I.ABSTRACT

GRAPHICAL PASSWORD AUTHENTICATION

Authentication is the technique for giving people admittance to framework object in light of client's uniqueness. On the off chance that the code match, the interaction will be achieved and client will get the endorsement to get to the framework. Text-based secret word plot observes the rules such as no less than 8 characters in length, ought to join capitalized and lower-case and digits. Client have issue to recollect their convoluted secret phrase over the long haul because of the restriction of human mind, client will generally disregard their secret phrase. Client will generally utilize something similar secret key for all kind of record. Thus, assuming one record is hacked, the opportunities for other record to be hack is high. Other than that, picking the straightforward printed based secret word may build its weakness for assaults or interruptions.

Thus, graphical secret key confirmation by utilizing passpoints conspire has been presented in this venture. Graphical secret key validation by utilizing passpoints plot is a model to recognize the most probable areas for client to click to make graphical secret word. The activity of the purposed conspire is basic and simple to learn for client since they recognizable with printed graphical secret word conspire. All in all, this graphical secret key plan will make it more straightforward for client to do their validation cycle since it is not difficult to recollect also, difficult to figure by others.

II. LIST OF FIGURES

CHAPTER 1
INTRODUCTION

Graphical Password confirmation is a technique for verification where clients are expected to utilize graphical components, like pictures, images, or shapes, rather than customary alphanumeric passwords. This technique has acquired consideration as an option in contrast to customary text based passwords because of its capability to be more significant and simpler to utilize Research on Graphical Password Authentication.

Over the years, researchers have conducted numerous studies to evaluate the effectiveness, usability, and security of graphical password authentication. Some of the key findings are:

1.1Memorability:

Studies have shown that graphical passwords can be easier to remember than traditional textbased passwords, especially for people who are more visually oriented. However, users tend to choose simple and predictable images, which can make their passwords more vulnerable to guessing attacks.

1.2 Usability

Graphical passwords can be more user-friendly than text-based passwords, especially for users who have difficulty remembering complex passwords. However, the usability of graphical passwords can be affected by factors such as the size of the image grid, the number of images in the set, and the difficulty of the task assigned.

1.3 Security

The security of graphical passwords can be affected by various factors, such as the type of images used, the order of the images, the number of login attempts allowed, and the complexity of the password. Some studies have shown that graphical passwords can be more vulnerable to shoulder surfing attacks and smudge attacks than text based passwords.

1.4 User acceptence

The acceptance of graphical passwords by users depends on various factors, such as their familiarity with the technology, their perception of the security and usability of the method, and their previous experience with password authentication. Some studies have shown that users generally have a positive attitude towards graphical passwords, especially when they are presented as an alternative to traditional text-based passwords.

1.5 Objectives

1.5.1The first objective of the research is:

1. Creating a mobile application that employs graphical password authentication.
2. To use the Passpoint technological advances to develop the Graphical Password Authentication application.
3. The assessment of the Graphical Password Authentication system's efficiency utilising.

1.6 Project Scope

The project's scope has been determined in order to simplify the web system procedure.

The system's security is the primary focus of this project.

1.6.1 Scope of User:

- When registering and logging in, enter your username, password, and email address.
- During the login and registration phases, choose a picture.
- During the login and registration phases, click five points.

1.6.2 Scope of System

- Sign up – The user can choose an image and click the appropriate number of times to earn points using the authentication method.
- - Log in – verify that the picture, clicked points, password, and user username are correct and stored in the data store

Aim of the project

The Aim intended use of graphical password authentication is to provide users a safe, intuitive,and enduring authentication mechanism that may take the place of conventional text based passwords .

1.7 Objective of the Project:

- Security.
- Usability.
- Accessability.
- Scalability.
- Resistance to attacks

1.8 Scope of the Project

Graphical password authentication is a topic that can be explored in various ways, with different levels of complexity and scope depending on the objectives and goals of the project. Here are some possible areas of focus for a graphical password authentication project: Design and assessment of graphical password schemes: creating and placing to the test novel graphical password schemes may be part of this project. It could include designing new types of images, icons, or symbols that users could use to create passwords. The project could also evaluate the usability, security, and memorability of the new graphical password schemes through user studies and experiments.

1.9 Experimental Setup:

This chapter includes a comprehensive summary of the specs in in addition to the prerequisites for software and hardware needed for the project.

1.10 System Specifications:

Hardware Requirements:

PC with Windows/Linux OS

Processor with 1.7-2.4gHz speed

Minimum of 4gb RAM

2gb Graphic card

Software Specification:

Text Editor (e.g.: -VS-code)

1.11 Advantages:

Graphical password authentication systems have a number of advantages over traditional text based password authentication systems. Here are some of the advantages:

Enhanced Security: Compared to conventional text-based passwords, graphical passwords are typically more safe. By integrating images, colours, forms, and patterns into their passwords, users may make them tougher to guess or steal.

Easy to use: Because graphical passwords make use of visually appealing elements like images, colours, forms, and patterns that the user is more likely to remember, they are usually simpler for users to recall than text-based passwords.

Resistance to Keystroke Logging: Graphical passwords are resistant to keystroke logging attacks, which are commonly used to steal text-based passwords.

Accessibility: Graphical passwords can be easier for users with certain disabilities, such as dyslexia, to use because they do not require typing or reading.

