

BASIC GRAPHICAL PASSWORD AUTHENTICATION

*An Application Development – I (Project) Report Submitted
In partial fulfillment of the requirement for the award of the degree of*

***Bachelor of Technology
in
Computer Science and Engineering (Cyber Security)***

by

A SAMBA SIVA REDDY

Regd No: 21N31A6202

K SANDEEP KUMAR

Regd No: 21N31A6239

K BHARADWAJ

Regd No: 22N35A6202

Under the Guidance of

Mr. P SREENIVAS

Associate Professor

Department of Emerging Technologies

MRCET (Autonomous Institution, UGC Govt. of India)



**DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
(EMERGING TECHNOLOGIES)**

MALLA REDDY COLLEGE OF ENGINEERING AND TECHNOLOGY

(Autonomous Institution – UGC, Govt. of India)

(Affiliated to JNTU, Hyderabad, Approved by AICTE, Accredited by NBA & NAAC – 'A' Grade, ISO 9001:2015 Certified)

Maisammaguda (v), Near Dullapally, Via: Kompally, Hyderabad – 500 100, Telangana State, India

2023-2024



Estd : 2004

MALLA REDDY COLLEGE OF ENGINEERING & TECHNOLOGY

(Autonomous Institution – UGC, Govt. of India)

(Sponsored by CMR Educational Society)

Recognized under 2(f) and 12 (B) of UGC ACT 1956

(Affiliated to JNTUH, Hyderabad, Approved by AICTE- Accredited by NBA & NAAC– ‘A’ Grade - ISO 9001:2015 Certified)



CERTIFICATE

This is to certify that this is the bonafide record of the project titled “**Basic Graphical Password Authentication**” submitted by **A SAMBA SIVA REDDY** bearing **21N31A6202**, **K SANDEEP KUMAR** bearing **21N31A6239**, **K BHARADWAJ** bearing **22N35A6202** of **B. Tech III Year – I Semester** in the partial fulfillment of the requirements for the degree of **Bachelor of Technology in Computer Science and Engineering (Cyber Security)**, Dept. of CSE (Emerging Technologies) during the year 2023-2024. The results embodied in this project report have not been submitted to any other university or institute for the award of any degree or diploma.

Mr. P Sreenivas
Associate Professor
Department of CSE (ET)

Dr. P Dileep
Project Co Ordinator
Department of CSE (ET)

EXTERNAL EXAMINER

Dr. M V Kamal
Professor &
Head of Department (ET)

DECLARATION

We hereby declare that the project entitled “**Basic Graphical Password Authentication**” submitted to **Malla Reddy College of Engineering and Technology**, affiliated to Jawaharlal Nehru Technological University Hyderabad (JNTUH) as part of III Year B. Tech – I Semester and for the partial fulfillment of the requirement for the award of **Bachelor of Technology in Computer Science and Engineering (Cyber Security)** is a result of original research work done by us.

It is further declared that the project report or any part thereof has not been previously submitted to any University or Institute for the award of degree or diploma.

A SAMBA SIVA REDDY (22N31A6202)

K SANDEEP KUMAR (21N31A6239)

K BHARADWAJ (22N35A6202)

ACKNOWLEDGEMENTS

We feel ourself honored and privileged to place our warm salutation to my college “Malla Reddy College of Engineering and Technology (Autonomous Institution – UGC Govt. of India) and our Principal **Dr. S Srinivasa Rao**, Professor who gave us the opportunity to do the Application Development -1 (Project) during our III Year B. Tech and profound the technical skills.

We express our heartiest thanks to our Director **Dr. V S K Reddy**, Professor for encouraging us in every aspect of our project and helping us realize our full potential.

We also thankful to our Head of the Department **Dr. M V Kamal**, Professor for providing training and guidance, excellent infrastructure and a nice atmosphere for completing this project successfully.

We would like to express our sincere gratitude and indebtedness to our project supervisor **Dr. P Dileep**, Professor for his valuable suggestions and interest throughout the course of this project.

We convey our heartfelt thanks to our Project Coordinator **Mr. P Sreenivas**, Associate Professor for allowing for their regular guidance and constant encouragement during our dissertation work.

We would like to thank all our supporting **staff** of the Department of CSE (Emerging Technologies) and even all other department who have been helpful directly and in-directly in making our project a success.

Finally, we would like to take this opportunity to thank our **families** for their support and blessings for completion of our project that gave us the strength to do our project.

A SAMBA SIVA REDDY
(21N31A6202)
K SANDEEP KUMAR
(21N31A6239)
K BHARADWAJ
(22N35A6202)

TABLE OF CONTENTS

S.No.	Topic	Page No.
	CHAPTER 1: INTRODUCTION -----	1
	1.1: Introduction	
	1.2: Motivation	
	1.3: Problem Definition	
	1.4: Objective of the Project	
	CHAPTER 2: SYSTEM ANALYSIS -----	5
	2.1: Existing system and Proposed System	
	2.2: Functional Requirements (Hardware and Software)	
	CHAPTER 3: SOFTWARE ENVIRONMENT -----	9
	3.1: Software	
	3.2: Modules used in Project	
	CHAPTER 4: SYSTEM DESIGN AND UML DIAGRAM -----	11
	4.1: Dataflow Diagram	
	4.2: Architecture Diagram	
	4.1: UML Diagram	
	CHAPTER 5: SOFTWARE DEVELOPMENT LIFE CYCLE -----	15
	5.1: Phases of SDLC	
	CHAPTER 6: IMPLEMENTATION -----	17
	6.1 Source Code	
	CHAPTER 7: TESTING -----	19
	7.1: Introduction	
	7.2: Sample Test cases	

CHAPTER 8: OUTPUT SCREEN -----	23
8.1: Screenshots	
CHAPTER 9: CONCLUSION AND FUTURE SCOPE -----	25
9.1: Conclusion	
9.2: Future Scope	
CHAPTER 10: REFERENCES -----	27
10.1: Websites	
10.2: Books	
10.3: Research Papers	

ABSTRACT

Graphical password authentication has emerged as a promising alternative to traditional text-based methods due to its potential for enhanced security and usability. This paper presents an overview and analysis of basic graphical password authentication systems.

The study reviews the fundamental concepts, types, and characteristics of graphical passwords, focusing on their design principles and usability aspects. Various basic graphical password schemes such as recognition-based, recall-based, and hybrid approaches are examined, highlighting their strengths, weaknesses, and security implications.

The research explores the underlying psychological and cognitive factors influencing the effectiveness of graphical passwords, discussing the importance of user-generated images, memorability, and resistance against different types of attacks. Furthermore, the paper discusses usability challenges, including the balance between security and user experience, the impact of image selection on usability, and accessibility concerns for diverse user groups.

In addition, the study evaluates the resilience of basic graphical password systems against common attacks such as shoulder surfing, brute-force attacks, and various forms of guessing attacks. It also examines the potential vulnerabilities arising from the inherent characteristics of human memory and perception in graphical password creation and authentication.

Finally, the paper concludes with a summary of the key findings, emphasizing the importance of considering both security and usability in the design and implementation of basic graphical password authentication systems. The research underscores the need for further advancements and research efforts to address the challenges and enhance the overall effectiveness of graphical password schemes in modern cybersecurity paradigms.

LIST OF FIGURES

S.No	Figure Title	Page No
1	Dataflow diagram	11
2	Architecture Diagram	12
3	Use Case Diagram	13
4	Sequential Diagram	14
5	Seven Stages of SDLC	15
6	Sample Code 1	17
7	Sample Code 2	17
8	Sample Code 3	18
9	Sample Code 4	18
10	Sample Test 1	22
11	Sample Test 2	22
12	Output Screen 1	23
13	Output Screen 2	23
14	Output Screen 3	24
15	Output Screen 4	24

LIST OF TABLES

S.No	Table name	Page No
1	Requirements	8
2	Modules	10

CHAPTER 1

INRODUCTION

1.1 INTRODUCTION

In the realm of computer security, the human element stands as a pivotal vulnerability in safeguarding sensitive information. Human computer interaction plays a crucial role across three critical domains: authentication, security operations, and the construction of secure systems. Among these, authentication emerges as a primary concern, often plagued by the complexities of password management.

