GRAPHICAL PASSWORD AUTHENTICATION

A DESIGN PROJECT REPORT

Submitted by

BALA VAISHNAVI K

FAHMITHA NASRIN S

KEERTHANA S

SANDHYA SHALINI S.M

in partial fulfilment for the award of the degree

of

BACHELOR OF TECHNOLOGY

IN

ARTIFICIAL INTELLIGENGE AND MACHINE LEARNING

K.RAMAKRISHNAN COLLEGE OF TECHNOLOGY

(An Autonomous Institution, affiliated to Anna University Chennai and Approved by AICTE, New Delhi)

SAMAYAPURAM–621112

NOVEMBER-2024

K.RAMAKRISHNAN COLLEGE OF TECHNOLOGY
(AUTONOMOUS)
SAMAYAPURAM–621112

BONAFIDE CERTIFICATE

Certified that this design project report titled **" GRAPHICAL PASSWORD AUTHENTICATION "** is the bonafide work of **BALA VAISHNAVI K (REG.NO : 811721001004), FAHMITHA NASRIN S (REG.NO : 811721001008), KEERTHANA S (REG.NO : 811721001017), SANDHYA SHALINI S.M (REG.NO : 811721001035)** who carried out the project under my supervision. Certified further, that to the best of my knowledge the work reported here in does not form part of any other project report or dissertation based on which a degree or award was conferred on an earlier occasion on this or any other candidate.

SIGNATURE
Dr.T.AVUDAIAPPAN M.E., Ph.d.,
HEAD OF THE DEPARTMENT
Department of Artificial Intelligence
K.Ramakrishanan College of Technology (Autonomous)
Samayapuram - 621112

SIGNATURE
Mrs.M.A.REETHA JEYARANI M.E.,
SUPERVISOR
Department of Artificial Intelligence
K.Ramakrishnan College of Technology (Autonomous)
Samayapuram - 621112

Submitted for the viva-voce examination held on ……..

INTERNAL EXAMINER **EXTERNAL EXAMINER**

DECLARATION

We jointly declare that the project report on **"GRAPHICAL PASSWORD AUTHENTICATION"** is the result of original work done by us and best of our knowledge, similar work has not been submitted to **"ANNA UNIVERSITY CHENNAI"** for the requirement of Degree of **BACHELOR OF TECHNOLOGY**. This design project report is submitted on the partial fulfilment of the requirement of the award of Degree of **BACHELOR OF TECHNOLOGY**.

SIGNATURE

_____

BALA VAISHNAVI K

_____

FAHMITHA NASRIN S

_____

KEERTHANA S

_____

SANDHYA SHALINI S M

PLACE : SAMAYAPURAM

DATE :

ACKNOWLEDGEMENT

It is with immense pride that we convey our deep gratitude and indebtedness to our esteemed institution, **"K. RAMAKRISHNAN COLLEGE OF TECHNOLOGY (AUTONOMOUS)"** for granting us the privilege to undertake this project.

We take this opportunity to extend our sincere appreciation to the honorable Chairman, **Mr. K. RAMAKRISHNAN B.E.,** for generously providing the necessary facilities throughout our academic journey.

We express our heartfelt thanks to our esteemed Executive Director, **Dr. S. KUPPUSAMY MBA., Ph.D.,** for his continuous support and facilitation of our project, allowing us the requisite time for its successful completion.

Special gratitude goes to our Principal **Dr. N. VASUDEVAN, M.E., Ph.D.,** for affording us the opportunity to shape the project to our utmost satisfaction.

A profound thank you is extended to **Dr. T. AVUDAIAPPAN, M.E., Ph.D.,** Head of the Department (HOD), Department of Artificial Intelligence, for his encouragement and support in the pursuit of this project.

We would like to express my deep and sincere appreciation to our Project Guide, **Mrs. M.A. REETHA JEYARANI, M.E.,** ASSISTANT PROFESSOR, Department of Artificial Intelligence, for his invaluable suggestions, creativity, assistance, and unwavering patience, which served as a constant motivation for the successful execution of the project.

Our sincere thanks are extended to our Project Coordinator, **Mrs. JOANY FRANKLIN, M.E.,** ASSISTANT PROFESSOR, Department of Artificial Intelligence, as well as other faculties and non-teaching staff members for sharing the valuable information during the project.

ABSTRACT

The Graphical Password Authentication System is designed to enhance security by utilizing visual patterns instead of traditional alphanumeric passwords. This system leverages human memory's strength in recalling images, making it more user-friendly and resistant to common password attacks such as brute force or dictionary attacks. Various techniques like click-based, image-based, and hybrid methods are employed to generate secure graphical passwords. The system is resilient against shoulder surfing and reduces the likelihood of users selecting weak passwords. Its usability is improved through familiar interfaces, and it can be integrated into mobile and web applications. With increasing concerns over data breaches, graphical passwords offer a promising alternative to enhance authentication mechanisms.Additionally, the graphical password system promotes a more engaging user experience by allowing users to create unique visual representations of their credentials. This not only enhances memorability but also fosters a sense of personalization in password creation. Furthermore, ongoing research into combining graphical passwords with biometric authentication methods, such as facial recognition or fingerprint scanning, could lead to even more robust security solutions. As cyber threats evolve, this innovative approach to authentication can significantly reduce the risk of unauthorized access, ensuring that sensitive information remains protected. Overall, the adoption of graphical password systems represents a significant step forward in creating secure, user-friendly authentication methods that cater to the needs of modern digital environments.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF ABBREVATION

GUI	Graphical User Interface
CCP	Cued Click Points
GPS	Graphical Password Scheme
SLR	Systematic Literature Review
SSD	Solid State Drive
GPU	Graphics Processing Unit
MFA	Multi-Factor Authentication
DAS	Draw-A-Secret
OTP	One-Time Passcode
UI	User Interface

CHAPTER 1

INTRODUCTION

With increasing technical advancements the world is becoming digital at a high pace and everything is happening online. From paying your bills to ticket bookings to paying the person sitting next to you, you prefer to pay online. Not only payments but all activities, be it, communication through e-mails and messaging apps, keeping your documents in a digital locker, etc happen online. With everything turning online, the risk of cybercrimes and privacy breaches is also increasing. Passwords play a huge role in keeping your data safe online as well as offline platforms. Passwords are the default method of authentication to get access to our accounts. There are various types of authentication available for users to secure their accounts.