User Preference: Some users simply prefer graphical passwords over traditional text-based passwords, which can increase user satisfaction and adoption of the authentication system.

Visual Appeal: Graphical passwords can be more visually appealing and engaging than traditional textbased passwords, which can make the authentication process more enjoyable for users.

1.13 Project Flow and Methodology:

In The proposed system for developing a graphical password and authentication system typically follows a structured path. It begins with project planning and requirements gathering, where the objectives and scope of the system are defined, and user requirements are collected. Extensive research is conducted to explore potential graphical elements for passwords and security measures.

Once the conceptualization is complete, the system's architecture and user interfaces are designed, taking into account security and usability considerations. The actual implementation involves creating interfaces for password creation, authentication logic, and user management, all while prioritizing security measures. Extensive usability testing is carried out to ensure that the system is user-friendly, and performance optimization is performed for efficient authentication. Security testing, documentation, and compliance checks are essential steps before deployment. Continuous maintenance, updates, and user training are necessary for long-term success, and a feedbackdriven approach ensures that the system evolves to meet evolving user needs and security threats. Throughout the entire project, collaboration with experts in security, usability, and legal compliance is crucial to deliver a robust and user-friendly graphical password and authentication system.

1.13.1 Login and Registration:

This phase involves login and registration for User. The user's details are maintained confidential by maintaining separate account for each user.

1.13.2 Notification:

This phase involves the notification to the User. The site will send the notification which contains the user has authenticated.

1.13.3 Admin Module:

In admin module, the administrator maintains the user details. The administrator maintains security to password.

1.13.4 Selection Method

The user after registration has to choose his convinent type of graphical password that he has been need and lead

INFORMATION TECHNOLOGY

CHAPTER -2

LITERATURE SURVEY

A literature survey of graphical password authentication encompasses various research papers, articles, and studies investigating different aspects of graphical password systems.

Here's a condensed overview of some key themes and notable works in this area:

1. **Authentication Schemes and Techniques**:

- "Graphical Password Authentication: A Survey" by Das, Bonneau, and Caesar (2014) provides an extensive overview of graphical password schemes, covering various techniques such as recall-based, recognition-based, and cued-recall graphical passwords.
- "A Survey of Graphical Passwords" by Khan et al. (2016) explores different types of graphical authentication methods, including image-based, pattern-based, and hybrid schemes.

2. **Usability and Security Evaluation**:

- "Graphical Passwords: Learning from the First Twelve Years" by Biddle et al. (2012) investigates the usability and security of graphical password schemes based on a twelveyear study.
- "Towards Reliable Storage of Graphical Passwords on Smartcards" by C.-K. Pang et al. (2015) explores the challenges and solutions for securely storing graphical passwords on smartcards, considering both usability and security aspects.

3. **User-Centered Design**:

- "User Choice in Graphical Passwords" by Wiedenbeck et al. (2005) examines users' preferences and behaviors in selecting graphical passwords, highlighting the importance of user-centered design in graphical authentication systems.
- "Exploring the Design Space of Graphical Passwords on Smartphones" by Chen et al. (2015) investigates the design considerations and usability challenges specific to graphical passwords on smartphone devices.

4. **Attacks and Countermeasures**:

- "On the Security of Picture Gesture Authentication" by Aviv et al. (2010) explores attacks on picture gesture authentication systems and proposes countermeasures to enhance security.
- "Eye Tracking Shoulder Surfing on Mobile Devices" by Schechter et al. (2009) investigates the vulnerability of graphical passwords to shoulder surfing attacks and proposes mitigations using eye tracking technology.

5. **Biometric Integration**:

- "A Survey on Graphical Passwords Based on Human Cognitive Behaviors" by Zeng et al. (2016) discusses the integration of biometric features such as gaze patterns and touchscreen gestures into graphical password authentication systems.
- "A Survey on the Security of Biometric Authentication Systems" by Jain et al. (2016) provides an overview of security issues and challenges in biometric-based authentication systems, including those utilizing graphical passwords.

These works collectively contribute to advancing our understanding of graphical password authentication, addressing usability challenges, enhancing security measures, and exploring novel techniques for improving the effectiveness of graphical password authentication.

