DESIGN AND DEVELOPMENT OF GRAPHICAL PASSWORD AUTHENTICATION SYSTEM

A

MINOR PROJECT-II

Submitted in partial fulfillment of the requirements for the degree of

BACHELORS OF TECHNOLOGY

in

COMPUTER SCIENCE & ENGINEERING

By

GROUP NO. 22

SANJEEV KUMAR SINGH	**0187CS201147**
SACHIN KUMAR	**0187CS201141**
SAHIL CHOUDHARY	**0187CS201143**
VIVEK VERMA	**0187CS201183**

Under the guidance of

PROF. RUCHI JAIN

(ASSISTANT PROFESSOR)

Jan-April 2023

Department of COMPUTER SCIENCE & ENGINEERING Sagar Institute of Science & Technology (SISTec)

Bhopal (M.P.)
Approved by AICTE, New Delhi & Govt. of M.P.
Affiliated to Rajiv Gandhi Proudyogiki Vishwavidyalaya, Bhopal (M.P)

Sagar Institute of Science & Technology (SISTec), Bhopal
Department of COMPUTER SCIENCE & ENGINEERING
Bhopal (M.P.)

April-2023

CERTIFICATE

We hereby certify that the work which is being presented in the B.Tech. Minor Project-II Report entitled design and development of graphical password authentication system**,** in partial fulfillment of the requirements for the award of the degree of ***Bachelor of Technology*** in ***Computer Science & Engineering*** and submitted to the Department of Computer Science & Engineering, *Sagar Institute of Science & Technology (SISTec)***,** Bhopal (M.P.) is an authentic record of my own work carried out during the period from Jan-2023 to April-2023 under the supervision of **Prof. Ruchi Jain .**

The content presented in this project has not been submitted by me for the award of any other degree elsewhere.

Signature

Sanjeev Kumar Singh	0187CS201147
Sachin Kumar	0187CS201141
Sahil Choudhary	0187CS201143
Vivek Verma	0187CS201183

This is to certify that the above statement made by the candidate is correct to the best of my knowledge.

Date:

Prof. Ruchi Jain	**Prof. Rahul Dubey**	**Dr. Keshavendra Choudhary**
Project Guide	**HOD**	**Principal**

ABSTRACT

A graphical password authentication system is a type of security mechanism that uses images or graphical elements as the basis for authentication. Unlike traditional alphanumeric passwords, graphical passwords rely on users selecting specific images or performing specific actions on images to prove their identity. The basic idea behind a graphical password authentication system is that users create a unique password by selecting specific images, drawing shapes or patterns, or performing other actions on a graphical user interface. Graphical password authentication systems have emerged as a promising alternative to traditional text-based password systems. In these systems, users create a password by selecting specific images, drawing patterns, or clicking on certain parts of an image and build strong and easy to remember passwords. One of the main advantages of graphical password authentication systems is that they can be more secure than traditional password systems because they are often more difficult for hackers to guess or crack. They can also be easier for users to remember because they are based on visual memory. Graphical password authentication systems have the potential to be a more secure and user-friendly authentication method and emerging technique.

ACKNOWLEGMENT

We would like to express our sincere gratitude to several individuals and our college for supporting us throughout our project . First, we wish to express my sincere gratitude to Our guide, Prof. Ruchi Jain for her enthusiasm, patience, insightful comments, helpful information, practical advice and unceasing ideas that have helped us tremendously at all times in our research. Without her support and guidance, this project would not have been possible. We could not have imagined having a better supervisor in our study. We also wish to express my sincere thanks to the Sagar Institute of Science & Technology for giving us this opportunity. We are grateful and lucky enough to receive consistent motivation, assistance, and advice from all the faculties of the Department of Computer Science who have helped us to complete our project work.

We would also like to extend our heartfelt respects to the entire Department of Computer Science for their timely assistance.

We would like to express our sincere thanks to Dr. Swati Saxena, Vice Principal, SISTec, Gandhi Nagar, Bhopal for giving us an opportunity to undertake this project. We also wish to express our gratitude to Prof. Rahul Dubey Head, Department of Computer Science and Engineering, for his kind-hearted support.

TABLE OF CONTENTS

TITLE		PAGE NO
Abstract		iii
Acknowledgement		iv
List of figures		vi
List of abbreviations		vii
Chapter 1	Introduction	1
	1.1 About Project	1
	1.2 Project Objectives	3
Chapter 2	Software and Hardware Requirements	4
Chapter 3	Problem Description	5
Chapter 4	Literature Survey	7
Chapter 5	Software Requirements Specification	9
	5.1 Functional Requirements	9
	5.2 Non-Functional Requirements	9
Chapter 6	Software Design	10
	6.1 Use case diagram	10
	6.2 ER Diagram	11
	6.3 Data flow diagram	11
Chapter 7	Output Screens	12
Chapter 8	Conclusion and Future work	16
References		17
Appendix-1: Glossary of Terms		18
Project Summary		19

List of Figures

FIG. NO.	TITLE	PAGE NO.
Fig 1.1	Use case diagram	10
Fig 1.2	ER diagram	11
Fig 1.3	Data flow diagram	11
Fig 2.1	User data	12
Fig 2.2	Login page	13
Fig 2.3	Registration page	14
Fig 2.4	Set password	15

LIST OF ABBREVIATIONS

ACRONYM	FULL FORM
SDLC	Software Development Life Cycle
SQL	Structured Query Language
GPA	Graphical Password Authentication
UML	Unified Modeling Language

CHAPTER-1
INTRODUCTION

1.1 About Project

The authentication system are security measures put in place to secure data and systems by requiring additional input beyond username and password for user to access the system.