Types of authentication :

Token-based authentication includes key cards, bank cards, smart cards, etc.

Knowledge-based authentication includes text-based authentication and picture-based authentication.

Biometric authentication include fingerprints authentication, iris scan and facial recognition.

Considering the traditional username-password authentication, the alphanumeric passwords are either easy to guess or difficult to remember. Also, users generally keep the same passwords for all their accounts because it is difficult to remember a lot of them. Alternative authentication methods, such as biometrics, graphical passwords are used to overcome these problems associated with the traditional username-password authentication technique. In a graphical password authentication system, the user has to

select from images, in a specific order, presented to them in a graphical user interface (GUI). According to a study, the human brain has a greater capability of remembering what they see(pictures) rather than alphanumeric characters. Therefore, graphical passwords overcome the disadvantage of alphanumeric passwords.

1.1 Types of Graphical Passwords

Graphical Password Authentication has three major categories based on the activity they use for authentication of the password:

1. Recognition based Authentication
2. Recall based Authentication
3. Cued Recall

1.1.1 Recognition based Authentication:

A user is given a set of images and he has to identify the image he selected during registration. For example, Passfaces is a graphical password scheme based on recognizing human faces. During password creation, users are given a large set of images to select from. To log in, users have to identify the pre-selected image from the several images presented to him.

1.1.2 Recall based Authentication

A user is asked to reproduce something that he created or selected at the registration stage. For example, in the Passpoint scheme, a user can click any point in an image to create the password and a tolerance around each pixel is calculated. During authentication, the user has to select the points within the tolerance in the correct sequence to login.

1.1.3 Cued Recall

Cued Click Points (CCP) is an alternative to the PassPoints technique. In CCP, users click one point on each image rather than five points on one image (unlike

PassPoints). It offers cued-recall and instantly alerts the users if they make a mistake while entering their latest click-point.

1.2 Background and Motivation

This section explores the shortcomings of text-based passwords, focusing on issues like weak password choices, the necessity of regular updates, and the risks associated with password reuse. It highlights the motivation behind developing alternative systems like graphical passwords that prioritize both security and usability.

1.3 Importance of Graphical Passwords in Modern Authentication

With the rise of mobile devices and the shift toward gesture-based and touch-based interactions, graphical passwords have gained particular importance. This section delves into the role of graphical passwords in mobile environments, where typing complex alphanumeric passwords is often impractical.

1.4 Problem Statement

With the proliferation of digital devices and online services, secure and user-friendly authentication methods are more essential than ever. Traditional alphanumeric passwords, while widely used, often fall short in terms of both security and usability. Users frequently choose weak passwords, reuse them across multiple accounts, and struggle with remembering complex password combinations. These practices increase vulnerability to security breaches, making systems susceptible to brute-force attacks, phishing, and unauthorized access.

Graphical passwords, which leverage images, drawings, and spatial patterns, offer a promising alternative by improving memorability and user experience. However, graphical password systems face unique challenges, including susceptibility to shoulder surfing attacks, predictability in user patterns, and limitations in scalability for large systems. Developing an effective graphical password system that balances security and

usability without compromising either is crucial to advancing authentication technology.

1.5 Aim & Objective

1.5.1 Aim

Graphical password authentication aims to provide an alternative to traditional text-based passwords by using images, patterns, or sequences of images for user identification and access. This method leverages human memory strengths, such as the ability to remember visual information, making it more user-friendly and potentially more secure. By relying on graphical representations, this system seeks to reduce the likelihood of brute-force attacks and password-related vulnerabilities, offering a more intuitive way for users to authenticate their identity.

1.5.2 Objective

This project aims to design, implement, and evaluate a secure graphical password authentication system that is resistant to common security threats while providing a user-friendly experience. The system should:

- Enhance security by minimizing the vulnerabilities of traditional passwords.
- Improve usability by offering an intuitive interface that leverages users' natural ability to remember visual information.
- Address and mitigate challenges associated with graphical passwords, such as shoulder surfing and pattern predictability.

CHAPTER 2
LITERATURE SURVEY

2.1 TITLE : Shoulder Surfing attack in graphical password authentication

AUTHOR : Arash Habibi Lashkari, Samaneh Farmand, Dr. Omar Bin Zakaria, Dr. Rosli Saleh

YEAR OF PUBLICATION : IJCSIS 2009

ABSTRACT : Information and computer security is supported largely by passwords which are the principle part of the authentication process. The most common computer authentication method is to use alphanumerical username and password which has significant drawbacks. To overcome the vulnerabilities of traditional methods, visual or graphical password schemes have been developed as possible alternative solutions to text-based scheme. A potential drawback of graphical password schemes is that they are more vulnerable to shoulder surfing than conventional alphanumeric text passwords. When users input their passwords in a public place an attacker can capture a password by direct observation or by recording the individual's authentication session. This is referred to as shouldersurfing.

MERITS : Enhanced Memorability, Usability Improvement, Reduced Password Reuse, Resistance to Brute-Force Attacks.

DEMERITS : Vulnerability to Shoulder Surfing, Higher Storage Requirements, Complexity in Implementation, Limited Scalability.

2.2 TITLE : Comparison of Graphical Password Authentication Techniques

AUTHOR : Arti Bhanushali, Bhavika Mange, Harshika Vyas, Hetal Bhanushali and Poonam Bhogle

YEAR OF PUBLICATION : IJCA April 2015

ABSTRACT : User Authentication is the most crucial aspect of cyber security. To prevent systems from various types of attacks, password protection to the system is usually provided. The most widely used authentication method using normal text passwords which contains a sequence of alphabets, numbers, and special characters). User mostly tends to choose text passwords which are easy for them to remember (eg. Their birthdate, phone number, etc)... However, even though the technique is user friendly, it is susceptible to many attacks. The other type of Authentication scheme is using Graphical Passwords. These passwords contain images which are easier for humans to remember than the long stream of characters in text passwords. The paper discusses various approaches of using graphical passwords .The basic algorithms of graphical passwords are being compared based on security and usability parameters. User authentication is the heart of security systems. The authentication techniques can be distinguished in three types: knowledge based systems, token based system and biometrics based systems.