CODE

```
import pymongo from pymongo
import MongoClient import random
import string from datetime import
datetime import os from dotenv
import load_dotenv

class MongoDB(object):

        def _init_(self, dBName=None, collectionName=None):
load_dotenv()    self.dbURI =
os.getenv('DB_URL')    self.dBName =
dBName
         self.collectionName = collectionName

         self.client = MongoClient(self.dbURI, 27017, maxPoolSize=50)

self.DB = self.client[self.dBName]       self.collection =
self.DB[self.collectionName]     print("Successfully connected to
the monogodb server !!")
def FetchData(self):
         """
         :param : None
         :return: records
         """
         records = self.collection.find ({})  return
        list(records)

        def InsertData(self, data):
         """
```

```
            :param records: Array of Records
            :return: None
            """

self.collection.insert_many(data, ordered=True)          print("Data has
been inserted successfully to the Databse !!")
def UpdateData(self, data):
            """
            :param records: Array of objects {query, newvalues}
            :param example: data[i]["query"] = { "address": "Valley 345" },
data[i]["newvalues"] = { "$set": { "address": "Canyon 123" } }
            :return: None
            """
            for item in data:
  self.collection.update_one(item["query"], item["newvalues"])          print("Database has
been updated successfully !!")
def DropData(self, data):
            """
            :param records: Array of queries
            :param example: data[i] = { "address": "Mountain 21" }
            :return: None
            """
            for item in data:
            self.collection.delete_one(iteam)   print("Records has been deleted
            successfully from the Databse !!")

def          generateId(exitingIds):
  while True:
 x = ''.join(random.choices(string.ascii_letters + string.digits, k=16))              if
x not in exitingIds :
```

```
                    exitingIds.append(x)
                    break
            return x

if _name_ == "_main_":
mongodb = MongoDB(dBName = 'sih2022', collectionName='grammar')     now
= datetime.now()        current_time = now.strftime("%H:%M:%S")         #
records = GetMentorRecords()          records = mongodb.FetchData()
  print(f"{len(records)} records are fetched successfully!!")

exitingIds = []
  newGrammar = []
  alphabets = []          if
records:
          for data in records:
                    if data["previous"]:
           exitingIds.append(data["previous"])
  exitingIds.append(data["current"])    alphabets.append(data["alphabet"])
  newGrammar.append({
                        "query" : {"alphabet" : data["alphabet"]},
                        "newvalues" : {
                                "$set" : {
                                        "alphabet" : data["alphabet"],
                                        "previous" : data["current"],
                                        "current" : generateId(exitingIds),
                                        "previoustimestamp" : data["currenttimestamp"],
                                        "currenttimestamp" : current_time
                                }
                        }
                    })
```

```
print("Records are updated !! Updating the Database ...")
 mongodb.UpdateData(newGrammar)


        else :
alphabets = list(string.ascii_uppercase + string.digits)
 alphabets.remove("0")          for data in alphabets:
 newGrammar.append({
 "alphabet" : data,
                        "previous" : "",
                        "current" : generateId(exitingIds),
                        "previoustimestamp" : "",
                        "currenttimestamp" : current_time
                    })
print("New records are created !! Updating the Database ...")
 mongodb.InsertData(newGrammar)   print("Script Finished !!")
```

CHAPTER-3

METHODLOGY

A modified methodology tailored for testing the four graphical password authentication methodsUndoubtedly, the following modified approach is designed to evaluate the four graphical password authentication methods: evaluate Image Authentication, Test Garbled Image Authentication, Test Segmented Images, and Test Obscured Method.

3.1.1 Specify your goals and metrics.

- The goals for each technique you wish to test should be specified in detail. Examining security, usability, and resilience to certain threats are a few examples.
- Determine the precise metrics for each technique, such as the proportion of successful authentications, the time required for authentication, resilience to certain assaults, and user satisfaction.

3.1.2Preparation of Data:

- Make a dataset including normal pictures, segmented photos, blurry images, and obscured images for each approach.

3.1.3 Creating a test environment:

- For each approach, create a controlled testing environment. Ensure hardware and software uniformity across all testing.

3.1.4 Recruiting and educating users:

- Make sure the participants you choose for each technique will be among the method's target audience.
- To guarantee that participants are familiar with the particular authentication procedure, train them independently for each technique.

CHAPTER - 4

4. Scenarios for Method-Specific Tests:

4.2.1 Test Obscure Approach:

- Test how effectively users can authenticate when certain portions of the authentication picture are obscured by situations.
- Analyze the duration and rate of acceptance for authentication employing obscured photos.

4.2.2 Segmented image testing

- Create instances whereas users must authenticate by choosing the proper segments from a segmented picture.
- Segmented photos can be used to gauge success rates, processing time, and user satisfaction.

4.2.3Authentication of garbled images test:

Create circumstances where users must verify using scrambled or warped photos. Analyze outcome rates, processing times, and user comments for garbled photos.

4.2.4 Authentication test for images:

Include scenarios that use typical, unedited photographs for this approach.

Analyze the time required for regular photos and the success rates for authentication.

4.2.5 Data Gathering

Gather information on how each scenario relevant to a method is performed by participants.Keep track every method’s outcome, authentication time, and user comments.

4.2.6Security Assessment:

Test each approach against appropriate assaults. examine their resistance to brute force, pattern analysis, or shoulder surfing, for instance. Record data based on how resistant the approach is to certain assaults.

4.2.7 Usability Assessment:

To get user input on each method's functionality and satisfaction, utilize surveys or Analyze each technique's user feedback, learnability, and general satisfaction.

4.2.8 Data Evaluation:

Using the unique metrics established for each approach, analyze the data gathered for each one and compare how well it performed.

Determine each method's advantages and disadvantages in light of the test findings.

4.2.9 Recommendations:

Give some guidance for each technique based on the findings of the examination. Mention places where each approach might be improved or strong.

Interpret the results and provide advice for each approach based on the evaluation of that method. With a focus on their distinctive qualities and goals, this updated technique enables you to thoroughly assess each of the four graphical password authentication methods separately.

CHAPTER-5

5.Workflow

Workflow that involves testing various methods related to image authentication and security.