Today's digital world is largely password-protected. Text-based passwords are typically used in password authentication systems. These passwords are vulnerable to a variety of online attacks, including brute-force, shoulder surfing, dictionary attacks, and phishing attacks. Many users, as has been found in numerous studies, have a tendency to forget their passwords, choose weak passwords, or write them down insecurely in an effort to remember them, all of which increase the risk of password compromise. To get around these difficulties, we created a graphical password authentication system that is based on the recalling idea. Insights from many institutions' research support the assumption that graphical passwords might be simpler to remember than conventional alphanumeric ones since the human brain is better at remembering what it sees.

A unique method of user authentication called Graphical Password Authentication (GPA) employs visuals or patterns to confirm the identity of the user. GPA is a sort of graphical password system that has various benefits over conventional alphanumeric passwords, including better memorability, more security, greater accessibility, and a more enjoyable user experience.

Users of GPA systems are frequently required to choose a selection of images or patterns, which they then use as their password. As an illustration, a user might be shown a collection of animal photographs and asked to choose a string of three animals as their password. An alternative is to require a user to choose their password from a grid of photos by clicking on a specified combination of images in a specific order. GPA passwords may be more safe than conventional alphanumeric passwords because there are so many options for picture selection.

GPA has a number of benefits, one of which is that it may be simpler to remember than alphanumeric passwords. Humans are better at memorising pictures than they are at remembering long strings of letters and numbers, which can be especially useful for users who have trouble managing their passwords. As a result, there may be fewer occurrences of password forgetfulness and requests for password resets.

Additionally, GPA may be safer than conventional passwords. Short and frequently guessable alphanumeric passwords are vulnerable to brute force assaults. In contrast, graphical passwords have a wider range of potential characters and can be more complicated, making them more challenging to decipher.

GPA can also provide a more interesting user experience. Users may be more engaged with an authentication system that uses intriguing visuals or patterns than one that simply asks them for their password, which can improve user happiness and lessen irritation with the authentication process.

As a viable replacement for conventional alphanumeric passwords, GPA has a number of advantages over conventional password systems. GPA may gain popularity as technology progresses as an authentication mechanism for both individuals and organisations looking to enhance their user authentication procedures.

1.1 PROJECT OBJECTIVE

Developing a secure authentication method: One of the primary objectives of a graphical password authentication system project is to develop a secure authentication method that is less vulnerable to attacks than traditional text-based passwords. This involves designing a system that can resist various types of attacks, such as brute force attacks, dictionary attacks, and shoulder surfing attacks.

Enhancing user experience: Another objective of a graphical password authentication system project is to enhance the user experience by providing a user-friendly and intuitive interface. The system should be easy to use and navigate, and users should be able to create and remember their graphical passwords with ease.

Integrating with existing systems: A graphical password authentication system may need to be integrated with existing systems and applications, such as databases, operating systems, and other software. The project objective could include developing an integration plan that ensures the system can communicate with other systems seamlessly.

Providing customization options: The project objective could also include providing customization options to users, such as the ability to choose from different types of images, colors, and patterns to create their password. This can increase user engagement and satisfaction.

CHAPTER-2
SOFTWARE & HARDWARE REQUIREMENTS

4.1 INTRODUCTION

To install and use the application efficiently, we required certain software and hardware components of the computer system. The system requirements on the package will be listed by the application manufacturer. After installation of the application, you could face technical issues, if your computer system does not meet the system requirements. System requirements for operating system will be hardware components, while other application software will list both hardware and operating system requirements and Brower. System requirements are most commonly seen listed as a minimum and recommended requirement. The minimum system requirements need to be met for the web application to run at all on your system, & the recommended system requirements, if met, will offer better software usability.

4.2 SOFTWARE REQUIREMENTS

Required software to work on this project:

- **Operating System:** Windows ,mac ,Linux
- **Languages** :
  - JAVA 19
- **Database Management System** :
  - MySQL 8.0
- **Tools:**
  - NetBeans 17

4.3 HARDWARE REQUIREMENTS

- **Hard Disk :** 80 GB
- **RAM :** at least 128 MB
- **Disc Space :** At least 128 MB for JRE and 2 MB for java updates.
- **Monitor :** LCD Color
- **Processor :** Minimum Pentium 2 266 MHz
- Hard Disk and SSD

CHAPTER-3
PROBLEM DESCRIPTION

Considering the traditional username-password authentication, there are several problems associated with traditional alphanumeric passwords that make them less than ideal for user authentication. One of the main problems is that they can be difficult to remember, especially if users are required to create complex passwords that include uppercase and lowercase letters, numbers, and special characters. As a result, many users resort to using the same password across multiple accounts or writing down their passwords, which can compromise their security.

Another problem with traditional passwords is that they can be easily guessed or cracked by attackers using brute force methods or social engineering techniques. Attackers can use information that they have obtained about a user, such as their name or date of birth, to try to guess their password. Alternatively, they can use sophisticated software tools to crack passwords by systematically testing different combinations of characters until they find the correct one.

In addition to these security concerns, traditional passwords can be challenging for users with disabilities. Users who have visual or motor impairments may find it difficult to read or type alphanumeric characters, which can make it more difficult for them to access their accounts.

Graphical password authentication offers several advantages over traditional alphanumeric passwords. One of the main advantages is that graphical passwords can be easier to remember than alphanumeric passwords. Humans are better at remembering images than they are at remembering strings of characters, which can make graphical passwords more memorable and less prone to being forgotten.

Another advantage of graphical passwords is that they can be more secure than traditional passwords. Graphical passwords can be more complex and can include a larger set of possible characters, which makes them more difficult to guess or crack. Additionally, the use of images or patterns as passwords can make it more difficult for attackers to determine the correct password.

Finally, graphical passwords can be more accessible for users with disabilities. Graphical passwords can be accessed using visual or touch-based interfaces, which can make them more inclusive and easier for users with disabilities to access their accounts.