The challenge is clear: intricate passwords, while theoretically robust, pose a practical hurdle in memorization. Studies reveal a troubling trend—users resort to jotting down passwords or reusing them across multiple accounts due to the limitations of human memory. This practice introduces vulnerabilities, undermining the very purpose of password security.

While biometric methods have surfaced as an alternative to conventional username-password authentication, our focus shifts toward a distinct approach: the utilization of images as passwords. This alternative avenue offers a promising solution to the memorability conundrum, potentially reshaping the landscape of authentication methods.

By leveraging images as authentication elements, we aim to explore a novel avenue that not only addresses the memorization challenges but also enhances the user experience in safeguarding sensitive data. This investigation delves into the realm of graphical passwords, probing their efficacy, security implications, and the intricate interplay between human cognition and digital authentication systems. Through this exploration, we seek to uncover the potentials and limitations of utilizing images as keys to unlock secure digital spaces.

1.2 MOTIVATION

"In the ever-evolving landscape of cybersecurity, the need for robust yet user-friendly authentication methods have become increasingly evident. Traditional text-based passwords, while pervasive, are plagued by inherent vulnerabilities stemming from human limitations in creating and managing complex passwords. This predicament has given rise to a pressing need for innovative, secure, and user-centric authentication systems.

The motivation behind developing the Image-Based Sequential Authentication System stems from a pursuit to revolutionize authentication paradigms. By harnessing the power of visual memory, this system offers a compelling alternative to conventional password methods. It aims to empower users with a more intuitive and potentially more secure means of safeguarding their accounts.

This approach aligns with the fundamental goal of bridging the gap between security and usability. It seeks to alleviate the burden of memorization while fortifying digital defenses against prevalent cyber threats. The system's reliance on image sequences as passwords not only enhances security but also aims to enhance user experience through familiarity and ease of use.

The motivation lies in providing users with an authentication solution that is both effective in protecting sensitive information and intuitive in its approach. By fostering a system that leverages images as keys to access digital spaces, we strive to redefine the way users interact with security measures, ultimately contributing to a safer and more user-friendly digital landscape

1.2 PROBLEM DEFINATION

The challenge lies in creating an authentication system that effectively balances security and usability, recognizing the inherent limitations of human memory in managing complex passwords. Traditional text-based password systems often compel users to create intricate passwords, leading to issues of forgetfulness, password reuse, or the practice of noting down passwords, all of which compromise security. This dilemma necessitates the exploration of alternative authentication techniques that can alleviate the memorization burden while upholding robust security standards. The problem at hand is to develop and evaluate an image-based authentication system that ensures both strong security measures and user-friendly interaction, mitigating the vulnerabilities associated with conventional password-based methods.

In the landscape of digital security, the persistent challenge of user authentication remains a focal point due to the vulnerabilities associated with traditional password-based systems. The inherent weaknesses in password-based authentication, such as password reuse, forgetfulness, and susceptibility to hacking, call for innovative and secure alternatives.

Users face a dilemma with conventional authentication methods, often resorting to weak passwords, writing them down, or reusing them across multiple accounts due to the limitations of memory. These practices expose individuals and organizations to heightened security risks, leading to potential data breaches and compromised user accounts.

Addressing this challenge necessitates the development of an advanced, user-centric authentication system that not only heightens security but also enhances user experience and usability. An Image-Based Sequential Authentication System emerges as a promising solution, leveraging visual memory and familiarity with images to offer a more intuitive and secure method of user authentication.

1.4 OBJECTIVE OF THE PROJECT

Enhanced Security: Develop a system that strengthens security measures by utilizing image-based authentication to mitigate common password-related vulnerabilities such as weak passwords, reuse, and easy-to-guess credentials.

Improved User Experience: Create a user-friendly authentication method that leverages visual memory, making it more intuitive and potentially easier to remember than traditional text-based passwords.

Reduced Password-Related Risks: Address the challenges associated with password management, aiming to minimize instances of forgotten passwords, writing down credentials, or reusing the same password across multiple accounts.

Usability and Accessibility: Design an authentication system accessible to diverse user demographics by providing a simple and intuitive interface for image selection without compromising security.

Reliable Authentication: Implement a robust system that accurately verifies user identity through the correct reproduction of the pre-selected sequence of images during login, ensuring secure access to accounts.

Adaptability and Scalability: Construct a system that can adapt to evolving security threats and user preferences, while also accommodating a growing user base without compromising performance or security.

Future Expansion: Lay the groundwork for potential future enhancements, such as integrating machine learning algorithms, biometric authentication, or multi-factor authentication methods, to further strengthen security measures and user convenience.

CHAPTER 2

SYSTEM ANALYSIS

2.1 EXISTING SYSTEM AND PROPOSED SYSTEM

Existing System

The existing systems for basic graphical password authentication primarily revolve around recognition-based and recall-based schemes.

Image-Based Authentication: Users select or upload an image and then designate specific points or regions within the image as their password. To log in, they must recreate the same selections.

Picture-Based Authentication with Passphrases: Users choose a picture or set of pictures and associate them with a passphrase or a sequence of interactions (e.g., tapping or drawing on specific areas of the image).

Visual Cryptography: This method involves splitting an image into multiple parts, and users need a specific combination of these parts to authenticate themselves.

Proposed System

The proposed system leverages image-based authentication in a sequential order, aiming to provide a balance between security and user-friendliness. Through this approach, the system seeks to offer an innovative and potentially more secure alternative to traditional text-based passwords.

Image Selection for Password Creation:

- Instead of traditional text-based passwords, the user selects a sequence of images from a provided set. This sequence of chosen images will serve as the user's password.

Login Authentication Process:

- Upon login, the user inputs their email-id as identification.
- The user must then select the same sequence of images in the same order as chosen during the signup process.
- If the user correctly reproduces the predetermined sequence of images, access to the account is granted. Otherwise, login is denied.

Authentication Failure Handling:

- In case of an incorrect sequence of selected images, the system prompts the user to retry the image selection process.
- After a predefined number of failed attempts, additional security measures, such as a secondary authentication method or a temporary account lockout, may be enforced to prevent unauthorized access.

Security Measures:

- The system encrypts and securely stores the user's chosen image sequence, ensuring the confidentiality of the authentication data.
- To mitigate potential attacks, the system can incorporate measures to prevent brute-force attempts or pattern analysis.

User Experience and Usability:

- The image-based authentication system aims to improve user experience by providing a more intuitive and potentially memorable method of authentication.
- A diverse set of images should be provided to enhance security while ensuring that users can easily recognize and recall their chosen sequence.

User Registration:

- During signup, the user provides basic details such as name and email-id.

Continuous Improvement:

- Regular assessments and user feedback should guide the evolution of the image selection process, optimizing it for both security and usability.
- Implementing machine learning or behavioral analysis may help refine the system to adapt to user preferences and improve the authentication process.

2.2 FUNCTIONAL REQUIREMENTS (HARDWAER AND SOFTWARE)

Software Requirements

HTML: HTML, or Hyper Text Markup Language, is the standard language used to create and structure web pages. It forms the backbone of web content, defining the layout and appearance of a webpage's elements.

CSS: CSS, or Cascading Style Sheets, is a styling language used alongside HTML to define the presentation and layout of web pages. It enables the customization of the appearance of HTML elements, controlling aspects like colors, fonts, spacing, positioning, and more.

JavaScript: JavaScript is a versatile programming language primarily used for web development. It enables the creation of dynamic and interactive web pages by adding behavior and interactivity to HTML and CSS.

Hardware requirements

Monitor or Screen: monitor is the user's primary visual interface, facilitating their interaction with the authentication system by presenting prompts, images and instructions throughout the authentication process.

Mouse or Touchpad: Necessary for users to interact with the graphical interface for image selection during authentication.

Processor: Capable processor for handling database queries and transactions.

Memory (RAM): Sizable memory for optimal database performance and quick access to data.