Here's a general workflow for these methods: **Test**

Obscure Approach:

First, choose or create an obscured picture—any image that has been purposefully distorted or concealed to make authentication more challenging. Use the suggested technique to verify obscured photos. To recover the occluded image, this approach could use deblurring, denoising, or other image processing procedures. Compare the verified image with the original, unobscured image or a reference standard to assess the effectiveness of the process. It is possible to employ metrics like the Mean Squared Error (MSE), the Structural Similarity Index (SSI), or evaluations of perceptual quality.

5.1 Segmented image testing:

Get a series of divided photos ready. pictures that have been split up into several areas or segments are called segmented pictures. Utilize the suggested technique to verify segmented photos. This might entail confirming each segment's accuracy and integrity. By contrasting the authenticated portions with the matching unique segments or reference standards, one may evaluate the effectiveness of the approach. In this situation, metrics like recall, border precision, and pixel-wise accuracy might be helpful.

5.2 Authentication of garbled images test:

Construct or acquire purposefully jumbled or warped pictures, sometimes known as garbled images. Apply the suggested technique to verify distorted photographs. Techniques like reverse scrambling, picture decryption, and other pertinent processes could be used in this way. Compare the certified image with the original, undistorted image or a standard for

reference to see how effective the procedure was. Reconstruction quality or decryption accuracy might be suitable measures in this case.

5.3 Test Image Authentication:

Gather a collection of pictures for use in standard image authenticity tests. These might be pictures from many categories and sources. Use the suggested picture authentication technique, which usually entails confirming the legitimacy of the image, making sure it hasn't been altered maliciously, or both. Evaluate the authentication method's performance by determining how well it can distinguish genuine photographs from ones that have been altered or edited. Evaluation metrics usually include false positives, false negatives, and total accuracy.

5.4 Work Flow:

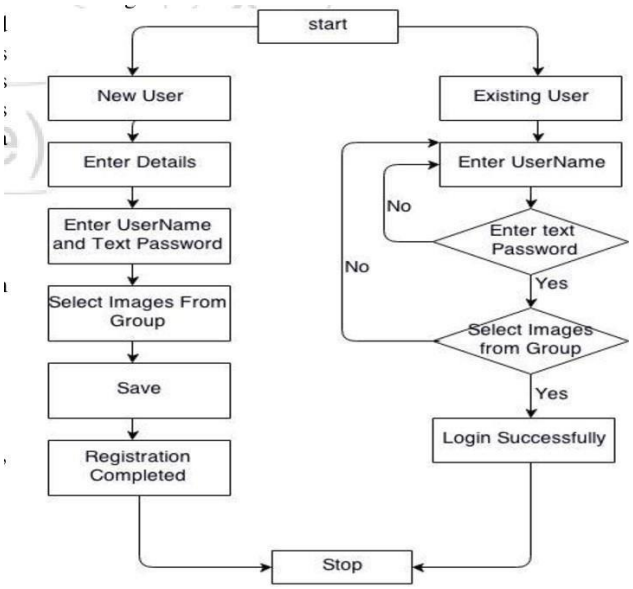


Figure 3.1: This is the image shows the workflow of the authentication.

CHAPTER-6

IMPLEMENTATION

ALGORITHM:

Step 1: Start the program.

Step 2: Select new user register.

Step 3: Fill your details.

Step 4: give your mail id.

Step 5: select the type of graphical password you liked.

Step 6: go on authentication process.

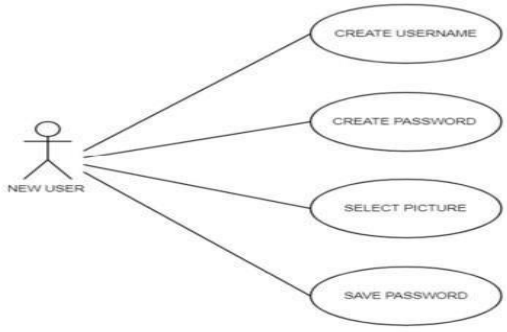
Step 7: verify the authentication process.

Step 8: if success it shows authentication successful.

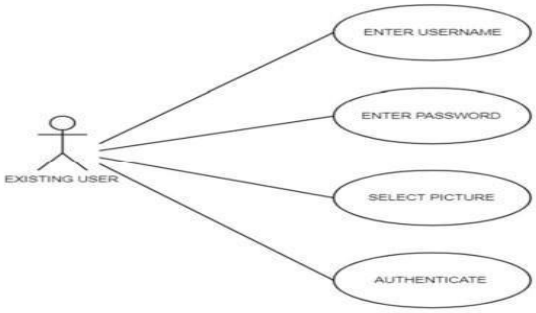
Step 9: if not it won't allows to login.

Step 10: It makes the user alert.

Usecase Diagram:



Use case diagram for new user



Use case diagram for exsisting user

Figure 1.1: This is the usecase diagram of the website.

