to-use since customers do nothing past entering one time username and affirmation code. By then select the pixel of picture, in case it is correct entering account for the most part pixels change reliably. The username, watchword is memory canny simple because customers of our arrangement don't have to review any secret at all. In perspective of the structure, our answer is versatile for customers since it diminishes the threat of username/mystery word reuse transversely finished various regions and organizations. Note that we are utilizing an individual contraption that is passed on by the customer as a general rule and the customer does not need to pass on an additional hardware or any physical inquiry for approval. This thought will be to a great degree profitable wherever all through the world in light of its extraordinary id age for each and every single note submitted to the system.

APPENDIX – 1

SAMPLE CODING

SOURCE CODE-LOGIN PAGE

```
<!DOCTYPE html>
<html lang="en" dir="ltr">
  <head>
    <meta charset="utf-8">
    <title>LOGIN</title>
  </head>
  <body>
    <div class="center">
      <h1>Login</h1>
      <form id="submit" onsubmit ="return verifyPassword() ">
        <div class="txt_field">
          <input id="txt" type="text" required>
          <span></span>
          <label for="UserName"> UserName</label>
        </div>
        <div class="txt_field">
          <input id="pass"type="password" required>
          <span></span>
          <label for="password">password</label>
        </div>
        <div class="text_field">
          <input type="submit" value="Login">
        </div>

        <div class="signup_link">
          Not a member? <a
href="PersonalDetails.html">Signup</a>
        </div>



      </form>
    </div>

<style>
*{
  margin: 0;
  padding: 0;
  box-sizing: border-box;
  font-family: "Poppins", sans-serif;
}
body{
  margin: 0;
  padding: 0;
  background: linear-gradient(120deg,#2980b9, #8e44ad);
  height: 100vh;
  overflow: hidden;
}
.center{
  position: absolute;
  top: 50%;
  left: 50%;
  transform: translate(-50%, -50%);
  width: 400px;
  background: white;
  border-radius: 10px;
  box-shadow: 10px 10px 15px rgba(0,0,0,0.05);
}
.center h1{
  text-align: center;
  padding: 20px 0;
  border-bottom: 1px solid silver;
}
.center form{
  padding: 0 40px;
  box-sizing: border-box;
}
form .txt_field{
  position: relative;
  border-bottom: 2px solid #adadad;
  margin: 30px 0;
}
.txt_field input{
  width: 100%;
  padding: 0 5px;
  height: 40px;
  font-size: 16px;
  border: none;
  background: none;
  outline: none;
```

```
}
.txt_field label{
  position: absolute;
  top: 50%;
  left: 5px;
  color: #adadad;
  transform: translateY(-50%);
  font-size: 16px;
  pointer-events: none;
  transition: .5s;
}
.txt_field span::before{
  content: '';
  position: absolute;
  top: 40px;
  left: 0;
  width: 0%;
  height: 2px;
  background: #2691d9;
  transition: .5s;
}
.txt_field input:focus ~ label,
.txt_field input:valid ~ label{
  top: -5px;
  color: #2691d9;
}
.txt_field input:focus ~ span::before,
.txt_field input:valid ~ span::before{
  width: 100%;
```

```
}
.pass{
  margin: -5px 0 20px 5px;
  color: #a6a6a6;
  cursor: pointer;
}
.pass:hover{
  text-decoration: underline;
}
input[type="submit"]{
  width: 100%;
  height: 50px;
  border: 1px solid;
  background: #2691d9;
  border-radius: 25px;
  font-size: 18px;
  color: #e9f4fb;
  font-weight: 700;
  cursor: pointer;
  outline: none;
}
input[type="submit"]:hover{
  border-color: #2691d9;
  transition: .5s;
}
.signup_link{
  margin: 30px 0;
  text-align: center;
  font-size: 16px;
  color: #666666;
}
.signup_link a{
  color: #2691d9;
  text-decoration: none;
}
.signup_link a:hover{
  text-decoration: underline;
}

</style>
<script>
function verifyPassword() {
          var tx = document.getElementById("").value;
          var pw = document.getElementById("pass").value;
          if (tx=="Ronald" && pw=="1234")
          {
            document.getElementById("submit").action = "2nd-Page.html";
          }
         else{
              alert("WRONG PASSWORD or USER-NAME");
             }
}
</script>
</body>
</html>
```