Requirements	Used for
<i>HTML</i>	<i>Creating the structure of WEBSITE</i>
<i>CSS</i>	<i>Styling of the WEBSITE</i>
<i>JavaScript</i>	<i>Create a Interactive WEBSITE</i>
<i>Monitor or Screen</i>	<i>A Visual interface to interact with WEBSITE</i>
<i>Mouse or Touchpad</i>	<i>For Interacting with the WEBSITE</i>
<i>Processor</i>	<i>For handling the Transactions in the WEBSITE</i>
<i>Memory (RAM)</i>	<i>For Database</i>

Table 1 Requirements

CHAPTER 3

SOFTWARE ENVIRONMENT

3.1 SOFTWARE

Visual Studio: Visual Studio is a robust Integrated Development Environment (IDE) developed by Microsoft, widely used for various types of software development, including web applications, desktop applications, mobile apps, cloud-based services, and more.

Code Editor: Visual Studio provides a powerful code editor with features like syntax highlighting, IntelliSense (code completion), code refactoring, and debugging capabilities.

Testing Environment: It includes integrated testing frameworks for unit testing, performance testing, and code coverage analysis, ensuring code quality and functionality.

3.2 MODULES USED IN THE PROJECT

User Registration Module:

User Information Input: Allows users to enter their basic details (name, email-id) during signup.

Image Selection Interface: Provides a platform for users to choose a sequence of images to create their password.

Authentication Module:

Email-id Verification: Verifies user identification through matching of both email's given at the time of sign up and sign in.

Image-Based Login Interface: Presents the interface for users to input the predetermined sequence of images for authentication.

Authentication Failure Handling Module:

Retry Mechanism: Allows users to retry image selection in case of an incorrect sequence input.

MODULES	USES
<i>User Registration Module</i>	<i>This module is used for registering the user i.e creating the account.</i>
<i>Authentication Module</i>	<i>This module is used for user to log in into their account.</i>
<i>Authentication Failure Handling Module</i>	<i>This module is used if the user enters wrong credentials while logging in.</i>

Table 2 Modules

CHAPTER 4

SYSTEM DESIGN AND UML DIAGRAMS

4.1 DATAFLOW DIAGRAM

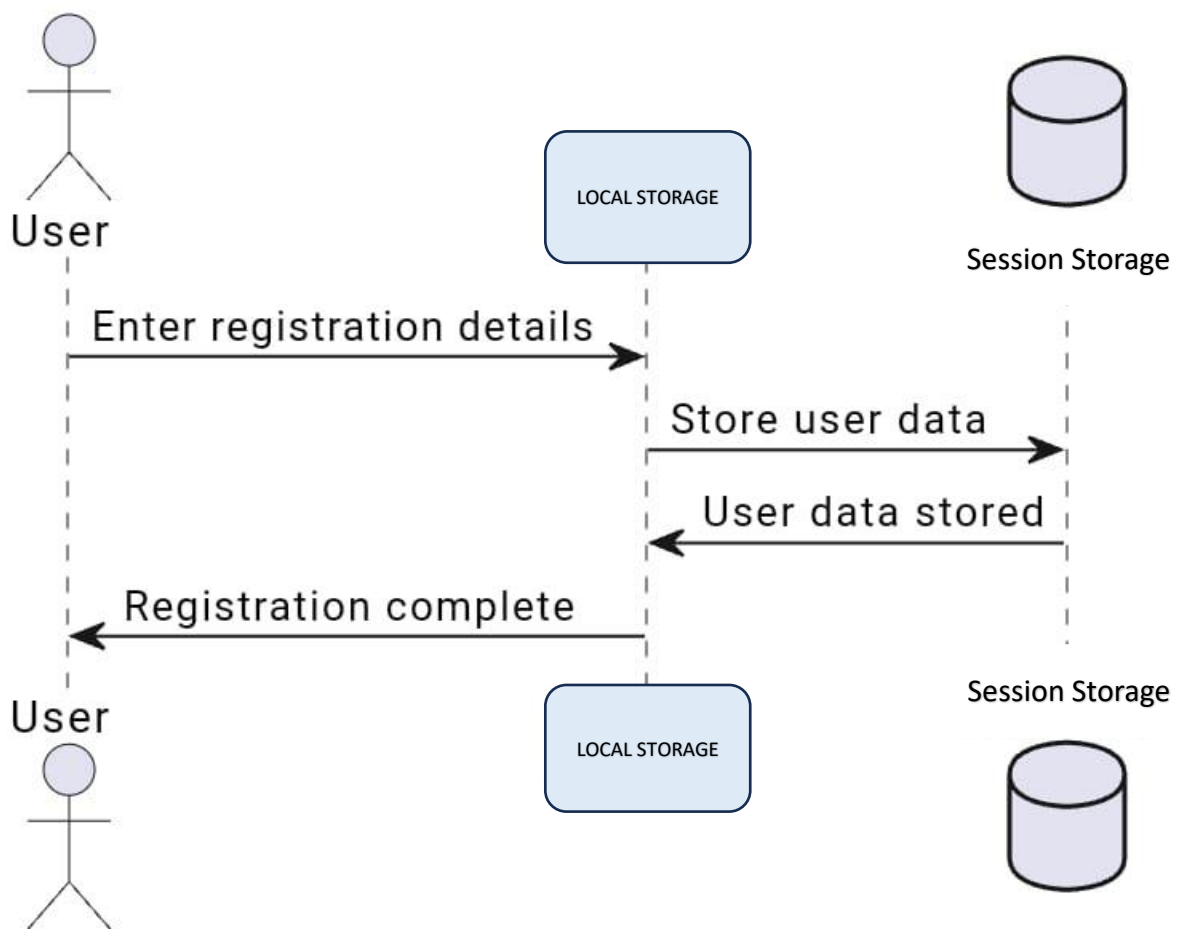


Fig 1 Data Flow Diagram

4.2 ARCHITECTURE DIAGRAM

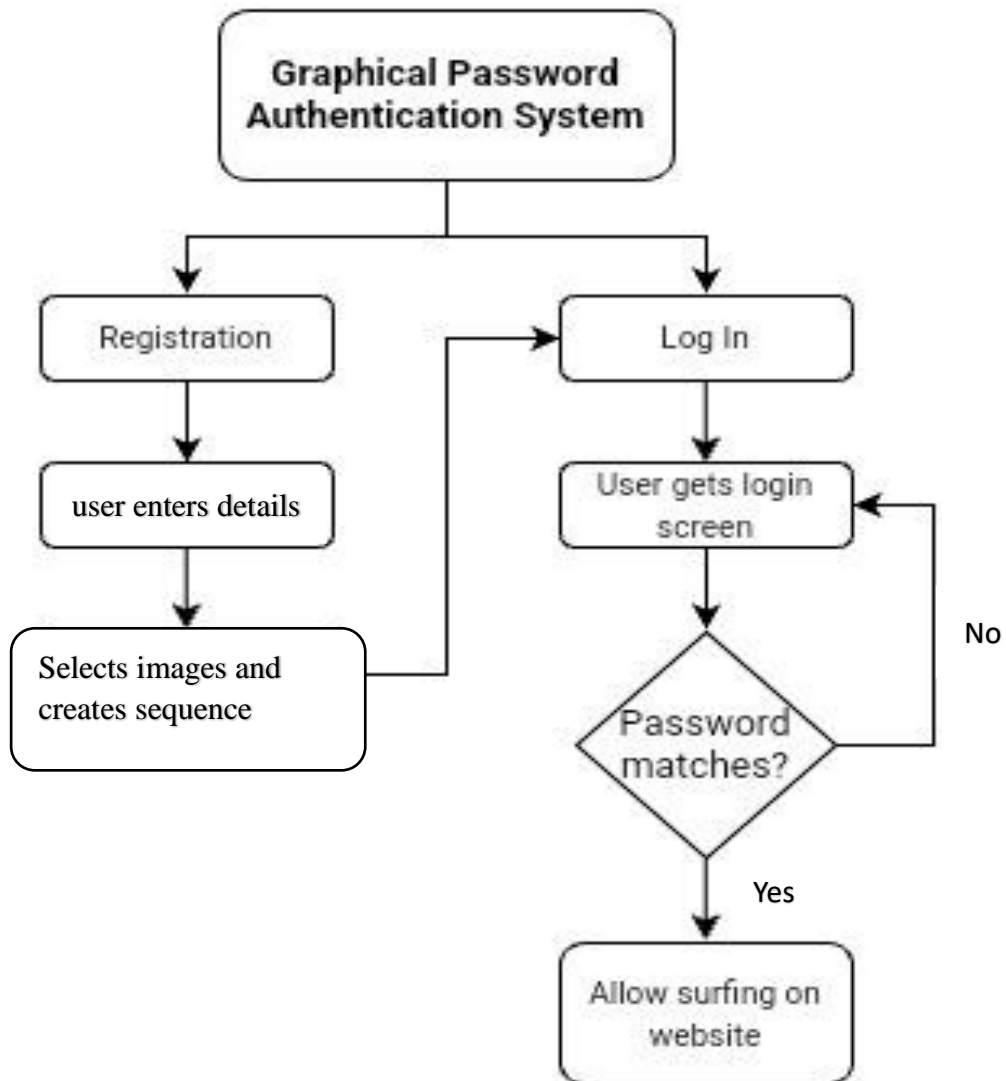


Fig 2 System Architecture

4.3 UML DIAGRAMS

Use Case Diagram:

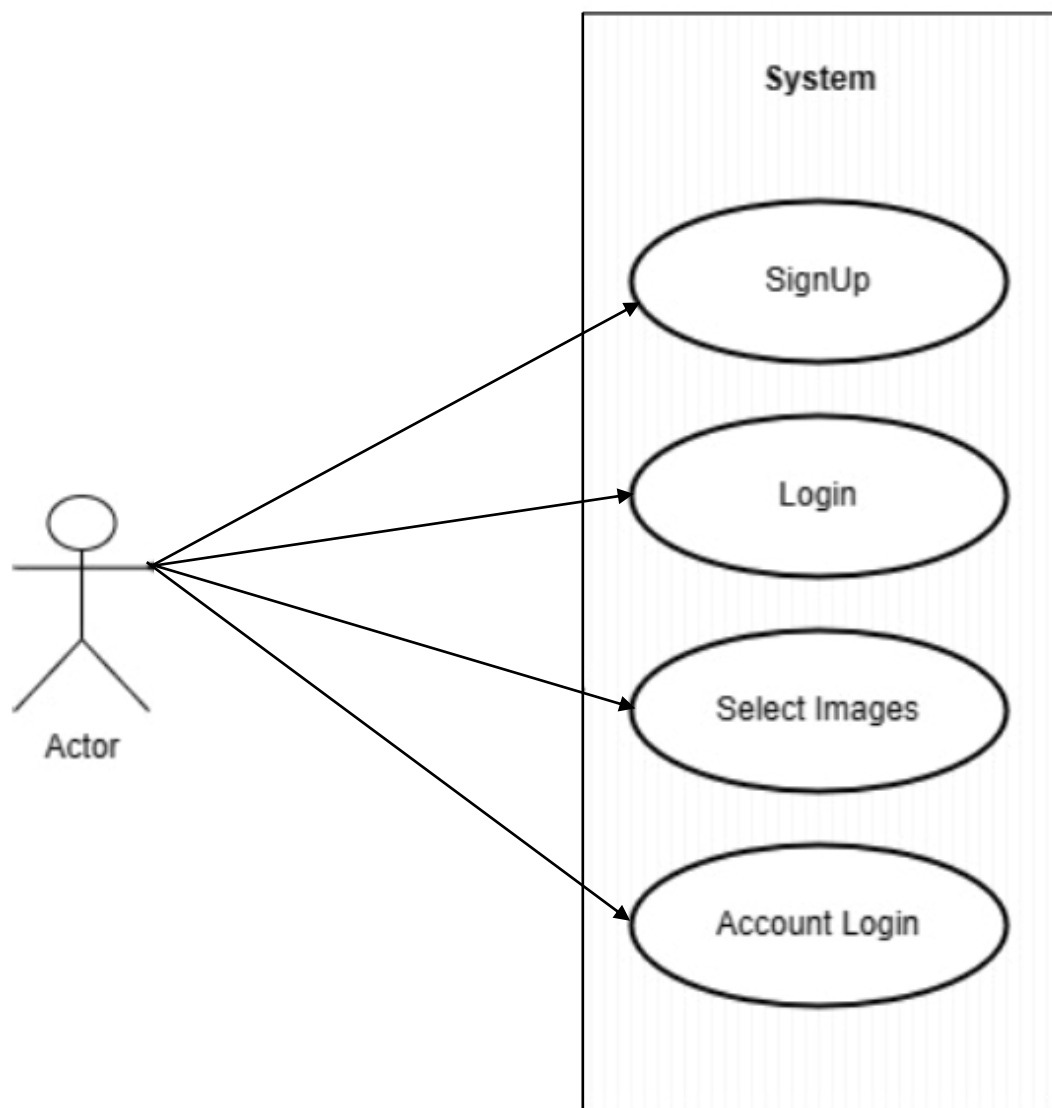


Fig 3 Use Case Diagram

Sequential Diagram:

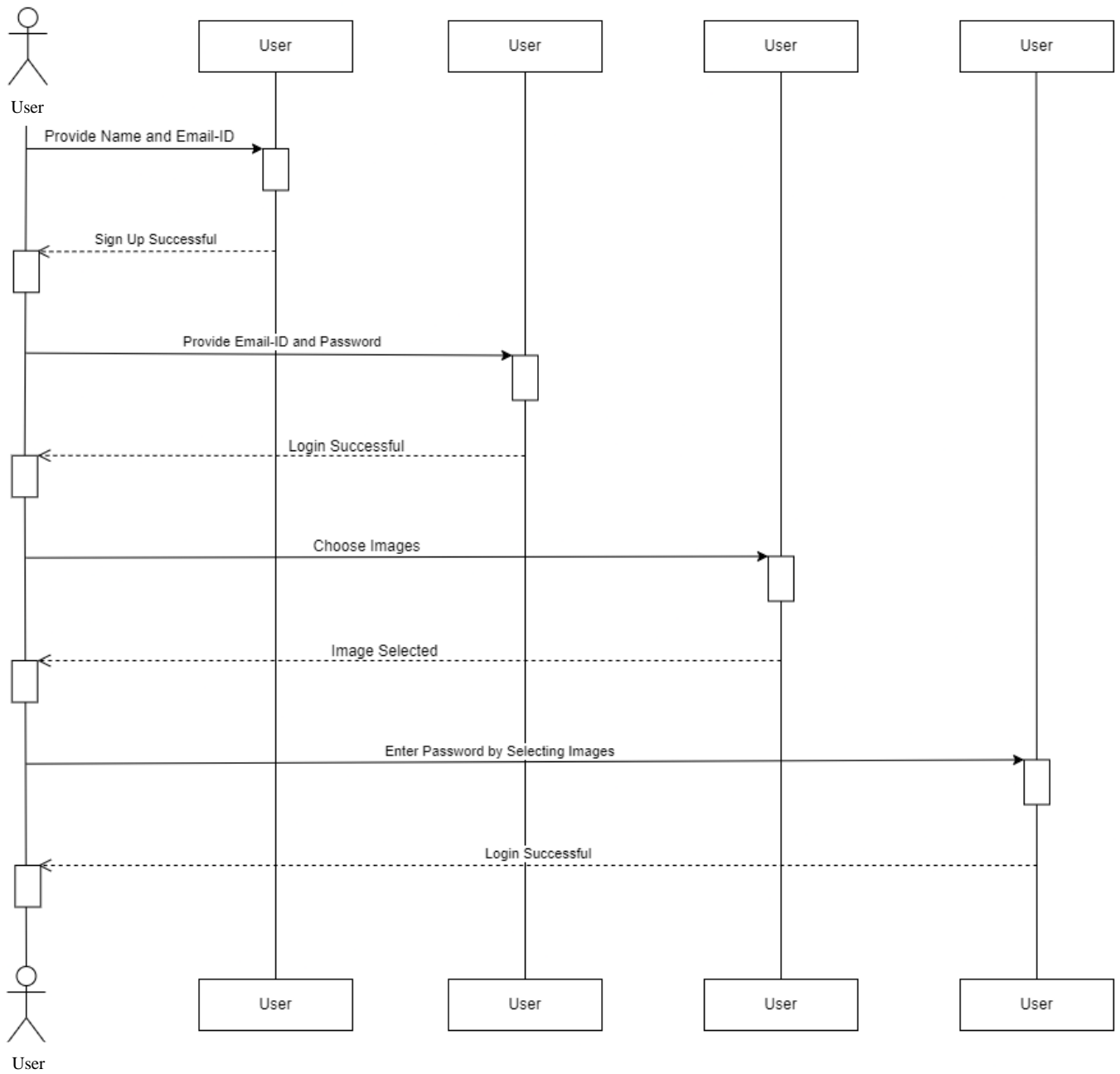


Fig 4 Sequential Diagram

CHAPTER 5

SOFTWARE DEVELOPMENT LIFE CYCLE

5.1 PHASES OF SDLC



Fig 5 Seven Stages of SDLC

The Software Development Life Cycle (SDLC) comprises several distinct phases that guide the development of software applications from conception to deployment and maintenance. The common phases of SDLC include:

Planning: Involves establishing project goals, requirements gathering, feasibility analysis, and creating a project plan. It outlines the scope, objectives, timelines, and resource allocation.