Keywords used in this survey paper is Authentication, Graphical password, Security, Attacks, Password space, Password Entropy, Usability.

MERITS : Improved Memorability, Enhanced Usability, Reduced Guessability, Flexibility in Design.

DEMERITS : Security Vulnerabilities, Higher Implementation Costs, Longer Authentication Time, Compatibility Issues.

2.3 TITLE : Graphical Password Authentication

AUTHOR : Towseef Akram, Vakeel Ahmad, Israrul Haq, Monisa Nazir

YEAR OF PUBLICATION : IJCSMC June 2017

ABSTRACT : A graphical password is an authentication system that works by having the user select from images, in a specific order, presented in a graphical user interface (GUI). For this reason, the graphical-password approach is called graphical user authentication (GUA). The most common computer authentication method is to use alphanumerical usernames and passwords. This method has been shown to have significant disadvantages. For e.g, users tend to choose passwords that can be easily guessed. On the other hand, if a password is difficult to guess, then it is often difficult to remember. To overcome this problem of low security, Authentication methods are developed by researchers that use images as password. In this research paper, we conduct a comprehensive survey of the existing graphical password techniques and provide a possible theory of our own. Graphical password schemes have been proposed as a possible alternative to text-based schemes, by the fact that humans can remember pictures better than text; Pictures are generally easier to be remembered or recognized than text.

MERITS : Increased Memorability, Enhanced Security, User-Friendly Interface, Reduced Password Fatigue.

DEMERITS : Vulnerability to Shoulder Surfing, High Storage and Processing Needs, Longer Authentication Time, Compatibility Limitation.

2.4 TITLE : A Systematic Literature Review of Graphical Password Schemes

AUTHOR : Tahmina Islam Shammee, Taslima Akter, Muthmainna Mou, Farida Chowdhury, and Md Sadek Ferdous

YEAR OF PUBLICATION : JCSE December 2020

ABSTRACT : Graphical passwords are an alternative to traditional alphanumeric passwords and can similarly be used to secure online accounts. The widely used alphanumeric passwords have memorability issues and users often find it difficult to memorize a large number of unique passwords. Since 1996, researchers have implemented different graphical password schemes (GPSs) to address such security and usability issues. There are a wide variety of such schemes available. To initiate a study in this domain, it is necessary for a researcher to have a good understanding of the existing research. There are a number of existing review articles, but no systematic literature review (SLR). Additionally, the existing reviews have not covered recent papers. This paper aims to fill in these gaps by reviewing existing GPSs, and intends to address their contributions, limitations, the contexts in which they are used, and the relevant algorithms/techniques. To this end, we conducted an SLR of empirical studies on a number of GPSs published from 1996 to 2019. This article also identifies the security threats that the reviewed schemes are resilient against. A number of schemes have been found to have greater resiliency against different attacks, but not a single scheme is completely resistant to all known attacks.

MERITS : Enhanced Memorability, Improved Usability, Diverse Scheme Options, Resistance to Certain Attacks.

DEMERITS : Incomplete Security Coverage, Higher Resource Demand, Longer Authentication Process, Limited Compatibility and Adoption.

2.5 TITLE : Security Vulnerabilities and Protective Strategies for Graphical Passwords

AUTHOR : Zena Mohammad Saadi, Ahmed T. Sadiq, Omar Z. Akif and Alaa K. Farhan

YEAR OF PUBLICATION : MDPI August 2024

ABSTRACT : As technology advances and develops, the need for strong and simple authentication mechanisms that can help protect data intensifies. The contemporary approach to giving access control is through graphical passwords comprising images, patterns, or graphical items. The objective of this review was to determine the documented security risks that are related to the use of graphical passwords, together with the measures that have been taken to prevent them. The review was intended to present an extensive literature review of the subject matter on graphical password protection and to point toward potential future research directions. Many attacks, such as shoulder surfing attacks, SQL injection attacks, and spyware attacks, can easily exploit the graphical password scheme, which is one of the most widely used. Each of the proposed measures has its pros and cons. This study begins by elucidating some of the graphical password schemes studied between 2012 and 2023, delving into potential threats and defense mechanisms associated with these schemes. Following a thorough identification and selection process, five of the reviewed papers explain the threat of shoulder surfing and spyware attacks on graphical password schemes, while two explain the threat of brute force attacks. One paper focuses on dictionary attacks, while four other papers address social engineering, SQL injection attacks, and guessing attacks as potential threats to graphical password schemes.

MERITS : Enhanced Memorability, Diverse Defensive Strategies, Reduced Brute-Force Susceptibility, Potential for Enhanced Security in Specific Environments.

DEMERITS : Susceptibility to Shoulder Surfing, Vulnerability to Advanced Attacks, Increased Complexity in Security Implementation, Variable Effectiveness of Protective Measures.

CHAPTER 3
SYSTEM SPECIFICATION

3.1 HARDWARE SYSTEM CONFIGURATION

1. Processor:

- **Recommended Specification:** Intel Core i5 or higher, AMD Ryzen 5 or higher.
- **Purpose:** A multi-core processor ensures efficient handling of graphical authentication algorithms, especially if image processing or pattern recognition is involved. Faster processing power reduces authentication time, enhancing the user experience.

2. Memory (RAM):

- **Recommended Specification:** 8 GB RAM minimum, 16 GB preferred.
- **Purpose:** Adequate RAM is essential for processing complex graphical passwords, especially in memory-intensive recognition-based systems that involve large image databases or detailed graphics. It also ensures smooth operation when multiple users access the system concurrently.