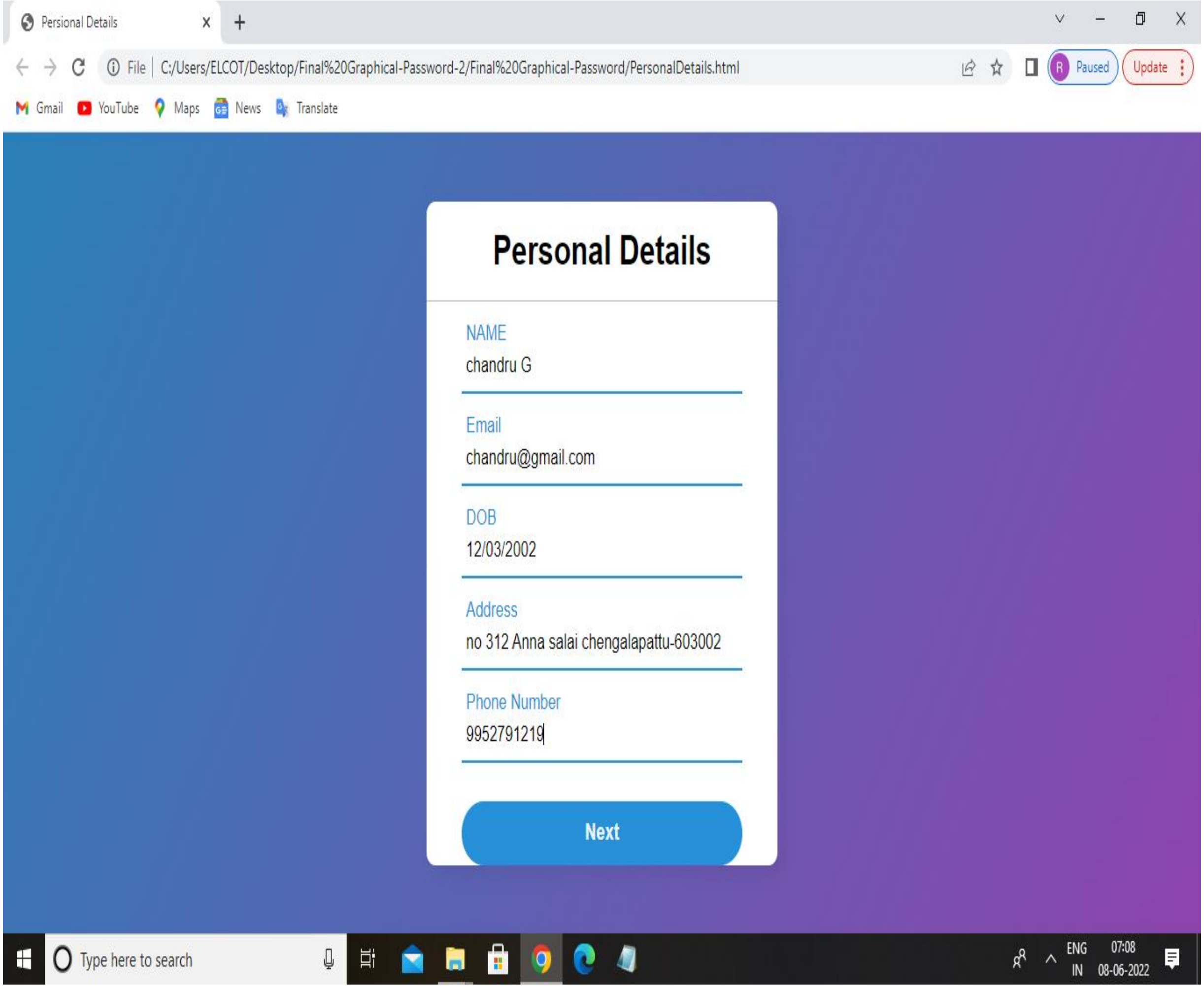
SOURCE CODE - CHOOSE POINT

```
    <html>

    <head>

       <title>Image-Authentication</title>

     </head>

    <script>

      function dis(val)

    {

   document.getElementById("pswd").value+=val

}

 function verifyPassword()

var pw = document.getElementById("pswd").value;

        if (pw=="7PI"){

            document.getElementById("submit").action = "3rd-Page.html";

  }

   else{

            alert("WRONG PASSWORD")

}
```

```
}
 </script>
  <body>
 <div class="body">
   <div class="container1">
  <input class="grid-cell" type="button" value="0" onclick="dis('0')"/>
 <input class="grid-cell" type="button" value="1" onclick="dis('1')"/>
 <input class="grid-cell" type="button" value="2" onclick="dis('2')"/>
<input class="grid-cell" type="button" value="3" onclick="dis('3')"/>
 <input class="grid-cell" type="button" value="4" onclick="dis('4')"/>
 <input class="grid-cell" type="button" value="5" onclick="dis('5')"/>
  <input class="grid-cell" type="button" value="6" onclick="dis('6')"/>
  <input class="grid-cell" type="button" value="7" onclick="dis('7')"/
<input class="grid-cell" type="button" value="8" onclick="dis('8')"/>
  <input class="grid-cell" type="button" value="9" onclick="dis('9')"/>
  <input class="grid-cell" type="button" value="A" onclick="dis('A')"/>