Analysis: In-depth analysis of requirements gathered in the planning phase. This involves understanding user needs, defining system features, and creating detailed specifications.

Design: Based on the gathered requirements and analysis, this phase involves creating the architectural design, database design, user interface design, and defining the overall system structure.

Implementation: Actual coding or development of the software according to the design specifications. It involves writing code, integrating different components, and ensuring code quality through testing.

Testing: Comprehensive testing to identify and rectify defects or errors in the software. This includes unit testing, integration testing, system testing, and user acceptance testing (UAT).

Deployment: The software is deployed or released to the production environment or end-users after successful testing. This phase involves installation, configuration, data migration, and training if required.

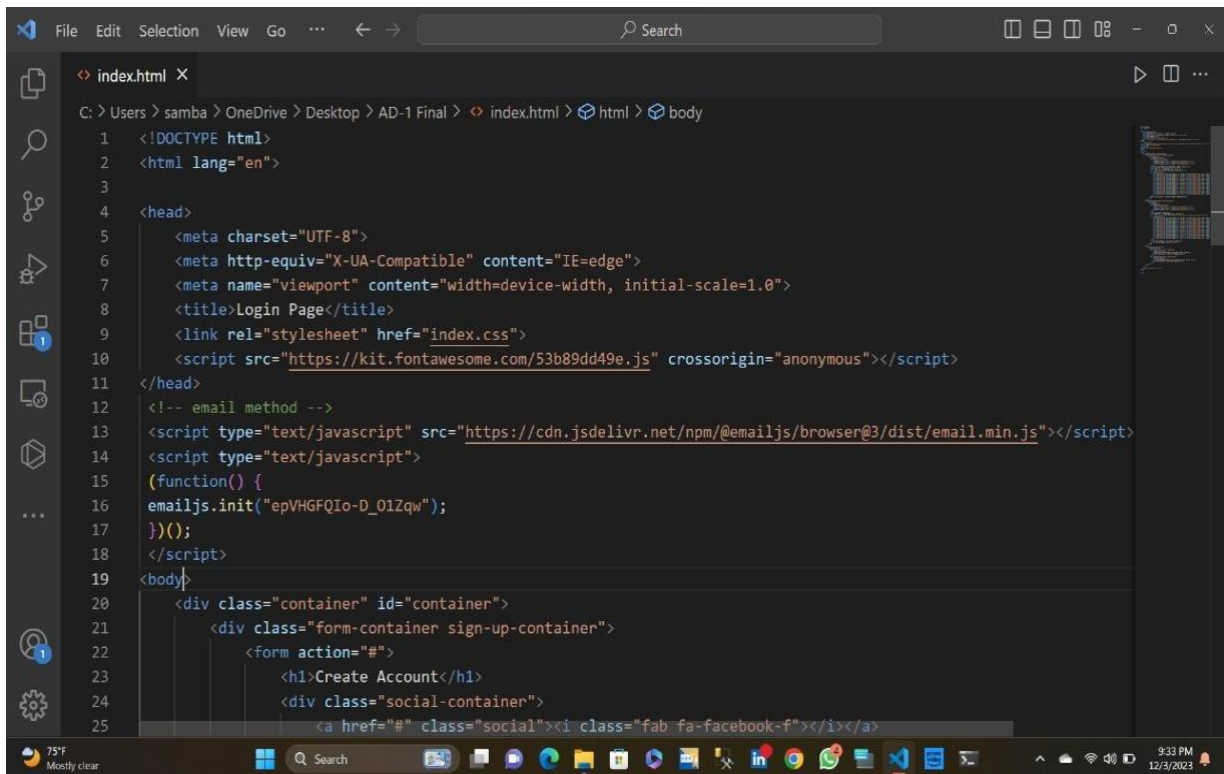
Maintenance: After deployment, the software enters the maintenance phase. It involves fixing issues, updating functionalities, adding new features, and ensuring continuous usability and performance.

These phases generally follow a linear sequence, often referred to as the waterfall model. However, modern software development methodologies, such as Agile, Scrum, or DevOps, promote iterative and flexible approaches where these phases might overlap or run in shorter cycles to adapt to changing requirements and ensure continuous improvement.