In conclusion, while traditional alphanumeric passwords have been the standard for many years, they have several problems associated with them that make them less than ideal for user authentication. Graphical password authentication offers several advantages over traditional passwords, including improved memorability, increased security, greater accessibility, and a more engaging user experience. As such, it may be a valuable alternative for organizations seeking to improve their user authentication processes.

CHAPTER-4
LITERATURE SURVEY

Graphical password authentication systems have been the subject of much research in recent years, with numerous studies examining various aspects of these systems, including their usability, security, and effectiveness. Here is a brief literature survey of some of the key studies in this area:

1. "A Comparative Study of Graphical Password Techniques" by K. N. Murthy et al. This study compares several different graphical password techniques, including image-based, gesture-based, and recognition-based approaches. The authors evaluate the usability and security of each approach and conclude that image-based approaches are the most effective.
2. "A Comprehensive Study of Graphical Passwords" by M. Mondal et al. This study provides an overview of graphical password authentication systems and examines their advantages and disadvantages. The authors also review several different graphical password techniques and evaluate their effectiveness in terms of security and usability.
3. "A Usability Study of Three Graphical Password Systems" by R. Biddle et al. This study examines the usability of three different graphical password systems and compares them to traditional alphanumeric passwords. The authors find that the graphical password systems are generally easier to use and more memorable than alphanumeric passwords.
4. "Authentication Using Multiple Choice Questions: An Alternative to Graphical Passwords" by M. Al-Rubaiee et al. This study proposes an alternative authentication system based on multiple-choice questions, which is designed to be more secure and easier to use than graphical password systems.
5. "Security and Usability of Graphical Passwords for Mobile Devices: A Review" by H. M. Abbas et al. This study reviews the state of the art in graphical password authentication for mobile devices and evaluates the security and usability of several different techniques. The authors conclude that graphical passwords are a promising approach to authentication on mobile devices but that more research is needed to improve their security.

These studies, along with many others, demonstrate the ongoing interest in graphical password authentication systems and the importance of further research in this area. As the use of technology continues to expand, it is likely that graphical password systems will become increasingly important for protecting user data and ensuring secure access to online resources.

- **Usability and user acceptance:** Several studies have investigated the usability and user acceptance of graphical password authentication systems. Research has shown that users generally find graphical passwords easier to remember and more enjoyable to use than text-based passwords. However, some studies have identified usability issues related to the complexity of the password creation process, the need for training, and the time required to enter passwords.

- **Security:** Graphical passwords have been shown to be more resistant to brute force attacks than text-based passwords. However, some studies have shown that graphical passwords are vulnerable to shoulder surfing attacks, where an attacker can observe the password being entered. To address this issue, researchers have proposed various solutions, such as using cued-recall graphical passwords, where users are asked to recall specific aspects of the image rather than the entire image.

- **Compatibility and implementation:** Researchers have also investigated the compatibility and implementation of graphical password authentication systems on different devices and platforms. Some studies have identified issues related to the size and resolution of the images, compatibility with touchscreens and mobile devices, and the need for additional hardware or software.

- **Performance comparison:** Several studies have compared the performance of graphical password authentication systems with traditional text-based password systems. Some studies have shown that graphical passwords can be more secure and easier to remember than text-based passwords, while others have found no significant difference between the two systems.

Overall, the literature suggests that graphical password authentication systems have the potential to provide a secure and user-friendly alternative to traditional text-based password systems. However, further research is needed to address the challenges related to usability, security, and implementation, and to develop standards and guidelines for the design and implementation of graphical password authentication systems.

CHAPTER-5
SOFTWARE REQUIREMENT SPECIFICATION

5.1 FUNCTIONAL REQUIREMENTS

- User Registration: The system allows users to register and create their unique graphical passwords by selecting specific images or performing specific actions on images.
- Password Storage: The system should securely store user passwords in a database in the hash form.
- Password Authentication: The system should allow users to authenticate themselves by entering their graphical password on the authentication interface.
- Hashing : password must be stored in its hash code in the data base.
- Password Recovery: The system should provide a mechanism for users to recover their passwords in case they forget them.
- Security Mechanisms: The system should include various security mechanisms, such as E-mail verification.

5.2 NON-FUNCTIONAL REQUIREMENTS

- **Security:** The system should be secure from unauthorized access

- **Compatibility:** The system should be compatible with various hardware and software environments.