3. Storage:

- **Recommended Specification:** Solid State Drive (SSD) with at least 256 GB storage, scalable based on the number of users.
- **Purpose:** SSDs provide faster data retrieval speeds, which reduces loading times for graphical elements in the authentication process. For large-scale applications with numerous image-based passwords, additional storage may be needed to accommodate high-resolution image databases securely.

4.Graphics Processing Unit(GPU):

- **Recommended Specification:** Integrated GPU for basic graphical password applications; Dedicated GPU (e.g., NVIDIA GTX 1650 or higher) for more complex graphical tasks.
- **Purpose:** A GPU is essential if high-resolution image processing or animation-based graphical passwords are used. It enables smooth image rendering and processing of visual data, which is crucial for user-friendly and responsive authentication interfaces.

5.Display:

- **Recommended Specification:** Full HD (1920x1080) or higher resolution display.
- **Purpose:** High-resolution displays improve the visibility of graphical elements, which is critical for accuracy in graphical passwords. This is especially important in systems using complex images or intricate patterns where clarity affects user success.

6.Input Devices:

- **Mouse and Keyboard:** Standard mouse and keyboard are necessary for testing text-based passwords and hybrid systems.
- **Touchscreen (Optional):** If the authentication system is designed for mobile devices or tablets, a touchscreen is essential. It enhances the experience for pattern-based or gesture-based graphical passwords, which rely on tactile interaction.
- **Purpose:** Input devices must be responsive and compatible with the graphical interface to ensure a smooth user experience during authentication. Touchscreens, in particular, are beneficial for systems where gestures or patterns are part of the password.

7.Network Interface:

- **Recommended Specification:** High-speed internet connection (at least 10 Mbps) with support for secure protocols (e.g., TLS/SSL).
- **Purpose:** Network connectivity is crucial for systems where graphical password authentication data is transmitted to a server. It ensures low latency and secure transmission of authentication credentials, especially for cloud-based or multi-user environments.

8.Power Supply and Backup:

- **Recommended Specification:** Uninterruptible Power Supply (UPS) with at least 30 minutes of backup.
- **Purpose:** Ensures continuous operation of the authentication system in case of power interruptions, especially in environments where uptime is critical.

3.2 SOFTWARE SYSTEM CONFIGURATION

1.Operating System:

Windows 10/11, macOS, or Linux (e.g., Ubuntu) for stability and security.

2.Development Environment:

- **Languages**: Python, Java, C++, JavaScript.
- **IDEs**: VS Code, PyCharm, Eclipse for efficient development and debugging.

3.GUI Frameworks:

- **Desktop**: Tkinter, PyQt.
- **Web**: HTML5, CSS3, JavaScript with React or Angular for user-friendly interfaces.

4.Database:

MySQL, PostgreSQL, MongoDB for secure and scalable data storage.

5.Image Processing Libraries:

OpenCV, PIL for handling image recognition and pattern processing.

6.Web Browser:

Google Chrome, Mozilla Firefox, Safari, and Microsoft Edge is essential for accessing the web-based applications.

7.Multi-Factor Authentication(MFA):

Google Authenticator, Authy, or SMS-based OTP to add an extra layer of security by requiring additional verification beyond graphical passwords.

CHAPTER 4
SYSTEM ANALYSIS

4.1 EXISTING SYSTEM :

The existing systems in graphical password authentication can be broadly categorized into three approaches: recognition-based, recall-based, and cued-recall methods. These methods leverage users' visual memory, aiming to improve both security and memorability compared to traditional text-based passwords.

In recognition-based systems, users authenticate by identifying previously selected images from a set of randomly displayed images. During registration, users select specific images—such as faces or symbols—as their password. To authenticate, they must correctly identify these chosen images from a random assortment. Recognition-based systems are user-friendly and easy to navigate; however, they can be vulnerable to shoulder-surfing and observation attacks due to the visual nature of the images. Examples include Passfaces, where users recognize familiar faces, making authentication intuitive but less secure in public settings.

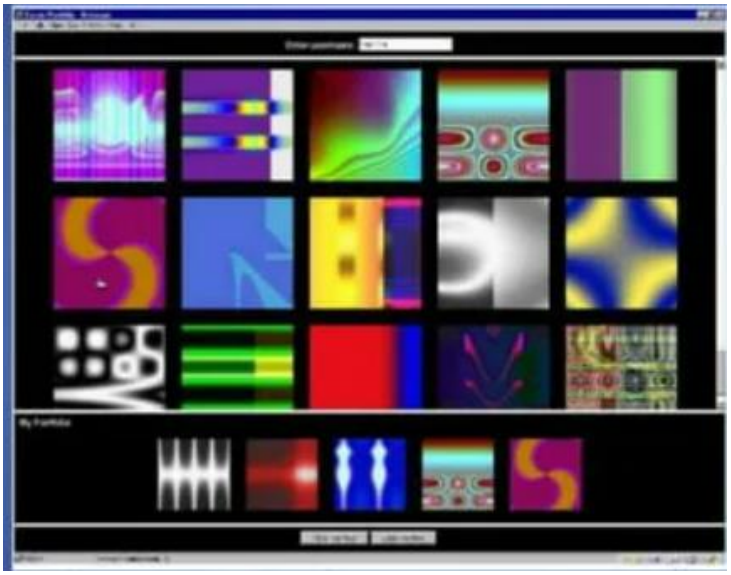

FIG 4.1 Recognition Based System

FIG 4.2 Passfaces

Recall-based systems require users to reproduce a pattern or shape they created during the registration phase. For example, the “Draw-A-Secret” (DAS) system asks users to draw a pattern on a grid, which they later recreate to authenticate. This method leverages users' ability to remember shapes or paths, making it resistant to brute-force attacks. However, complex patterns can be difficult to remember, especially over time, which may affect usability and lead to higher error rates in authentication.