CHAPTER 6

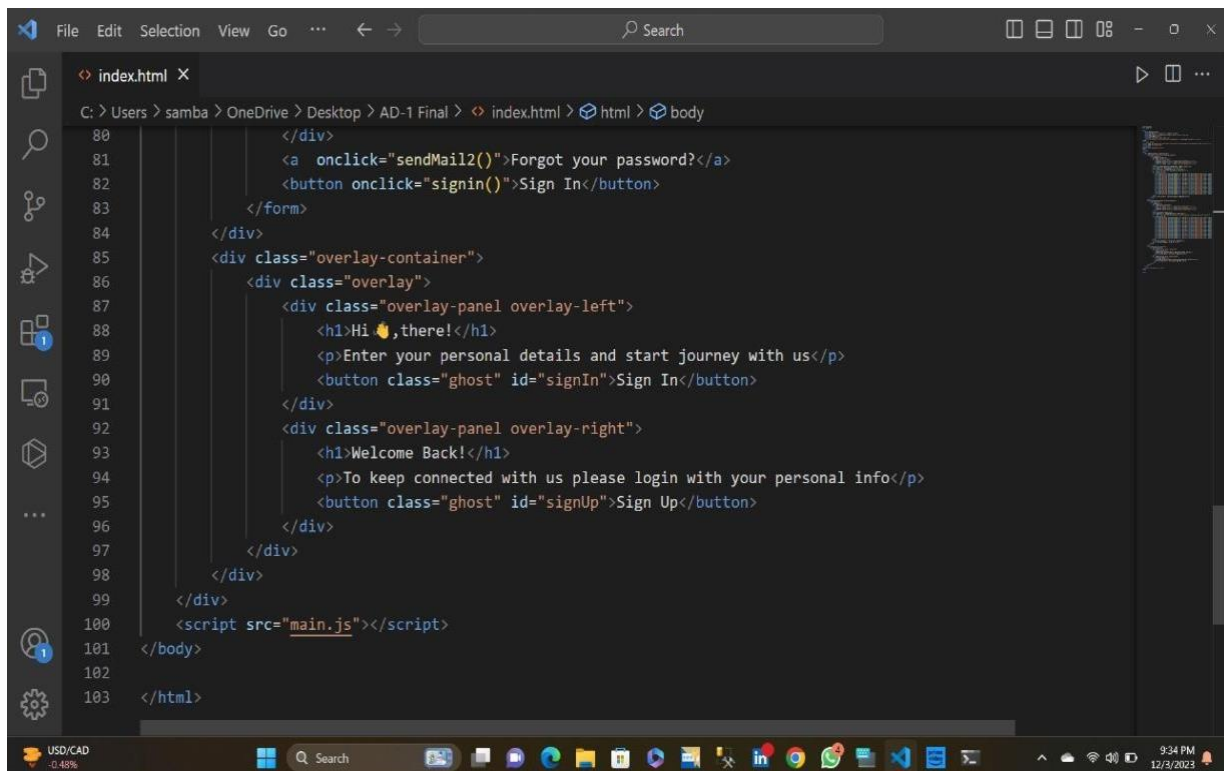
IMPLEMENTATION

6.1 SAMPLE CODE



```
index.html X
C:\Users\samba> OneDrive\Desktop> AD-1 Final > index.html > html > body
1  <!DOCTYPE html>
2  <html lang="en">
3
4  <head>
5      <meta charset="UTF-8">
6      <meta http-equiv="X-UA-Compatible" content="IE=edge">
7      <meta name="viewport" content="width=device-width, initial-scale=1.0">
8      <title>Login Page</title>
9      <link rel="stylesheet" href="index.css">
10     <script src="https://kit.fontawesome.com/53b89dd49e.js" crossorigin="anonymous"></script>
11 </head>
12 <!-- email method -->
13 <script type="text/javascript" src="https://cdn.jsdelivr.net/npm/@emailjs/browser@3/dist/email.min.js"></script>
14 <script type="text/javascript">
15 (function() {
16     emailjs.init("epVHGfQIo-D_01Zqw");
17 })();
18 </script>
19 <body>
20     <div class="container" id="container">
21         <div class="form-container sign-up-container">
22             <form action="#">
23                 <h1>Create Account</h1>
24                 <div class="social-container">
25                     <a href="#" class="social"><i class="fab fa-facebook-f"></i></a>
```

Fig 6 Sample Code 1



```
index.html X
C:\Users\samba> OneDrive\Desktop> AD-1 Final > index.html > html > body
80     </div>
81     <a onclick="sendMail2()">Forgot your password?</a>
82     <button onclick="signin()">Sign In</button>
83 </form>
84 </div>
85 <div class="overlay-container">
86     <div class="overlay">
87         <div class="overlay-panel overlay-left">
88             <h1>Hi 🤖,there!</h1>
89             <p>Enter your personal details and start journey with us</p>
90             <button class="ghost" id="signIn">Sign In</button>
91         </div>
92         <div class="overlay-panel overlay-right">
93             <h1>Welcome Back!</h1>
94             <p>To keep connected with us please login with your personal info</p>
95             <button class="ghost" id="signUp">Sign Up</button>
96         </div>
97     </div>
98 </div>
99 </div>
100 <script src="main.js"></script>
101 </body>
102
103 </html>
```

Fig 7 Sample Code 2

```

index.html X
C:\Users\samba>OneDrive\Desktop>AD-1 Final>index.html
<div class="social-container">
  <a href="#" class="social"><i class="fab fa-facebook-f"></i></a>
  <a href="#" class="social"><i class="fab fa-google-plus-g"></i></a>
  <a href="#" class="social"><i class="fab fa-linkedin-in"></i></a>
</div>
<span>or use your email for registration ('gmail' only)</span>
<input type="text" placeholder="Name (Optional)" />
<input type="email" placeholder="Email" id="upmail" />
<!-- <input type="password" placeholder="Password" /> -->
<div class="password">
  <div class="passimg" onclick="upimg(this)" id="s01">OneDrive\Desktop>AD-1 Final>JS main.js
1  const signUpButton = document.getElementById('signUp');
2  const signInButton = document.getElementById('signIn');
3  const container = document.getElementById('container');
4  //const c_mail=document.getElementById('upmail');
5  let uppass = [];
6  let inpass = [];
7
8  signUpButton.addEventListener('click', () => {
9    container.classList.add('right-panel-active');
10 });
11
12
13 signInButton.addEventListener('click', () => {
14   container.classList.remove('right-panel-active');
15 });
16 // adding and removing border
17 function upimg(element) {
18   var Image = element.querySelector('img');
19   if (Image) {
20     if (Image.classList.contains('clicked')) {
21       Image.classList.remove('clicked');
22       uppass.splice(uppass.indexOf(element.id), 1);
23       // console.log(element.id);
24       // console.log(uppass);
25     }

```

Fig 9 Sample code 4

CHAPTER 7

TESTING

7.1 INTRODUCTION

Software testing plays a crucial role in ensuring the quality, reliability, and functionality of software applications.

Detecting Defects: Identifying errors, bugs, or inconsistencies in the software to prevent issues that might arise during the application's operation.

Validation and Verification: Confirming that the software meets the specified requirements and functions as intended by the stakeholders.

Enhancing Quality: Improving the overall quality of the software by ensuring its usability, reliability, efficiency, and security.

Types of Software Testing:

Unit Testing:

- **Purpose:** It validates individual units or components of the software in isolation to ensure they function correctly.

- **Detailed Explanation:** Unit testing verifies the smallest testable parts of the application, typically functions or methods, to validate their behavior against expected outcomes. Developers commonly conduct unit tests using test frameworks like JUnit, N Unit, or Mocha.

Integration Testing:

- **Purpose:** It evaluates the interaction and communication between different units or modules integrated into larger components.

- **Detailed Explanation:** Integration testing verifies how various components function together after they are integrated. This testing level checks interfaces, data flow, and communication between modules. Tools like Selenium, SoapUI, or Postman aid in conducting integration tests.

White-box Testing:

- **Purpose:** It examines the internal structure, logic, and code of the software to validate its functionalities.
- **Detailed Explanation:** White-box testing, also known as structural or glass-box testing, involves scrutinizing the code, checking paths, branches, and internal logic to ensure all code paths are tested. Techniques like statement coverage, branch coverage, and path coverage are used to achieve thorough testing.

Black-box Testing:

- **Purpose:** It tests the software's functionalities without having knowledge of its internal code structure.
- **Detailed Explanation:** Black-box testing focuses on validating the software's behavior against specified requirements without considering its internal implementation.

Testers create test scenarios based on expected inputs and outputs, emphasizing user perspectives and system functionalities. Techniques like equivalence partitioning, boundary value analysis, and exploratory testing fall under this category.

Each type of testing serves a specific purpose and contributes to the overall quality and reliability of the software. Combining different testing types in a comprehensive testing strategy ensures robust and error-free software applications

7.2 SAMPLE TEST CASES

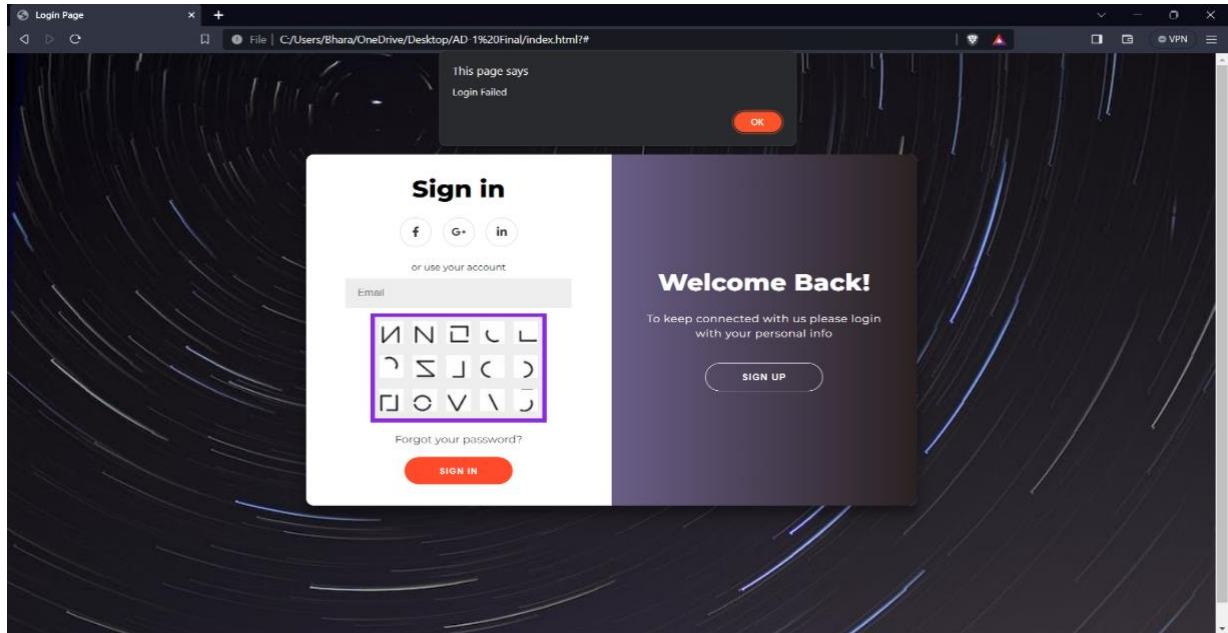


Fig 10 Sample Test 1

When we give an empty string and click sign in, it will not permit to enter in and 'login failed' is displayed