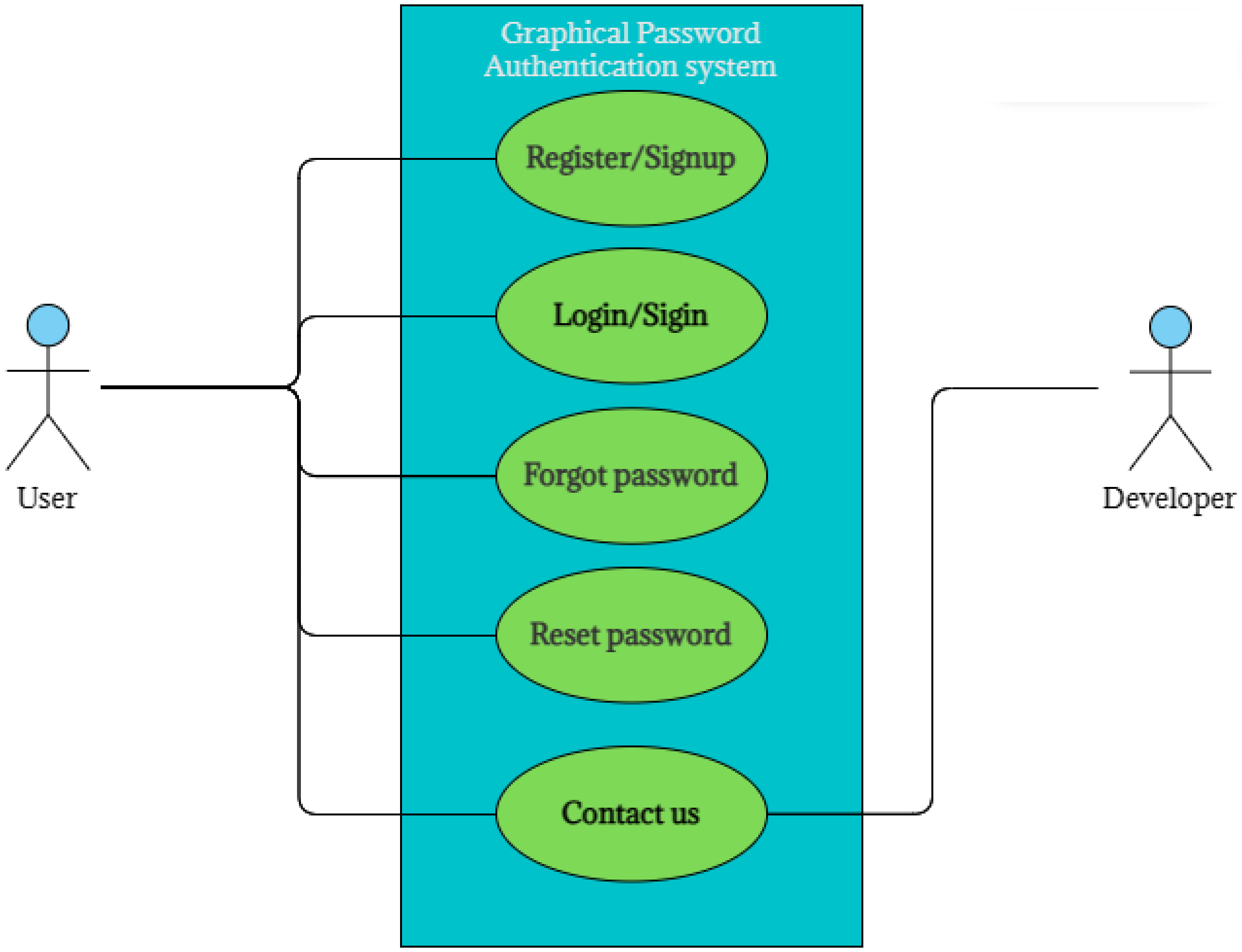
- **Usability:** The system should be easy to use, with a clear and intuitive graphical user interface.

- **Reliability:** The system should be reliable, with minimal errors or system failures.

- **Maintainability:** The system should have simple and clear procedures for upgrades, patches, and maintenance.