<input class="grid-cell" type="button" value="B" onclick="dis('B')"/>
 <input class="grid-cell" type="button" value="C" onclick="dis('C')"/>
 <input class="grid-cell" type="button" value="D" onclick="dis('D')"/>

<input class="grid-cell" type="button" value="E" onclick="dis('E')"/>

<input class="grid-cell" type="button" value="F" onclick="dis('F')"/>

<input class="grid-cell" type="button" value="I" onclick="dis('I')"/>

  <input class="grid-cell" type="button" value="J" onclick="dis('J')"/>

 <input class="grid-cell" type="button" value="K" onclick="dis('K')"/>

 <input class="grid-cell" type="button" value="L" onclick="dis('L')"/>

<input class="grid-cell" type="button" value="M" onclick="dis('M')"/>

<input class="grid-cell" type="button" value="N" onclick="dis('N')"/>

 <input class="grid-cell" type="button" value="O" onclick="dis('O')"/>

<input class="grid-cell" type="button" value="P" onclick="dis('P')"/>

 </div>

 <div class="container" style = "position:relative; left:80px; bottom:-600px;">

     <centre>

<form id="submit" class="button" onsubmit ="return verifyPassword()">

 <input type = "password" id = "pswd" value = "">

       </centre>

</div>
```

```
<div class="input" style = "position:relative; left:43%; top:530px;">

<input type = "submit" value = "Next">

 </div>

 </form>

</body>

</htlm>
```