Flowchart Diagram:

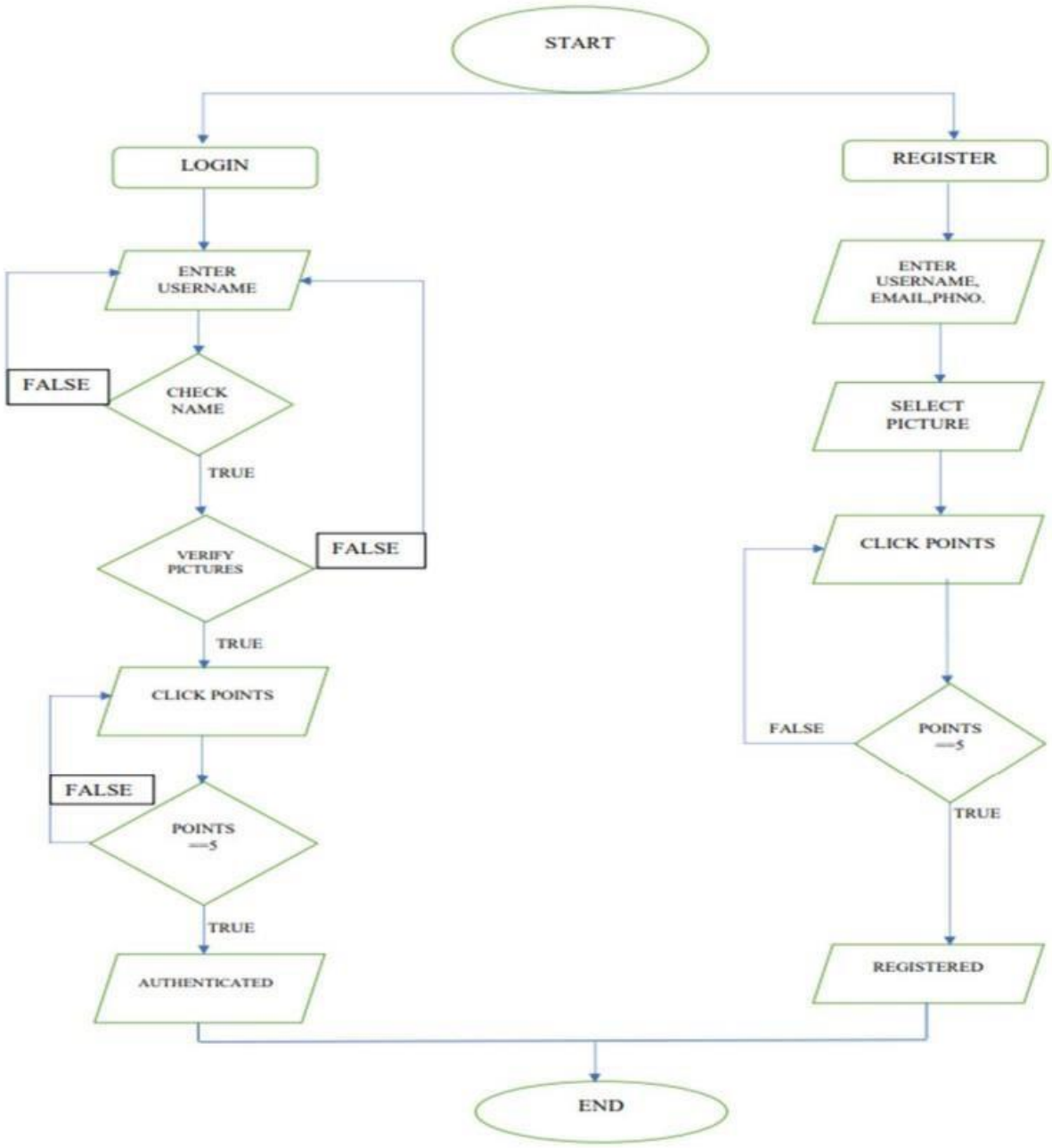
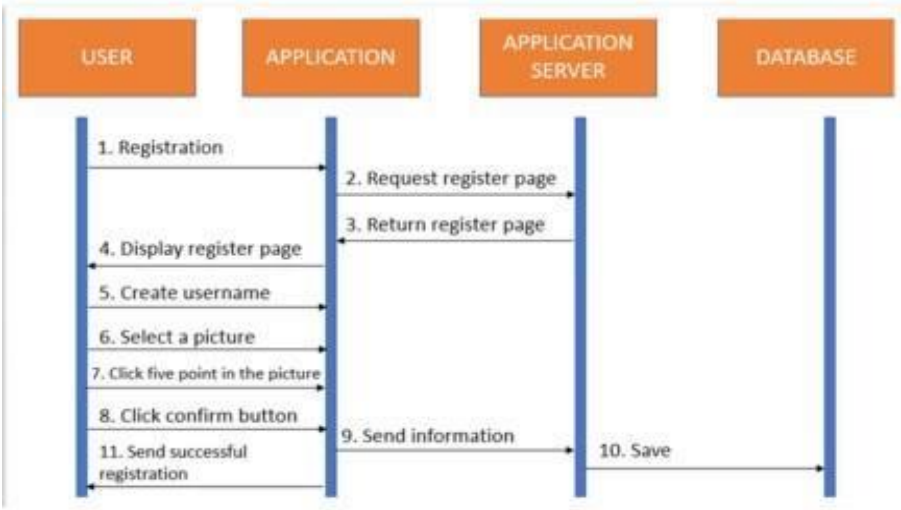
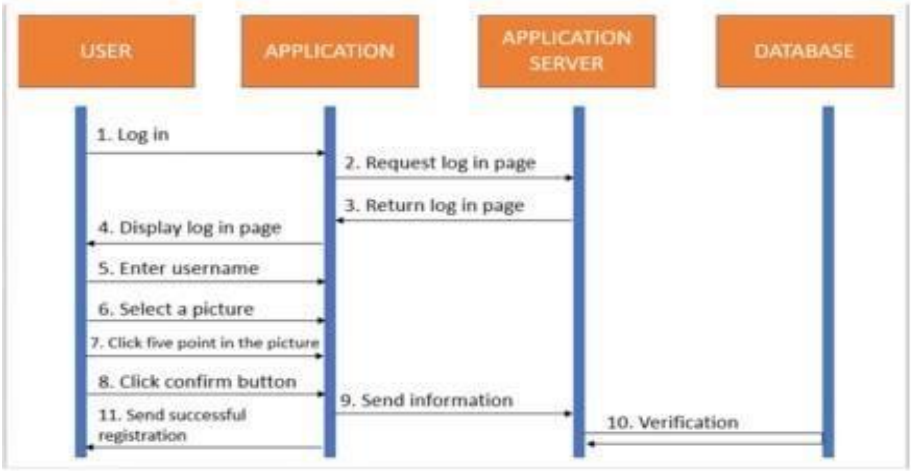