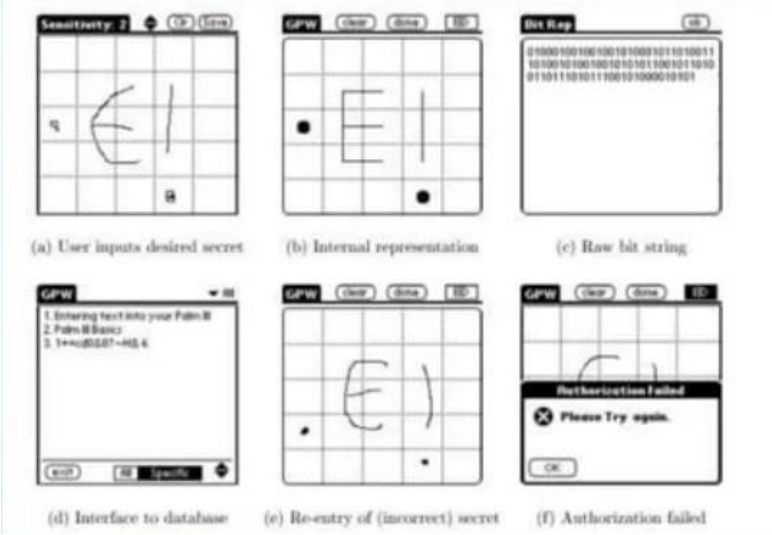

FIG 4.3 Draw a Secret

Cued-recall systems offer users mnemonic cues to assist in recalling their password. A popular example is PassPoints, where users select specific points on an image to form a password, and the image serves as a prompt during login. Cued-recall methods provide a balanced approach to usability and security, but they too are susceptible to attacks like smudge attacks (detecting oily residues on touchscreens) and observation-based attacks.

FIG 4.4 PassPoints

Overall, these existing graphical password systems enhance usability and memorability compared to text passwords but still face challenges in implementation, particularly in balancing security with ease of use.

4.1.1 Drawbacks

1. Vulnerability to Shoulder-Surfing:

Users selecting images in recognition-based systems are prone to observation attacks, where attackers can visually observe and deduce the password.

2. Susceptibility to Smudge Attacks:

In cued-recall systems, users interact with touchscreen devices, which can leave traces of fingerprints or oil marks, allowing attackers to infer the password by inspecting the device.

3. Usability Challenges in Recall-Based Systems:

Users may struggle to remember and accurately reproduce complex patterns or sequences, leading to errors or difficulty in recalling passwords over time.

4. Limited Security in Image Selection:

In recognition-based systems, the number of images from which users select passwords is often limited, reducing the overall complexity and making it easier for attackers to guess passwords.

5. Difficulties in Scaling:

As the number of users or stored graphical passwords increases, maintaining security and performance in the system becomes more challenging, especially for systems relying on large image databases.

6. Complexity in Implementation:

Developing and deploying graphical password systems involves intricate user interface design and image processing, which can increase system complexity and development time.

7. Device Dependency:

Some systems are heavily dependent on specific hardware (e.g., touchscreens for gesture-based passwords), making them less adaptable to different devices or platforms.

8. Cognitive Load:

Users may find it difficult to remember complex images, patterns, or sequences, leading to cognitive fatigue or increased password reset requests.

9. Incompatibility with Low-Resolution Displays:

Graphical passwords may not work well on low-resolution or older display technologies, affecting the accessibility and usability of the system.

10. Lack of Robust Multi-Factor Authentication:

Most graphical password systems do not inherently integrate multi-factor authentication, leaving them potentially vulnerable to phishing or other attacks.

4.2 PROPOSED SYSTEM :

The proposed system for graphical password authentication aims to address the security and usability challenges associated with existing systems. The new approach integrates a hybrid method that combines recognition-based, recall-based, and cued-recall techniques, enhancing both security and user experience. This hybrid method leverages the strengths of each approach while minimizing their individual weaknesses.

In the proposed system, users will first select a set of images during registration, similar to recognition-based methods, but with an added layer of complexity. Instead of merely selecting images, users will be required to interact with these images through a gesture-based approach, such as drawing a specific pattern or tracing an object within the image. This introduces a recall aspect to the process, making it more secure and less prone to shoulder-surfing or observation attacks.

To further enhance security, the system will incorporate dynamic cues during the authentication phase. These cues will prompt users with partial visual clues about their chosen images or patterns, making it easier to recall the password without sacrificing security. For example, users might be shown a part of the image or pattern they selected, which reduces the likelihood of forgetting the password without giving away too much information to an attacker.

Additionally, the system will implement multi-factor authentication (MFA), combining graphical passwords with another authentication method such as fingerprint recognition or one-time passcodes (OTPs). This integration ensures that even if an attacker gains access to a graphical password, they would still need the second authentication factor to complete the login process.

By combining these advanced techniques, the proposed system offers a more secure, user-friendly, and scalable solution for graphical password authentication, overcoming the limitations of existing systems while maintaining ease of use.

4.2.1 Advantages

1. Enhanced Security:

Combines recognition, recall, and cued-recall methods, making it harder for attackers to bypass using observation, shoulder-surfing, or brute-force methods.

2. Reduced Vulnerability to Shoulder-Surfing:

Users interact with images and patterns in a gesture-based manner, reducing the risk of attackers visually observing and deducing passwords.

3. Improved Usability:

The dynamic cues help users recall their graphical passwords without overly complicating the authentication process, balancing security and ease of use.

4. Multi-Factor Authentication (MFA):

Integrates additional layers of security, such as fingerprint recognition or OTPs, ensuring that a single compromised method does not result in unauthorized access.

5. Stronger Protection Against Smudge Attacks:

Gesture-based interaction and dynamic cues make it harder for attackers to infer passwords from oil marks or fingerprints left on touchscreens.

6. Customizable and Flexible:

Users can select personalized images and patterns, providing a more customized and engaging experience compared to traditional text-based passwords.

7. Scalable and Adaptable:

The system can be deployed across various platforms and devices, making it suitable for both desktop and mobile applications with touchscreen or gesture support.

8. Reduces Cognitive Load:

The dynamic cues provide helpful reminders, reducing the mental effort required for users to remember complex passwords, which improves user satisfaction.

9. Better User Engagement:

The inclusion of images and gestures makes the authentication process more interactive, increasing user engagement and reducing password fatigue.