CHAPTER-6
SOFTWARE DESGIN

- **USE CASE DIAGRAM**



- **ER Diagram**

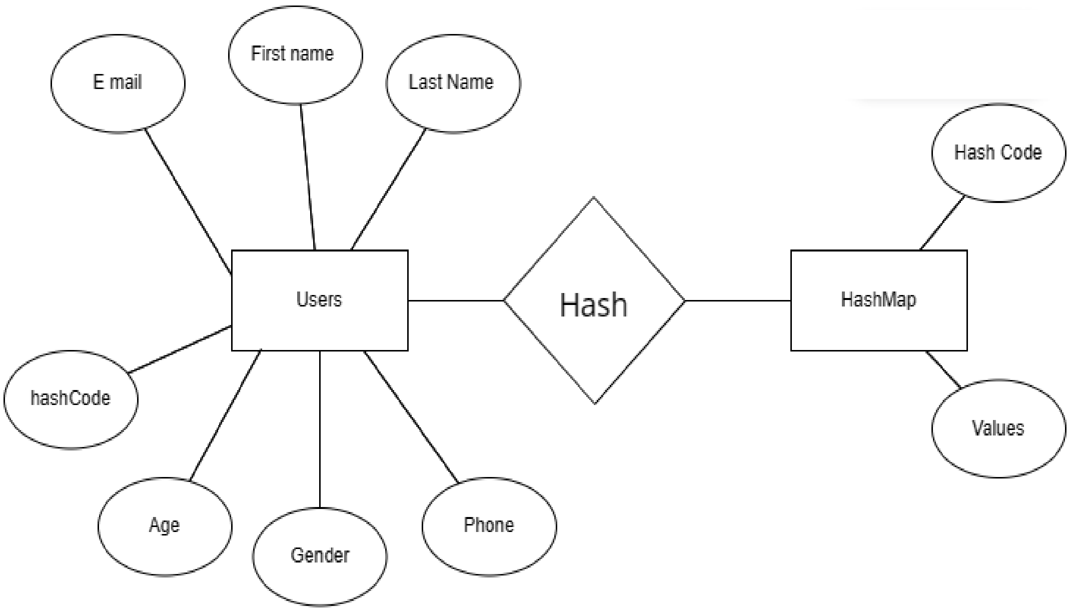


Fig 1.2 ER diagram

- **DATA FLOW DIAGRAM**

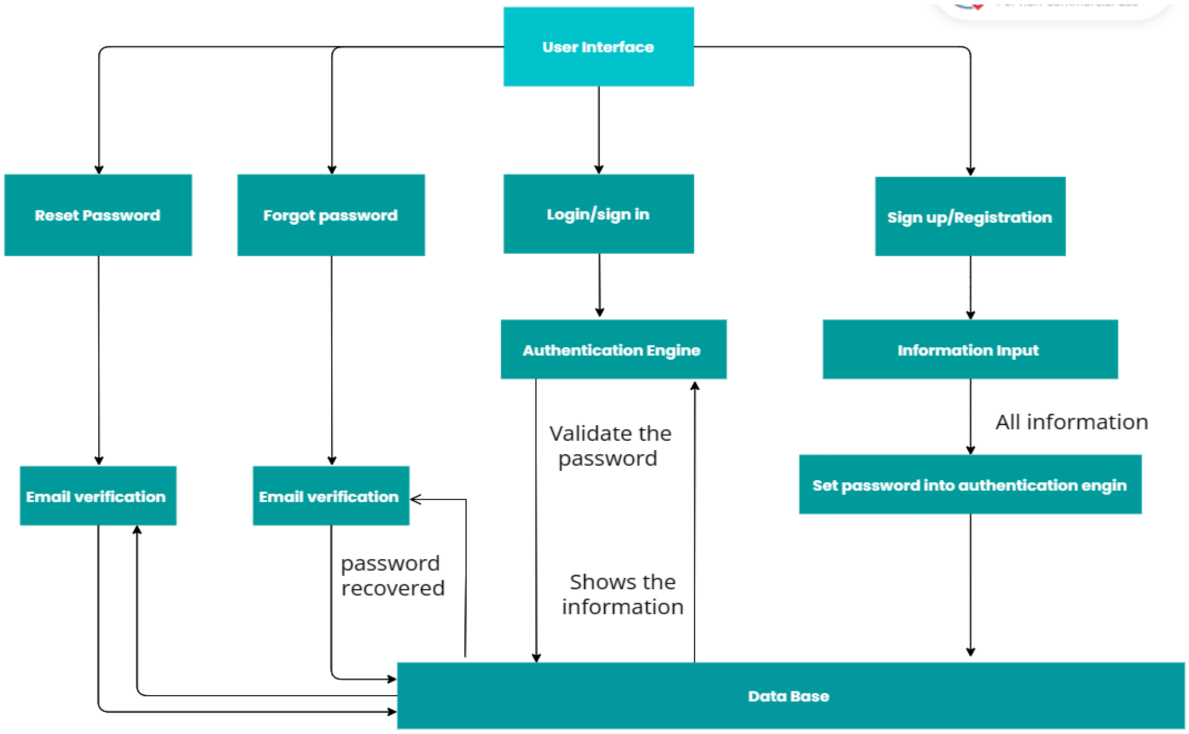
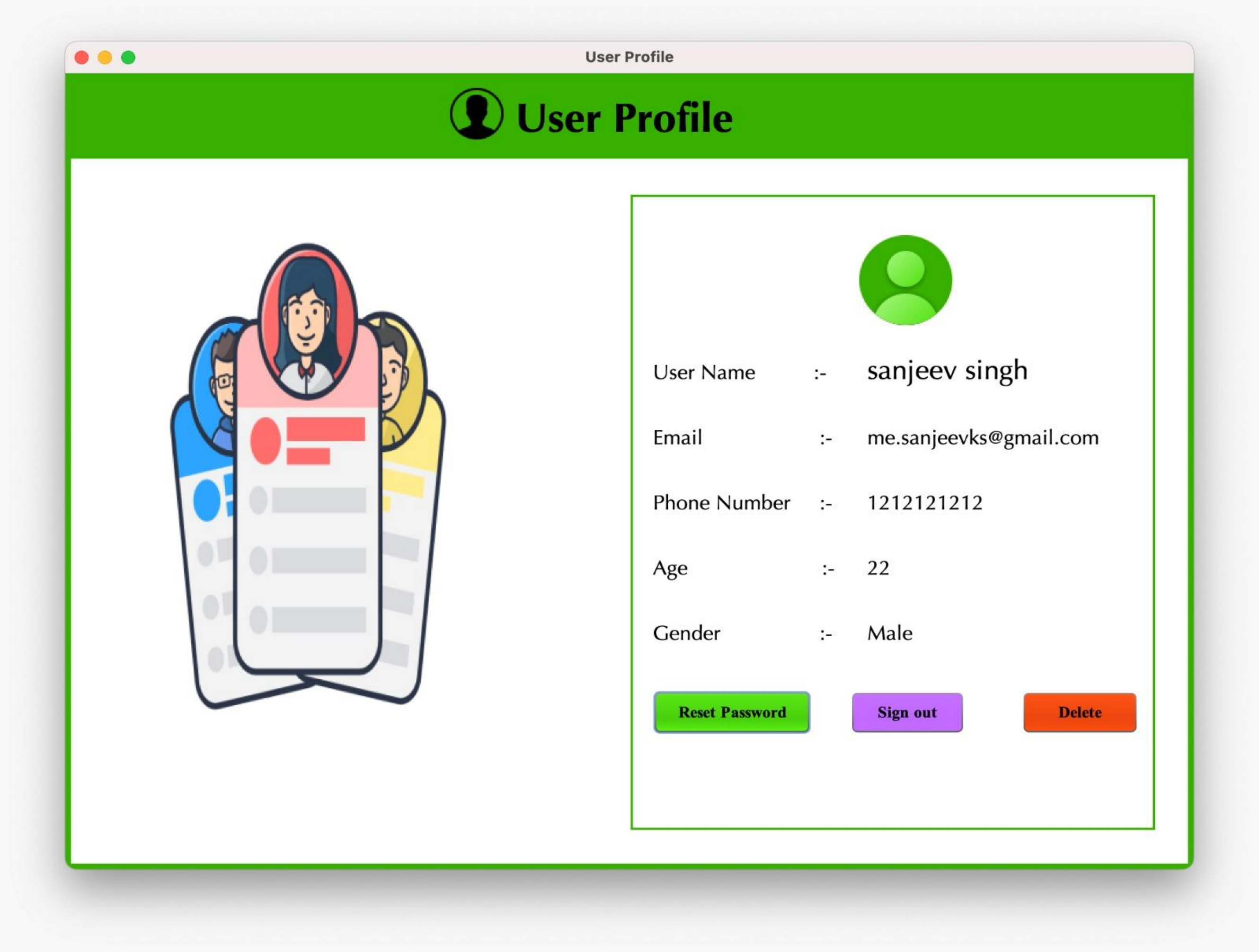