Figure 1.2: This is the flowchart diagram of the website.

Sequence Diagram



Sequence diagram for Registration phase



Sequence diagram for Login phase

Figure 1.3: This is the Sequence diagram of the website.

New user Registration

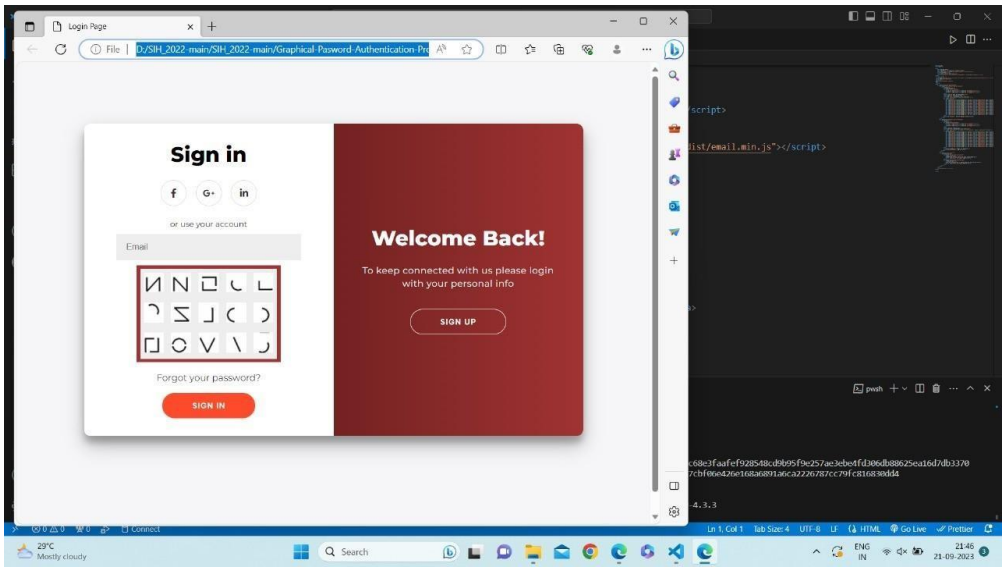


Figure1.4: This is the New user registeration from the website

Graphical password types:

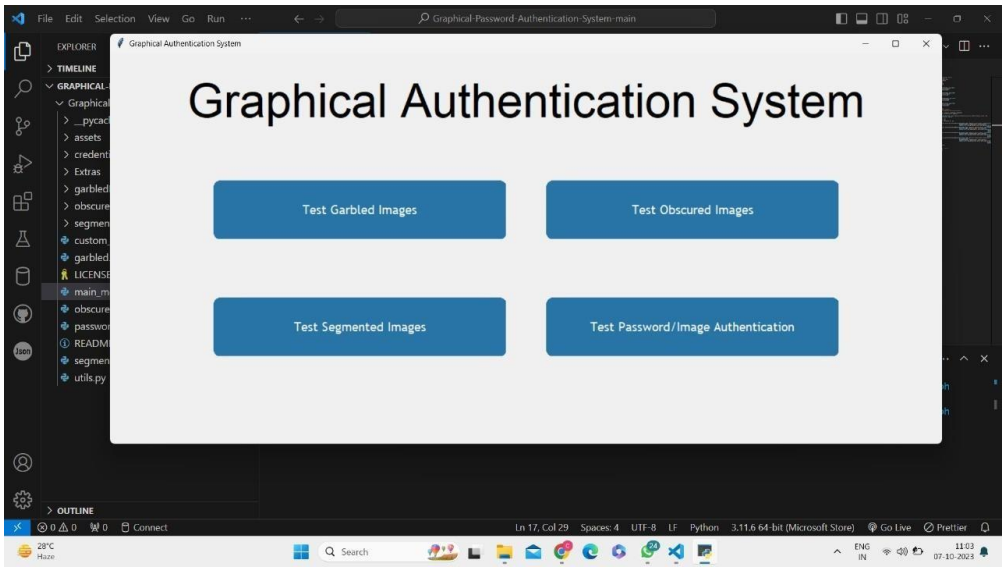


Figure 1.5: This is the Graphical password types

Test obscured image:

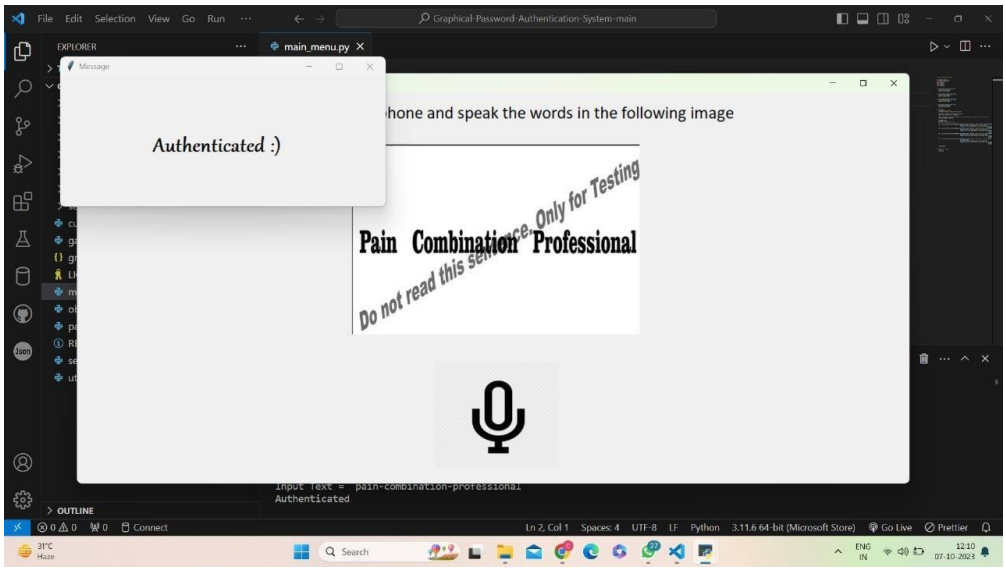
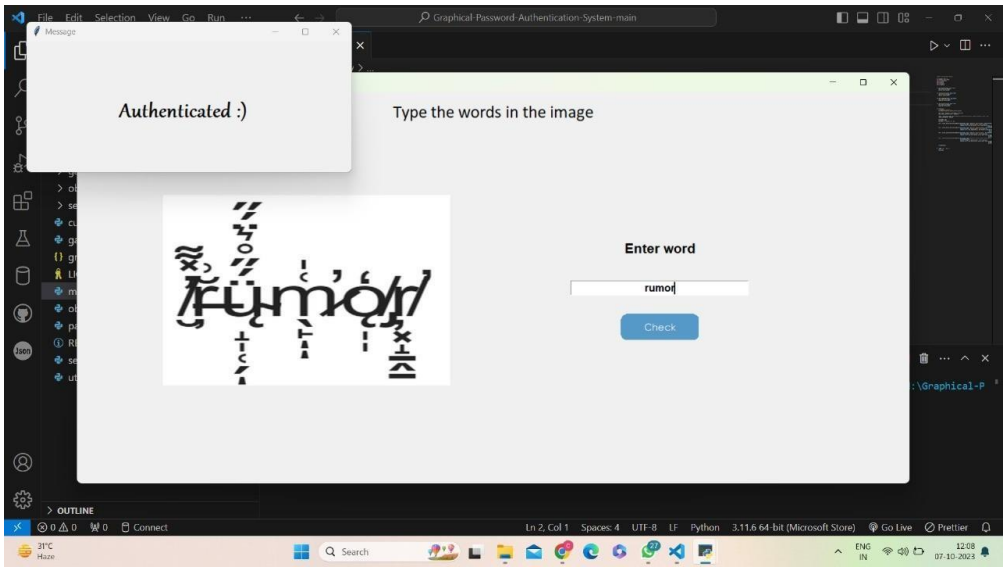


Figure 1.7: This is the image of test Obscured image authentication of the website.

Test Grabled Image:



CHAPTER-7

TESTING & VALIDATION

1. **Usability Testing**:

- **User Experience (UX) Testing**: Evaluate how easy it is for users to create and remember graphical passwords. This can involve tasks such as password creation, authentication, and password recovery.
- **Task Completion Time**: Measure the time it takes for users to perform authentication tasks using graphical passwords compared to traditional text-based passwords.
- **Error Rates**: Assess the frequency of errors made by users during authentication, such as incorrect password entries or forgotten passwords.
- **User Satisfaction Surveys**: Gather feedback from participants about their experience with the graphical password system, including likes, dislikes, and suggestions for improvement.

2. **Security Testing**:

- **Attack Simulation**: Conduct simulated attacks to evaluate the resilience of the graphical password system against common threats, such as shoulder surfing, brute force attacks, and dictionary attacks.
- **Password Strength Analysis**: Assess the strength of graphical passwords created by users to determine susceptibility to guessing or cracking.
- **Biometric Spoofing**: If the system integrates biometric features, test its resistance to spoofing attacks using fake fingerprints or facial images.
- **Stress Testing**: Evaluate the system's performance under heavy load conditions to ensure it remains secure and responsive during peak usage.

3. **Effectiveness Testing**:

- **Authentication Accuracy**: Measure the system's accuracy in correctly authenticating legitimate users while rejecting unauthorized access attempts.