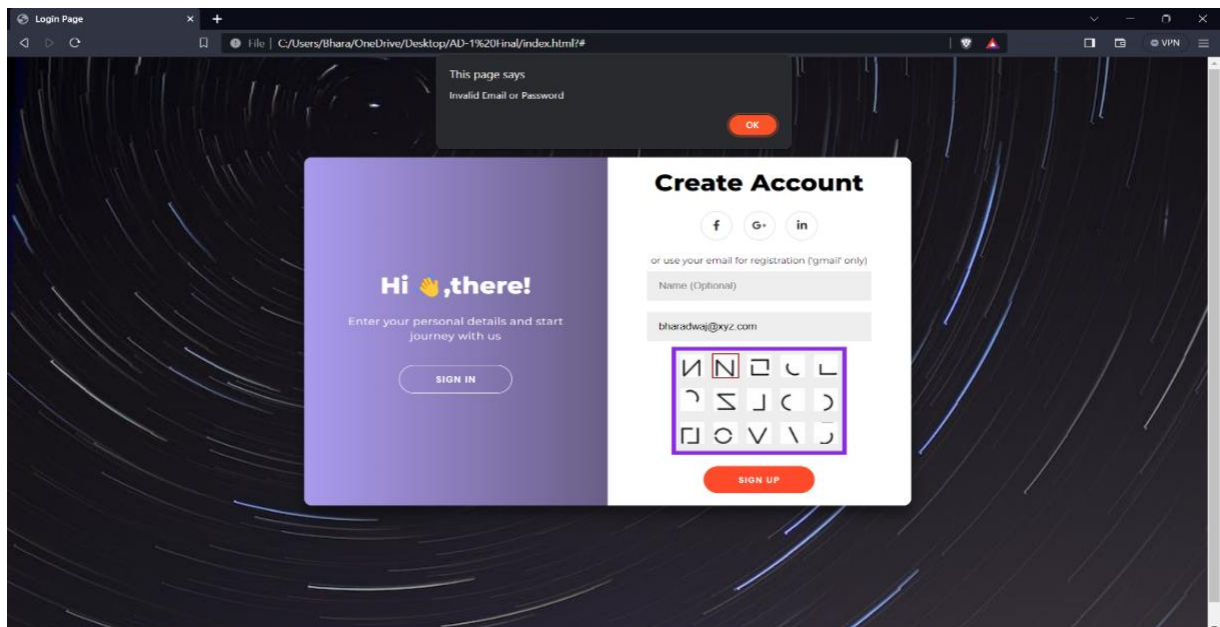


Fig 11 Sample Test 2

when any other mail except Gmail is given as input, it displays 'invalid email or password'

CHAPTER 8

OUTPUT SCREEN

8.1 SCREENSHOTS

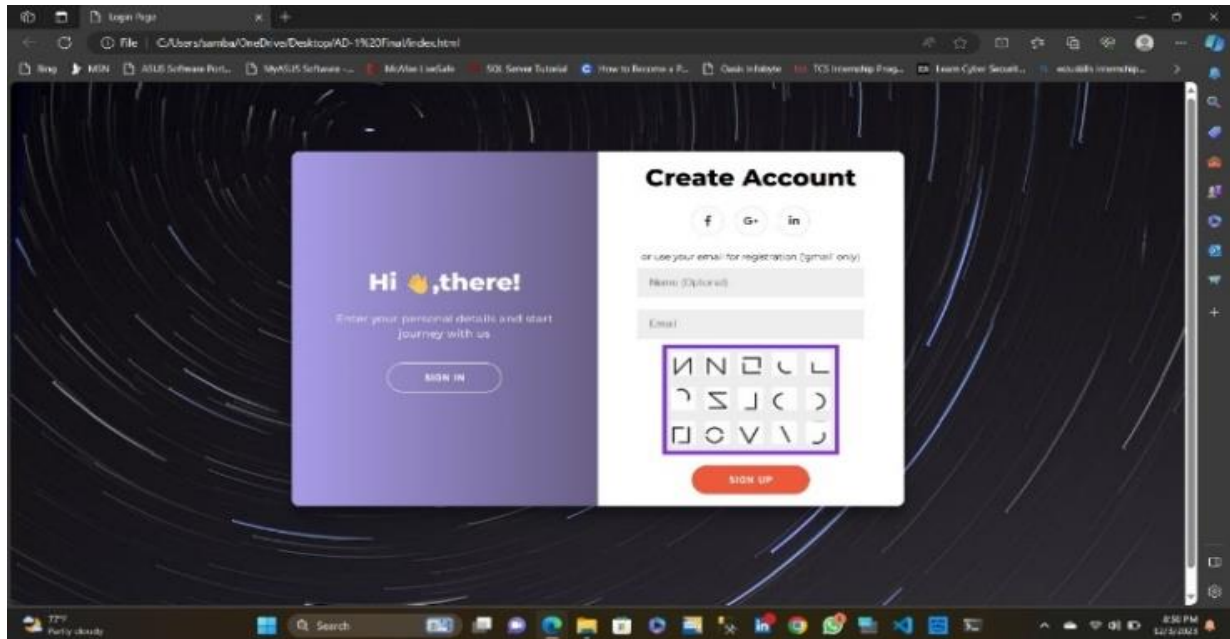


Fig 12 Output Screen 1

here we will give our credentials and if it matches the condition then the account will be created. if the condition fails then we will face an issue in signing up into the website