Fig 1.3 Data flow diagram

CHAPTER-7
OUTPUT SCREEN AND WORKING



User Name :- sanjeev singh

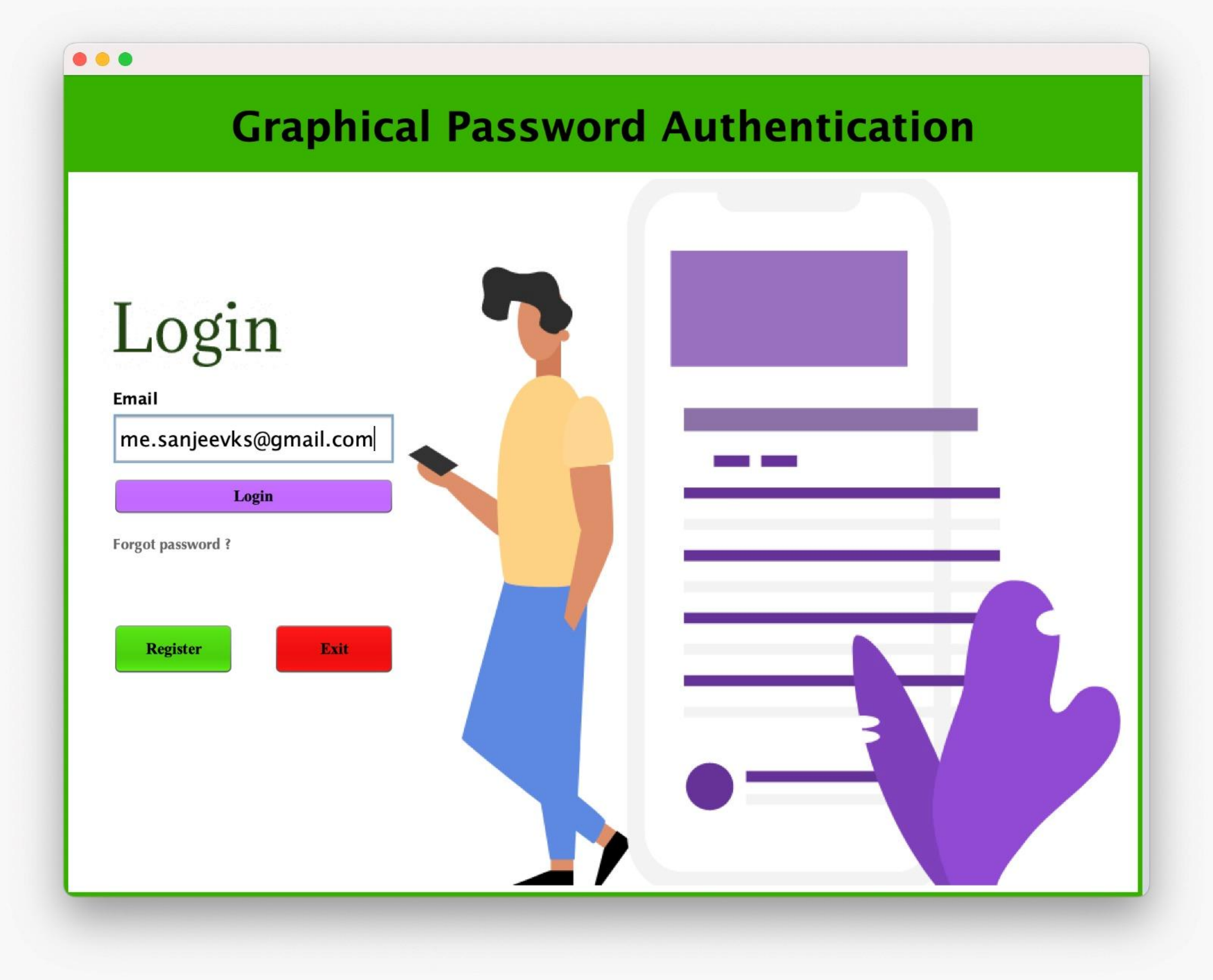
Email :- me.sanjeevks@gmail.com

Phone Number :- 1212121212

Age :- 22

Gender :- Male

Fig 2.1 User profile



Graphical Password Authentication

Login

Email: me.sanjeevks@gmail.com

Fig 2.2 Login page

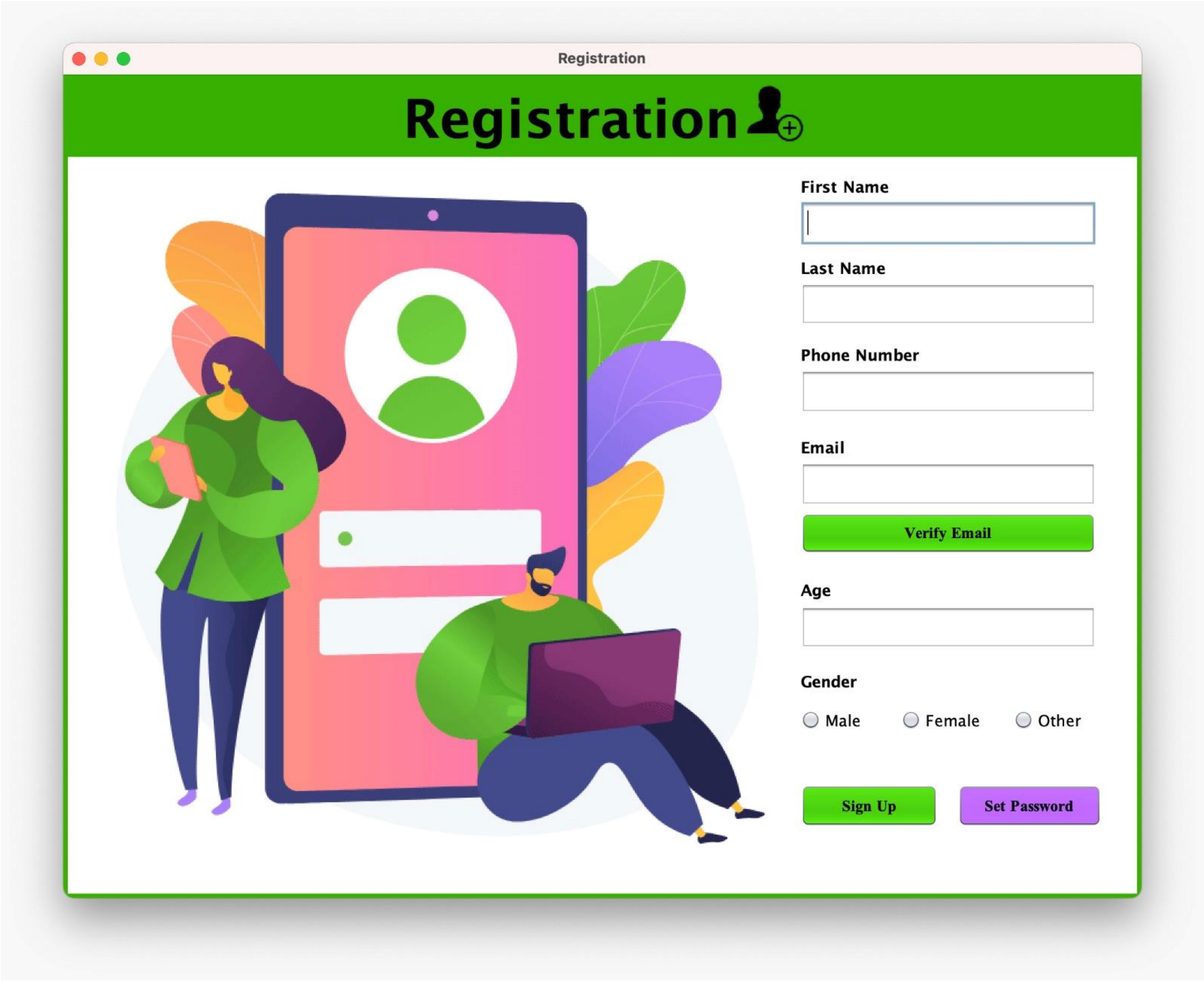


Fig 2.3 Regration page

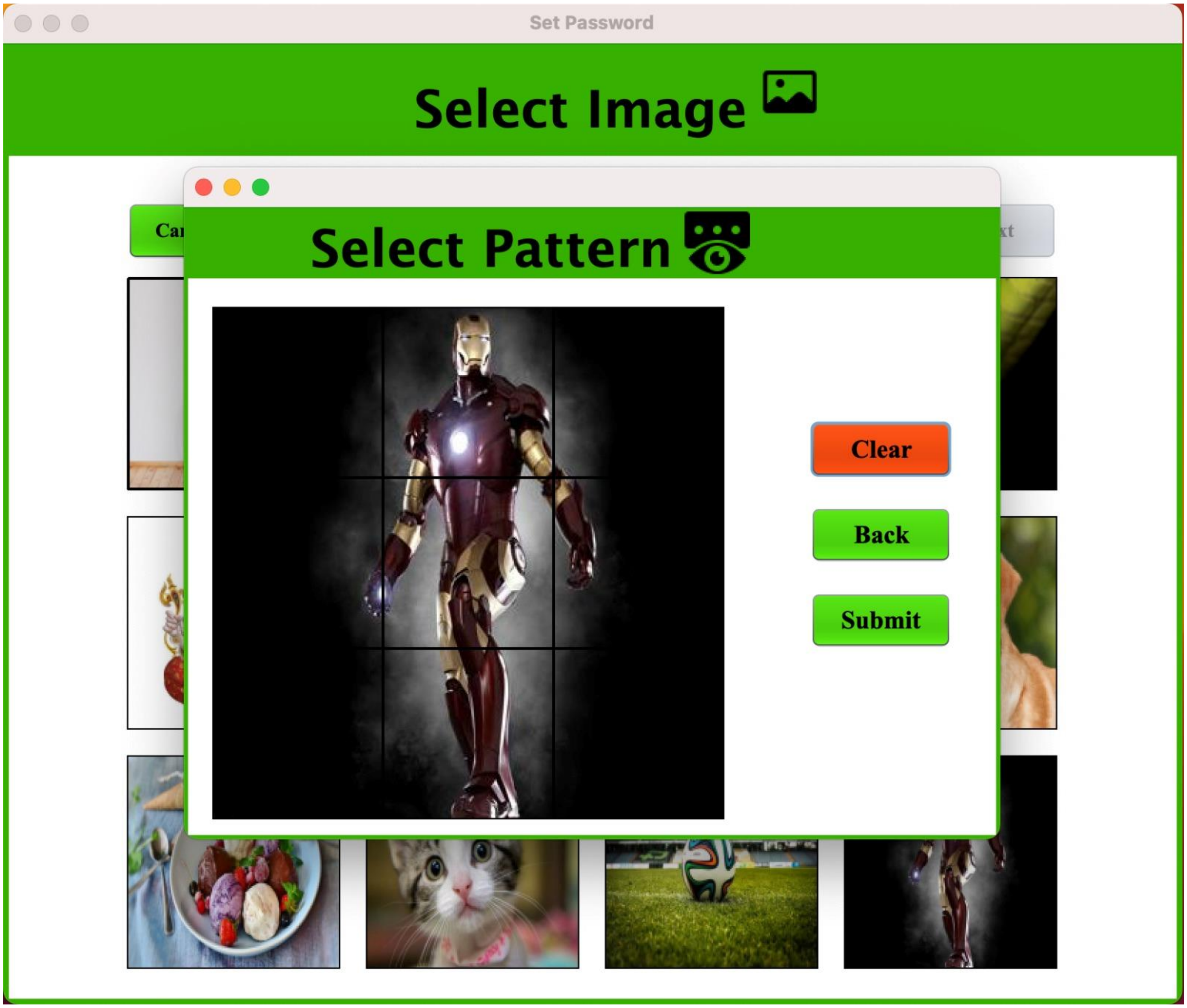


Fig 2.4 Set Password

CHAPTER-8
CONCLUSION AND FUTURE WORK

- Graphical password authentication system is an alternative to traditional alphanumeric passwords.
- where users authenticate themselves by selecting a *sequence of images* and patterns, rather than typing in a sequence of letters, numbers, and symbols.
- The graphical password is easy to remember and hard to crack and it is more resistant to phishing attacks.

REFERENCES

- **https://www.geeksforgeeks.org/graphical-password-authentication/**

- **https://docs.oracle.com/javase/7/docs/api/javax/swing/package-summary.html**

- **https://dev.mysql.com/doc/**

- **https://www.geeksforgeeks.org/send-email-using-java-program/**

- **https://unsplash.com/images/stock**

- **https://stackoverflow.com/questions/884943/how-do-i-send-an-e-mail-in-java**

APPENDIX 1
GLOSSARY OF TERMS

(In alphabetical order)

A

ASD

Agile Software Development. An approach to software development under which requirements and solutions evolve through the collaborative effort of self-organizing and small highly motivated team. It advocates continual improvement and encourages rapid and flexible response to change.

G

GPA

Graphical Password authentication system

F

FR

Functional Requirements. FR are the working characteristics of a product. These are based on how end users will use the product.

M

MVT

The MVT (Model View Template) is a software design pattern. It is a collection of three important components Model View and Template. The Model helps to handle database. It is a data access layer which handles the data.

N

NFR