APPENDIX -2 SCREENSHOTS AND WORKING OF WEBSITE



Personal Details

NAME
chandru G

Email
chandru@gmail.com

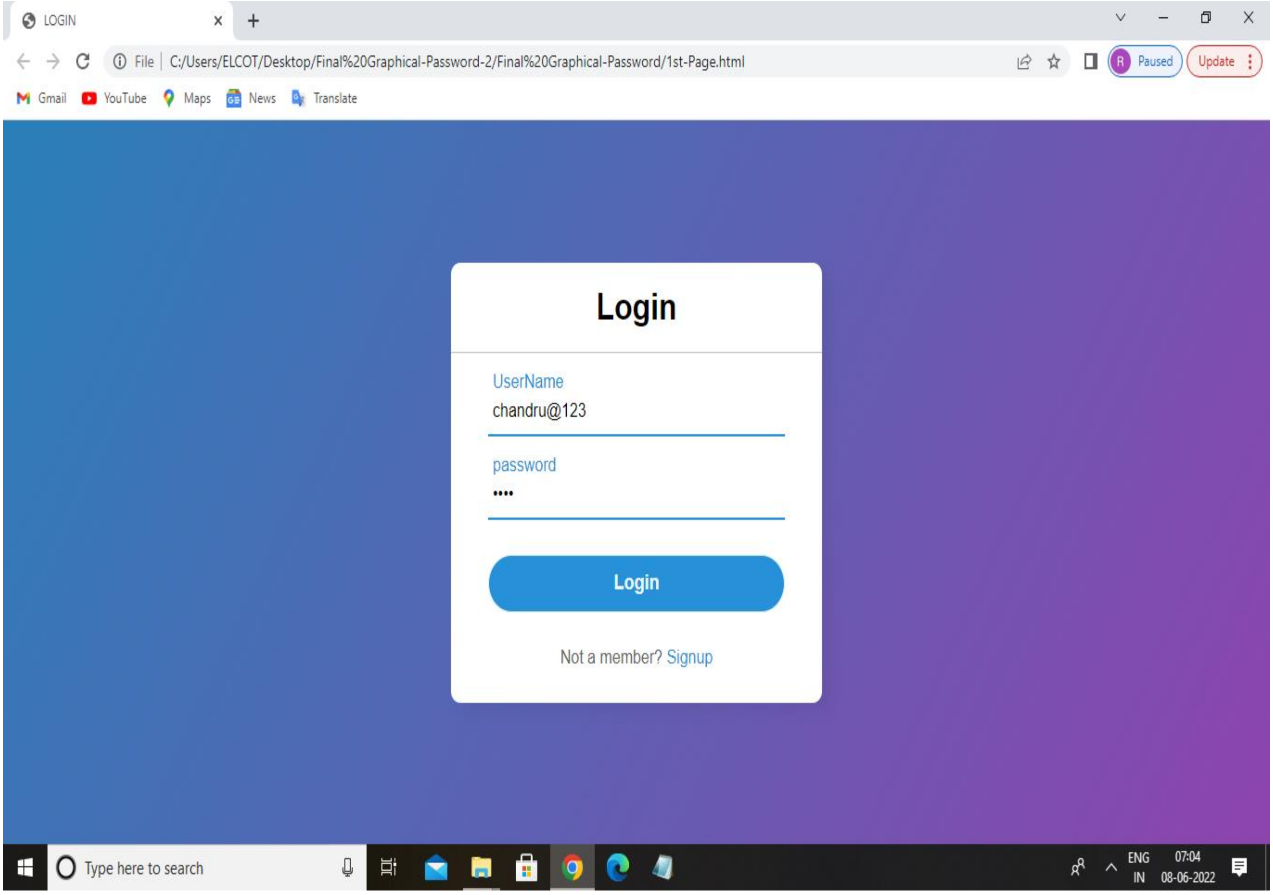
DOB
12/03/2002

Address
no 312 Anna salai chengalapattu-603002

Phone Number
9952791219

Persional Details
File | C:/Users/ELCOT/Desktop/Final%20Graphical-Password-2/Final%20Graphical-Password/PersonalDetails.html
Paused
Update
Gmail
YouTube
Maps
News
Translate
Next
Type here to search
ENG
IN
07:08
08-06-2022

REGISTRATION FORM



LOGIN
C:/Users/ELCOT/Desktop/Final%20Graphical-Password-2/Final%20Graphical-Password/1st-Page.html
Gmail
YouTube
Maps
News
Translate
Paused
Update
Type here to search
ENG
IN
07:04
08-06-2022