- **False Acceptance and False Rejection Rates**: Determine the rates at which the system incorrectly accepts valid passwords (false acceptance) or rejects legitimate users (false rejection).
- **Comparative Analysis**: Compare the performance of graphical password authentication with other authentication methods (e.g., text-based passwords, biometrics) in terms of security and usability.

4. **User Behavior Analysis**:

- **Pattern Analysis**: Analyze users' patterns and behaviors when creating and using graphical passwords to identify common strategies, trends, and preferences.
- **Feedback Collection**: Gather qualitative data through interviews or surveys to understand users' perceptions, attitudes, and concerns regarding graphical password authentication.

5. **Compliance and Standards Testing**:

- Ensure that the graphical password system complies with relevant security standards and guidelines, such as those outlined by NIST (National Institute of Standards and Technology) or ISO (International Organization for Standardization).
- Verify that the system meets legal and regulatory requirements, especially regarding the protection of sensitive user information and data privacy.

By employing these testing methodologies, developers and researchers can gain valuable insights into the strengths and weaknesses of graphical password authentication systems, leading to iterative improvements and better overall security and usability.

CHAPTER- 8
CONCLUSION

In conclusion, graphical password authentication represents a promising and evolving approach to addressing the limitations of traditional text-based passwords. Over the years, extensive research has been conducted to explore various graphical password schemes, evaluate their usability and security, and propose innovative solutions to enhance user authentication.

Graphical passwords offer several advantages, including the potential for increased security by leveraging users' visual memory and reducing vulnerability to dictionary attacks. Moreover, they have the potential to be more user-friendly and intuitive, particularly for individuals who struggle to remember complex alphanumeric passwords.

However, the field of graphical password authentication is not without its challenges. Issues related to predictability, memorability, and the risk of shoulder surfing have raised concerns about the overall security of these systems. Additionally, achieving a balance between security and usability remains a key challenge, as more secure graphical password schemes tend to be less user-friendly, and vice versa.

These problems are the topic of ongoing research efforts aimed at improving graphical password authentication. These initiatives include the creation of hybrid strategies that use biometric or other authenticate elements with graphical passwords, as well as the investigation of novel graphical password methods that more effectively balance both safety and ease of use.

As technology continues to evolve, graphical password authentication is likely to remain a relevant area of study and innovation. With the growing need for robust yet user-friendly authentication methods in an increasingly digital world, the continued exploration of graphical passwords offers the potential to provide secure and accessible solutions for users and organizations alike.

CHAPTER-9

FUTURE WORK

In Future We plan to work in the area of graphical authentication with passwords in the future since it has the potential to significantly improve security, usability, and adaptation to new technologies.

Systems of Hybrid Authentication Examining cutting-edge hybrid strategies that integrate graphical passwords with other authentication elements like biometrics (like fingerprint or face recognition) or behavioural traits (like keystroke dynamics).These hybrid systems can offer increased security while maintaining usabilits.

CHAPTER-10

REFERENCES

1. Title: “graphical password scheme using color login”. Authors: H.Gao proposed paper Published: Journal of Cleaner Production, 2022.
2. Title: Hybrid Textual Authentication Scheme. Authors: M. Sreelatha Published: The International Journal of Web-Based Learning and Teaching Technologies,2020.
3. Title: “Graphical Password Based Authentication Based System for Mobile Systems”. Authors: Er. Aman Kumar, Er. Naveen Bilandi Published: Department of Computer Science and Engineering, DAV University, Jalandhar, Punjab.
4. Title: “Password Authentication Using Text and Colors”. Authors: Miss.SwatiTidke, Miss Nagama Khan, Miss.SwatiBalpande Published: Computer Engineering, RTM nagpur

university, M.I.E.T Bhandara,.

5. Title:, “Graphical Password as an OTP”. Authors: .Veena Rathanavel, Swati Mali Publisher:Department of Computer Engineering, K J Somaiya, College of Engineering

Mumbai. Year:2021

6. Title:, “Color Shuffling Password Based Authentication”. Authors: Aayush Dilipkumar Jain,

Ramkrishna Khetan Krishnakant Dubey, Prof. Harshali Rambade K. Elissa Publisher:Department of Information Technology Vidyalankar Institute of Technology, Mumbai, Year:2017

7. Title:”Towards Reliable Storage of Personal Identification Numbers and Passwords on Smartcards”. Authors: G. R. Blakley, P. D. MacKenzie, and W. D. Mills. Publisher:IEEE

Transactions on Computers. Year:2021

8. Title: ”PassFaces: A User Friendly Graphical Password System”. Authors: D. M. K. Jermyn

A. Mayer, F. Monrose, M. K. Reiter, and A. D. Rubin . Publisher:USENIX Annual Technical Conference. Year:2018

9. Title:”A Decade of Research in Tenacious Passwords: Attacks, Weaknesses, and Future Directions” Authors: C. Biddle, S. Chiasson, and P. C. van Oorschot (2012). Publisher: In ACM Computing Surveys. Year:2019

10. Title:”The Usability and Security of Gestural Passwords”. Authors: K. Jansen and S. Chiasson

. Publisher:ACM Transactions on Computer-Human Interaction (TOCHI) . Year:2020