Non-Functional Requirements. NFRs define system attributes such as security, reliability, performance, maintainability, scalability etc

O

OOP Object Oriented Programming. OOP is a computer programming model that organizes software design around data, or objects, rather than functions and logic.

U

UML

Unified Modelling Language. It is a general-purpose modelling language. It’s not a programming language, it is rather a visual language. UML is linked with object-oriented design and analysis. UML makes the use of elements and forms associations between them to form diagram

PROJECT SUMMARY

About Project

Title of the project	DESIGN AND DEVELOPMENT OF GRAPHICAL PASSWORD AUTHENTICATION SYSTEM
Semester	6th
Members	4
Team Leader	Sanjeev Kumar Singh
Describe role of every member in the project	Sanjeev Kumar Singh :- Sachin Kumar :- Sahil Choudhary :- Vivek Verma :-
What is the motivation for selecting this project?	To make security system robust and remembering projects easy.
Project Type (Desktop Application, Web Application, Mobile App, Web)	Desktop application

Tools &Technologies

Programming language used	Java
IDE used (with version)	Apache Net Beans
Front End Technologies (with version, wherever Applicable)	Java swing
Back End Technologies (with version, wherever applicable)	Java
Database used (with version)	SQL

Software Design& Coding

Is prototype of the software developed?	*Yes*
SDLC model followed (Waterfall, Agile, Spiral etc.)	Agile
Why above SDLC model is followed?	Agile is a SDLC model that defines how software development needs to be done. It’s not a single or specific method, and it is the collection of various methodologies and best practices that follow the value statement signed with the customer
Justify that the SDLC model mentioned above is followed in the project.	Since, we didn’t exactly know all the functionalities or the functionalities were frequently changing, we use Agile model, so that we could make desired changes whenever needed.
Software Design approach followed (Functional or Object Oriented)	