Login

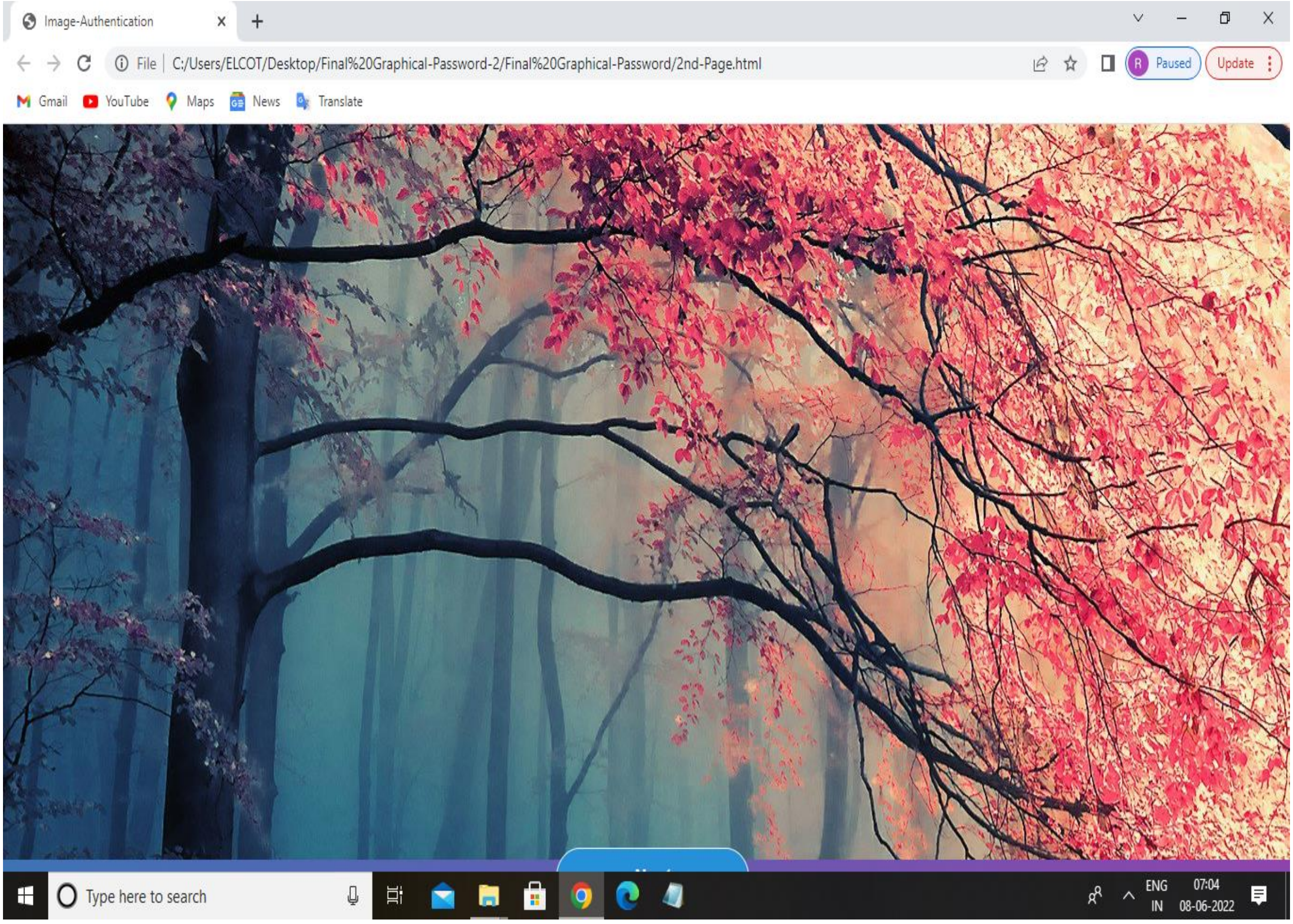
UserName
chandru@123

password
••••

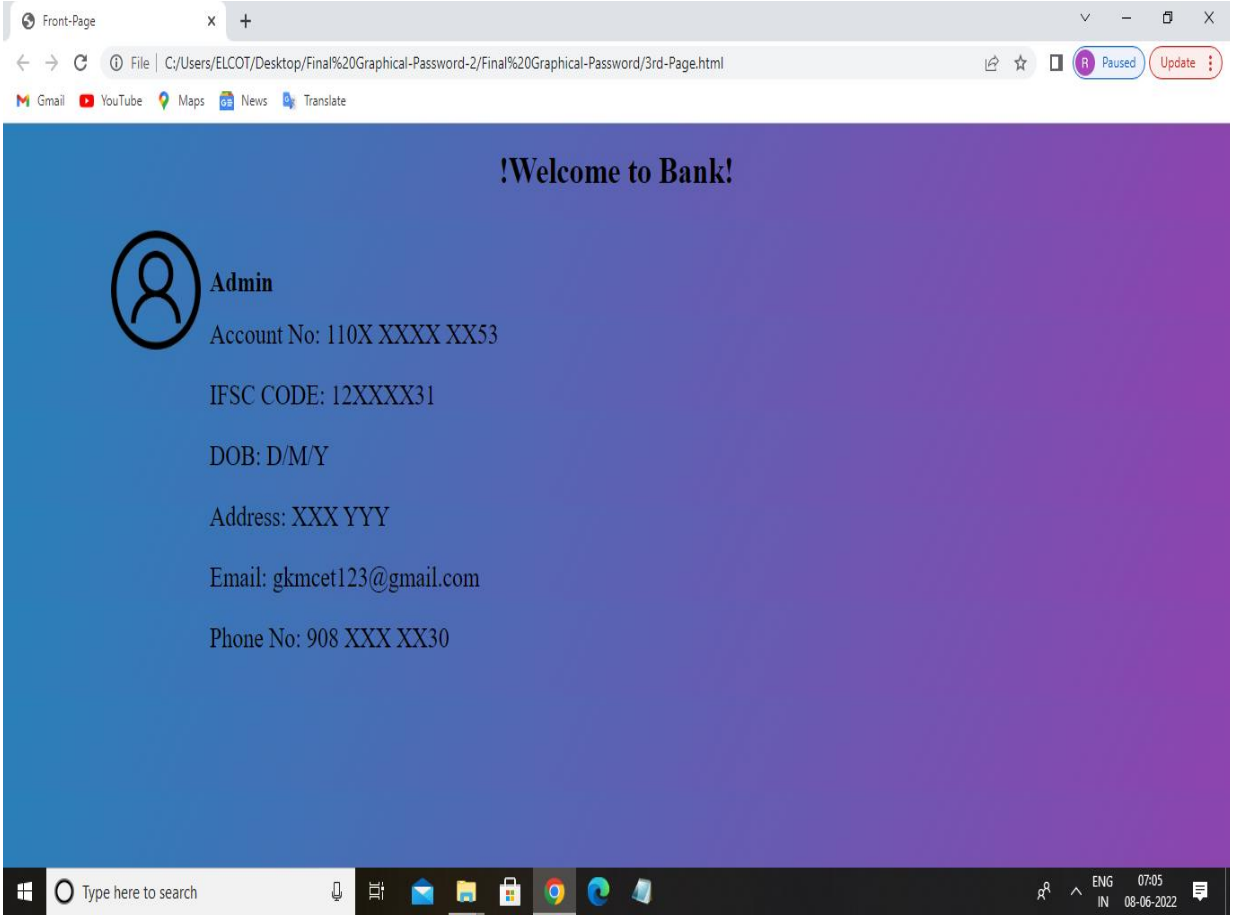
Login

Not a member? Signup

LOGIN PAGE



GRAPHICAL PASSWORD AUTHENTICATION



Front-Page
File | C:/Users/ELCOT/Desktop/Final%20Graphical-Password-2/Final%20Graphical-Password/3rd-Page.html
Paused
Update
Gmail
YouTube
Maps
News
Translate
Type here to search
ENG
IN
07:05
08-06-2022

!Welcome to Bank!

Admin

Account No: 110X XXXX XX53

IFSC CODE: 12XXXX31

DOB: D/M/Y

Address: XXX YYY

Email: gkmcet123@gmail.com

Phone No: 908 XXX XX30

LOGIN SUCCESSFULL

REFERENCES

1.Alhothaily, A. Alrawais, X. Cheng, and R. Bie. A novel verification method for payment card systems. Personal and Ubiquitous Computing, 19(7):1145–1156, 2015.

2. A. Alrawais, A. Alhothaily, C. Hu, X. Xing, and X. Cheng. An attributebased encryption scheme to secure fog communications. IEEE Access, 2017.

3. A. Hiltgen, T. Kramp, and T. Weigold. Secure internet banking authentication. IEEE Security Privacy, 4(2):21–29, March 2006.

4. Borchert and M. Gunther. Indirect nfc-login. In Internet Technology and Secured Transactions (ICITST), 2013 8th International Conference for, pages 204–209. IEEE, 2013.

5.Das, J. Bonneau, M. Caesar, N. Borisov, and X. Wang. The tangled web of password reuse. In Symposium on Network and Distributed System Security (NDSS), 2014.

6. L. O. Gorman. Comparing passwords, tokens, and biometrics for user authentication. Proceedings of the IEEE, 91(12):2021–2040, 2003.

7.Marforio, N. Karapanos, C. Soriente, K. Kostiainen, and S. Capkun. Smartphones as practical and secure location verification tokens for payments. In Proceedings of the Network and Distributed System Security Symposium, NDSS, 2014.

8.Miers, C. Garman, M. Green, and A. Rubin. Zerocoin: Anonymous distributed e-cash from bitcoin. In Security and Privacy (SP), 2013 IEEE Symposium on, pages 397–411, May 2013.

9. X. Fang and J. Zhan. Online banking authentication using mobile phones. In Future Information Technology (FutureTech), 2010 5th International Conference on, pages 1–5. IEEE, 2010.

10. Y. S. Lee, N. H. Kim, H. Lim, H. Jo, and H. J. Lee. Online banking authentication system using mobile-otp with qr-code. In Computer Sciences and Convergence Information Technology (ICCIT), 2010 5th International Conference on, pages 644–648. IEEE, 2010.