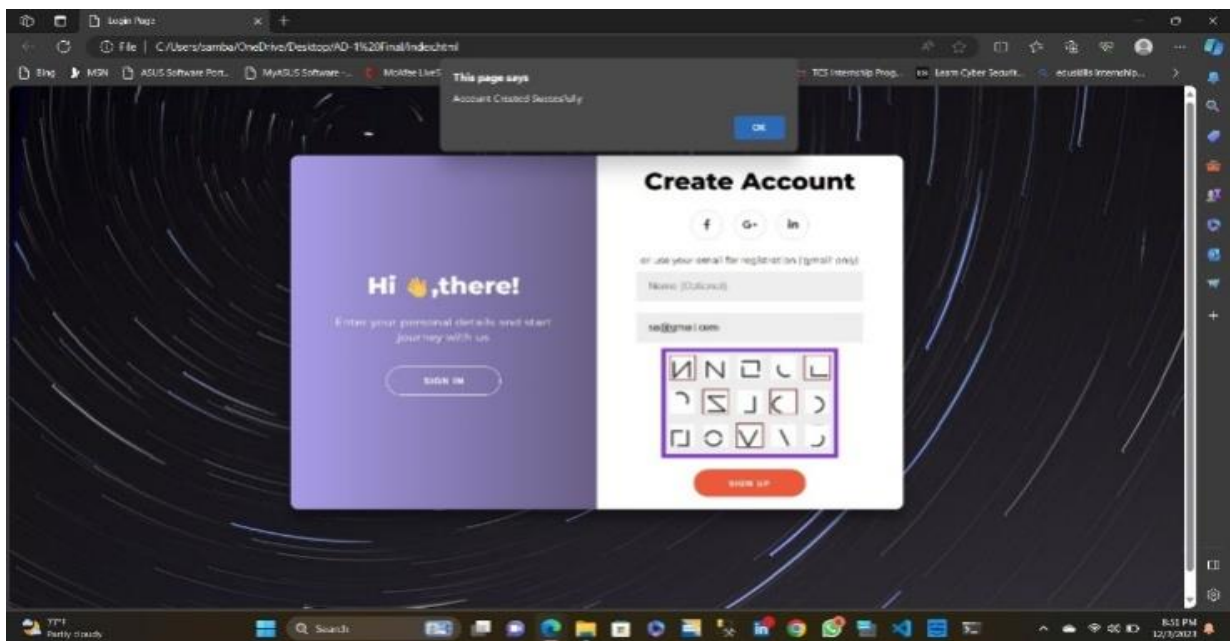


Fig 13 Output Screen 2

as the condition is matched, the account has been created successfully

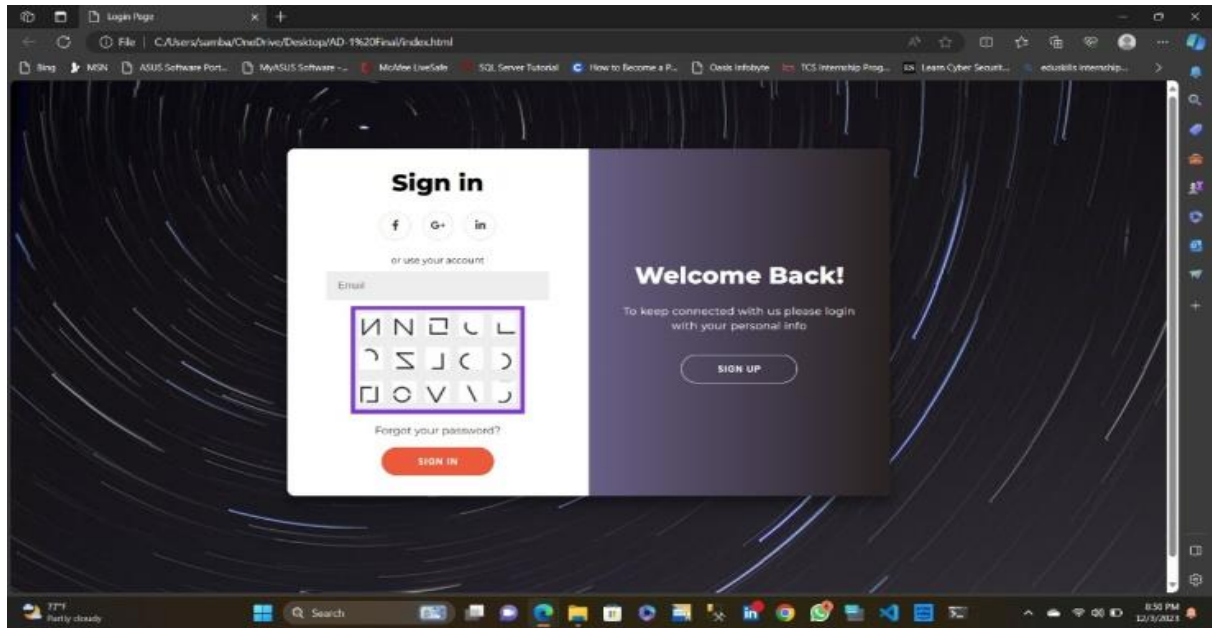


Fig 14 Output Screen 3

after signing up, we need to move to sign in page to login.

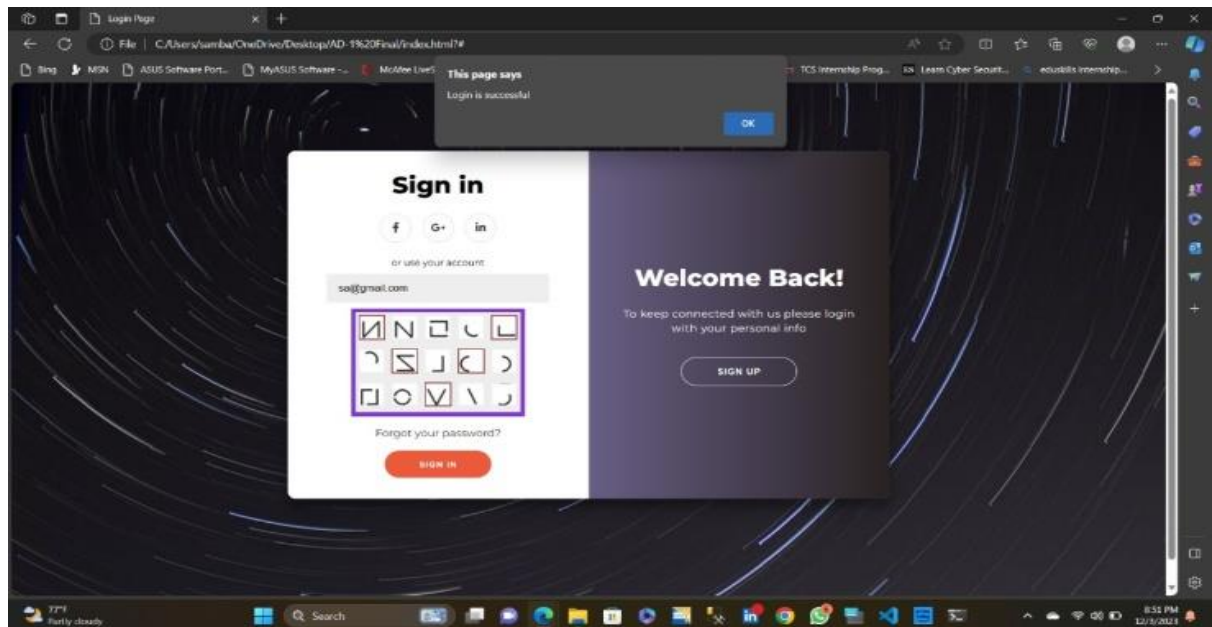


Fig 15 Output Screen 4

Once the details are matched, we will be able to sign in to our account

CHAPTER 9

COMCLUSION AND FUTURE SCOPE

9.1 CONCLUSION

The Image-Based Sequential Authentication System presents a promising alternative to conventional text-based passwords by leveraging human visual memory for authentication. By allowing users to create a sequence of images during signup and subsequently replicate this sequence for login, the system aims to enhance both security and usability.

Through the exploration of image-based authentication, this system acknowledges the limitations of traditional passwords, addressing issues related to memorization challenges and password reuse. The proposed approach aligns with the goal of providing a more intuitive and potentially more secure method for users to protect their accounts.

9.2 FUTURE SCOPE

Enhanced Security Measures: Continual advancements in encryption techniques and pattern analysis can fortify the system against emerging cyber threats, ensuring robust protection of user data.

Machine Learning Integration: Implementing machine learning algorithms to analyze user behavior and preferences in image selection can refine the system, optimizing the image sequence creation process.

Biometric Integration: Exploring the fusion of image-based authentication with biometric identifiers, such as facial recognition or fingerprint scanning, can further elevate security standards.

Usability Improvements: Iterative user testing and feedback collection can guide the development of a more intuitive image selection interface, ensuring ease of use for diverse user demographics.

Multi-Factor Authentication (MFA): Integrating this image-based authentication with other authentication factors, such as OTPs or hardware tokens, can strengthen the overall security posture of the system.

Mobile Application Implementation: Adapting the system into a mobile application format can enhance accessibility and convenience for users accessing accounts via smartphones or tablets.

Accessibility Considerations: Ensuring the system accommodates users with disabilities by providing alternative authentication methods or interface adaptations for diverse user needs.

Continued research and development in these areas can further refine and optimize the Image-Based Sequential Authentication System, solidifying its position as a robust, user-friendly, and secure authentication solution in the evolving landscape of cybersecurity.

CHAPTER 10

REFERENCES

10.1 WEBSITES

- i. <https://www.geeksforgeeks.org/graphical-password-authentication/>
- ii. <https://uxdesign.cc/graphical-passwords-for-authentication-4e716b94eb47>

10.2 BOOKS

- i. Security for Wireless Sensor Networks using Identity-Based Cryptography; Harsh Kupwade Patil, Stephen A. Szygenda
- ii. Modern Authentication with Azure Active Directory for Web Applications; Vittorio Bertocci
- iii. Password; Martin Paul Eve, Christopher Schaberg, Ian Bogost

10.3 RESEARCH PAPERS

- i. Abdleazeem S, El-Sherif Ezzat (2008) Arabic handwritten digit recognition. Int J Doc Anal Recogn IJDAR 11:127–141
- ii. Jirjees SW, Mahmood AM, Nasser AR (2022) Passnumbers: an approach of graphical password authentication based on grid selection. IJSSE 12(1):21–29