Name the diagrams developed (according to the Design approach followed)	Use Case diagram
In case Object Oriented approach is followed, which of the OOPS principles are covered in design?	
No. of Tiers (example 3-tier)	3-tier
Total no. of front end pages	5
Front end validations applied (Yes / No)	No
Session management done (in case of web applications)	
Is application browser compatible	

(in case of web applications)	
Exception handling done (Yes / No)	No
Commenting done in code (Yes / No)	Yes
Naming convention followed (Yes / No)	Yes
What difficulties faced during deployment of project?	
Total no. of Use-case s	
Give titles of Use-cases	Use-case Diagram

Project Requirements

MVC architecture followed (Yes / No)	
If yes, write the name of MVC architecture followed (MVC-1, MVC-2)	
Design Pattern used (Yes / No)	
If yes, write the name of Design Pattern used	
Interface type (CLI / GUI)	
No. of Actors	
Name of Actors	
Total no. of Functional Requirements	
List few important non-Functional Requirements	Correctness, Flexibility, Reliability and Maintainability.

Testing

Which testing is performed? (Manual or Automation)	Manual

Is Beta testing done for this project?	No

Write project narrative covering above mentioned points

This Graphical Password Authentication system has function to provide extra security to applications . The primary programming language is JAVA. Our front end and backend is built using Java only with NetBeans IDE. It will provide an graphical password interface for password and authentication .

This project is divided into two stages for the whole project :

1.Set password by selecting image patters : In this stage , the user will Select the patterns of images in a sequence and save it as a password.

2.Sava it for authentication : It gets stored in the form of hash in the database , user can get the password in case of forgot password ,via email validation.

Sanjeev Kumar Singh

0187CS201147

Sachin Kumar

0817CS201141

Sahil Choudhary

0187CS201143

Vivek Verma
0187CS201183

Project guide
Prof. Ruchi Jain