10. Enhanced Password Strength:

By using a combination of multiple methods and customizable elements, the proposed system significantly increases the password complexity, improving overall system security.

CHAPTER 5
ARCHITECTURAL DESIGN

5.1 SYSTEM DESIGN

The system design of the graphical password authentication project emphasizes both security and user convenience. During registration, users choose images and define gesture-based patterns, which are securely stored in an encrypted database. Authentication involves selecting the correct images and replicating the patterns, with dynamic cues to aid memory without compromising security. Multi-factor authentication (MFA) adds an extra layer of protection, requiring secondary verification methods such as fingerprint scanning or OTPs. The intuitive user interface ensures ease of use across various devices. Additionally, error handling and password recovery features provide seamless access while maintaining strong security standards throughout the system.

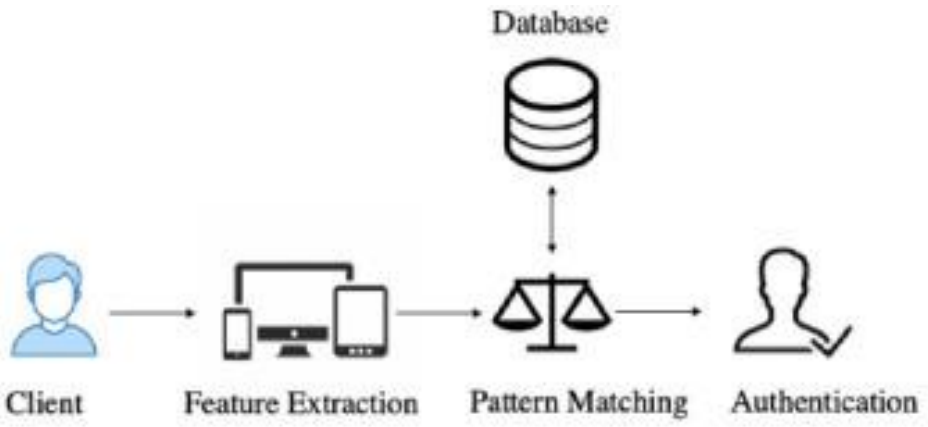

FIG 5.1 System Architecture

5.2 DATA FLOW DIGRAM

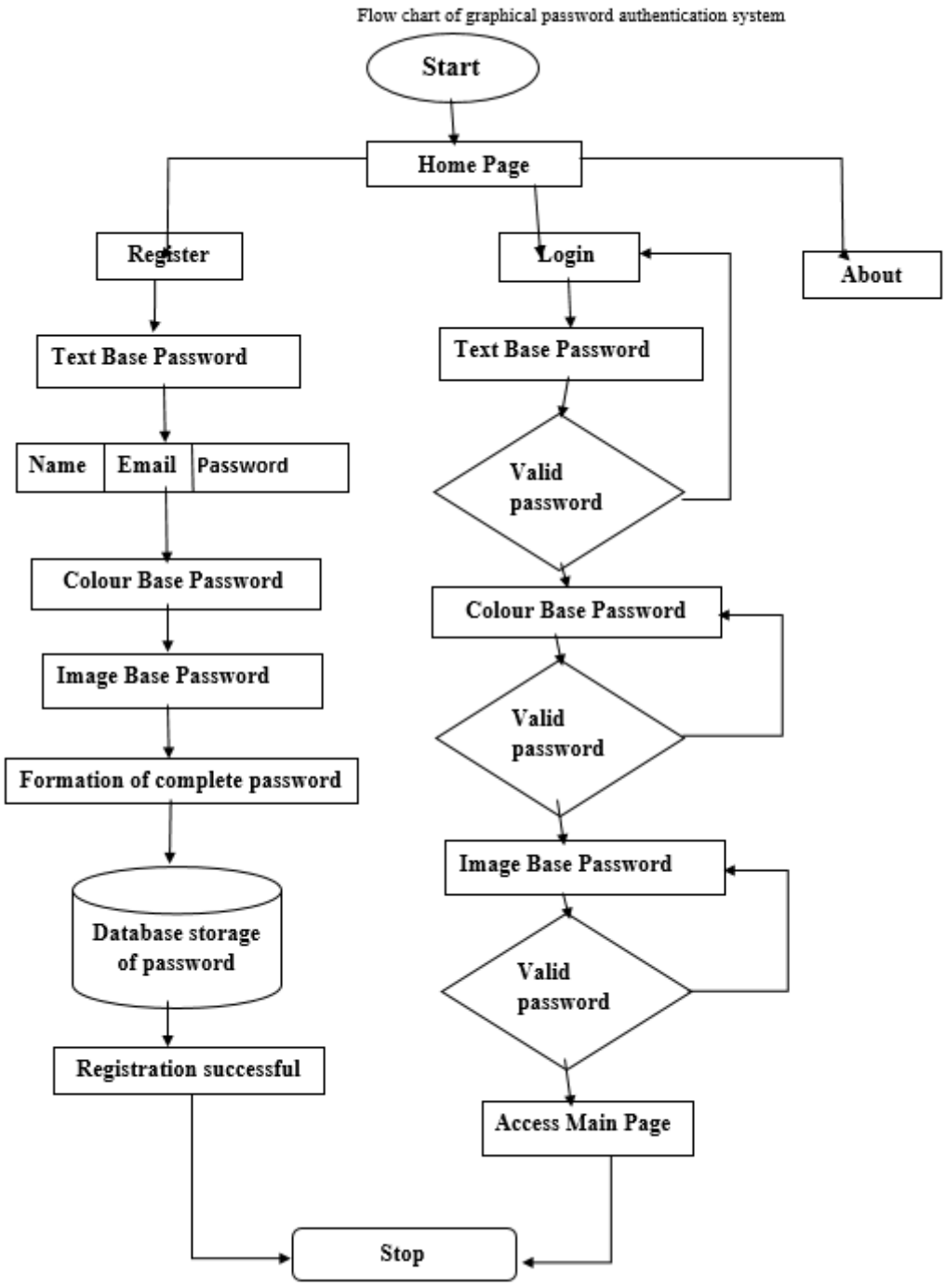

FIG 5.2 Data Flow Diagram

5.3 USE CASE DIAGRAM

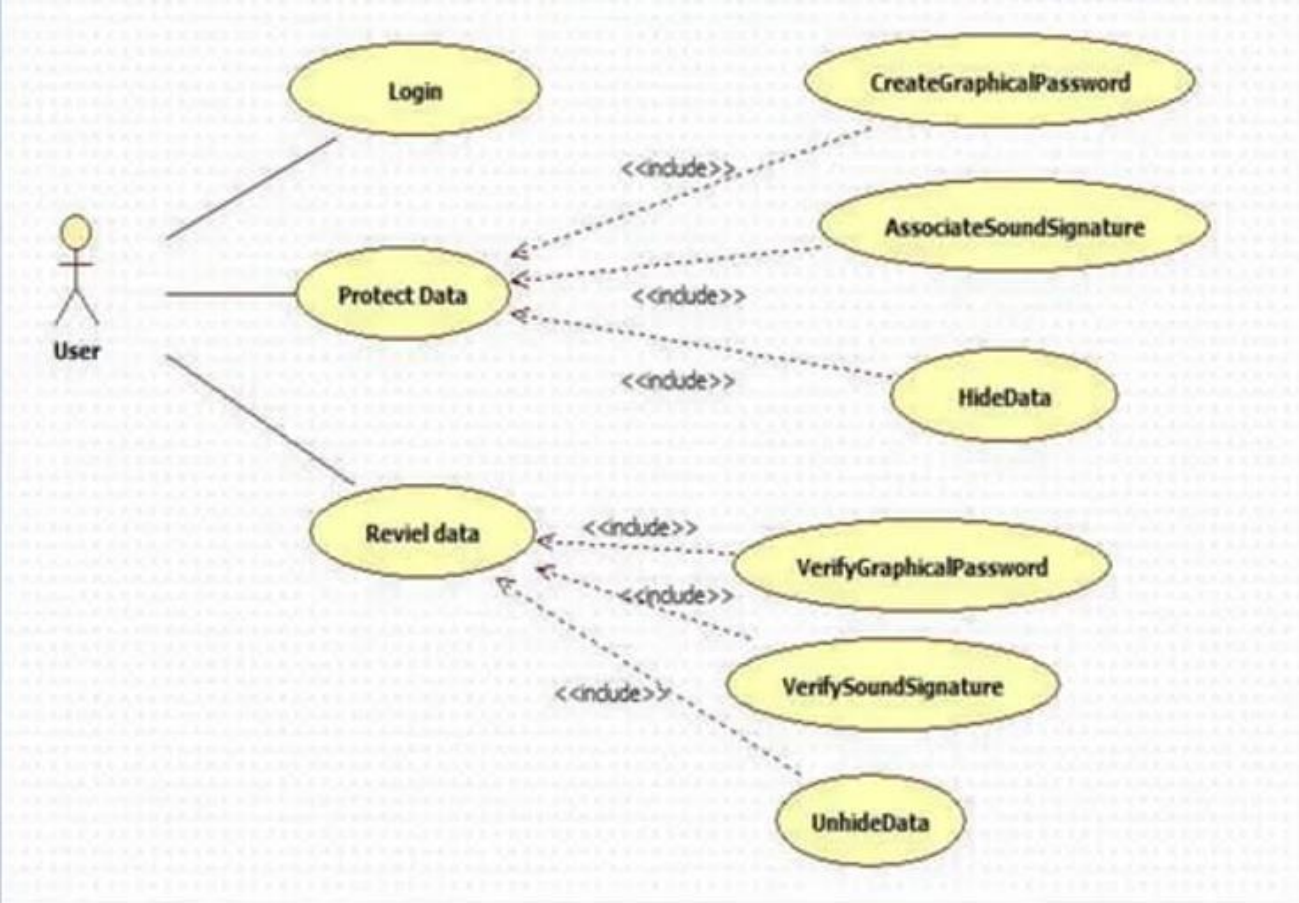

FIG 5.3 Use Case Diagram

5.4 ACTIVITY DIAGRAM

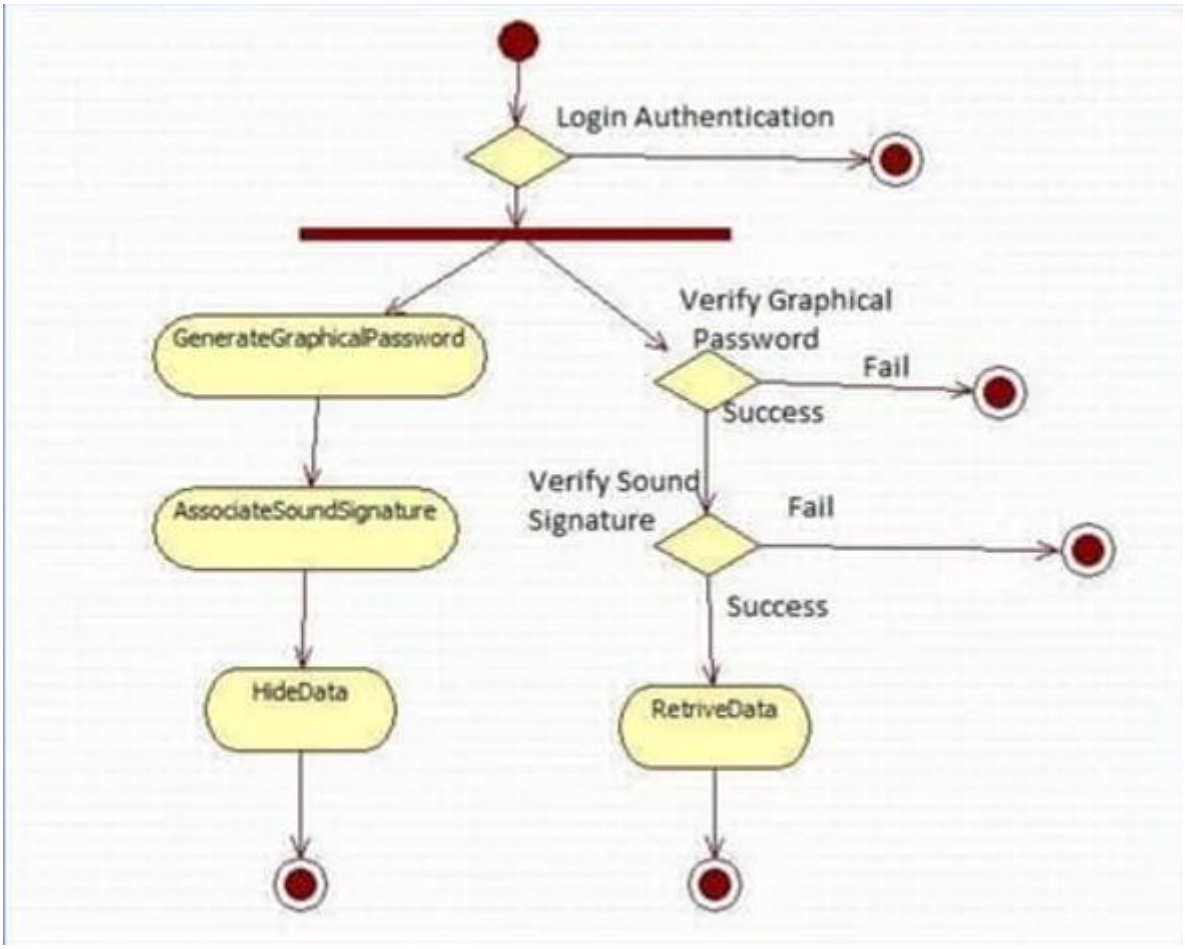

FIG 5.4 Activity Diagram

5.5 SEQUENCE DIAGRAM

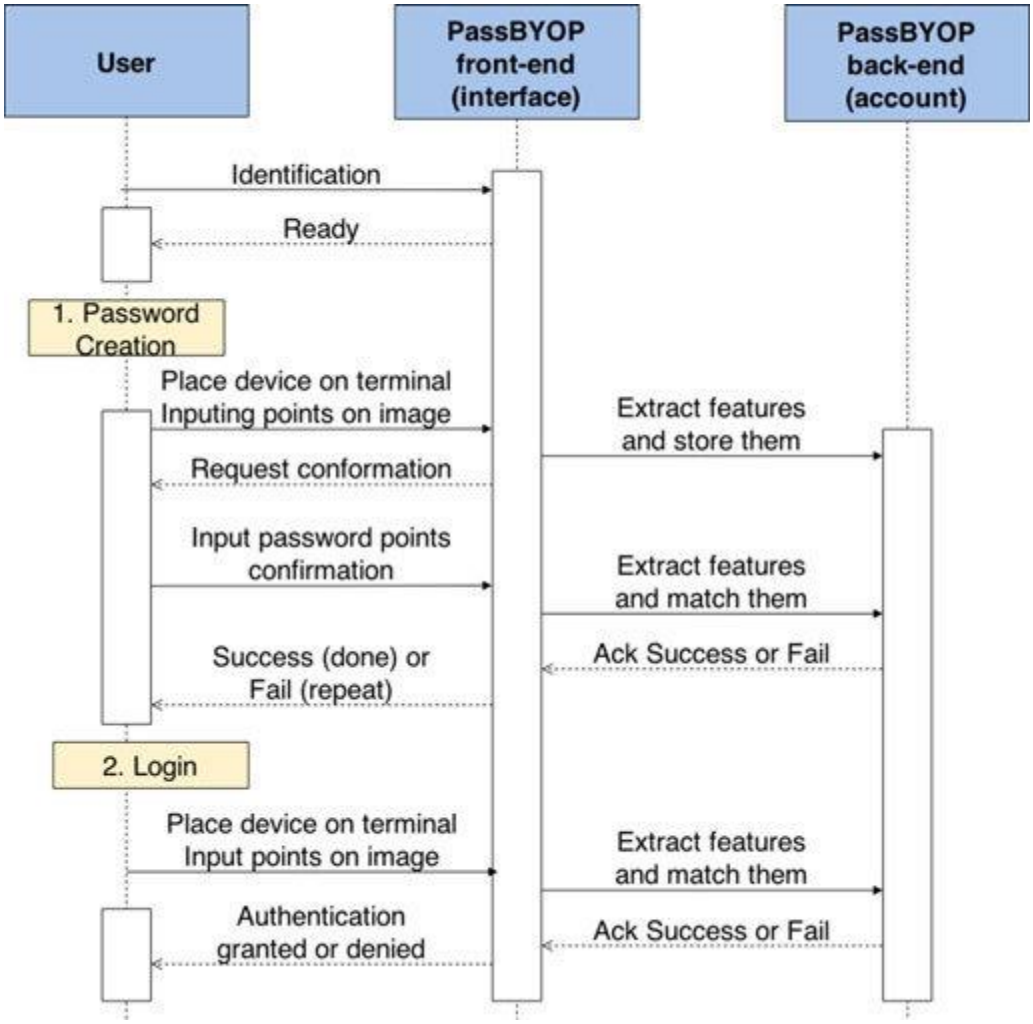

FIG 5.5 Sequence Diagram

CHAPTER 6
MODULES DESCRIPTION

6.1 MODULES

6.1.1 Registration Module:

Users create their graphical password by selecting images and defining gesture-based patterns. This data is securely stored in the database with encryption to protect user credentials.

6.1.2 Authentication Module:

Verifies the user's identity by asking them to select the correct images and replicate their gesture-based pattern. The system checks the entered data against stored credentials to grant or deny access.

6.1.3 Image Selection and Interaction Module:

Facilitates the selection of password images and incorporates gesture-based interactions, such as drawing or tracing patterns on the image to enhance password complexity.

6.1.4 Dynamic Cue Generation Module:

During authentication, this module provides partial visual cues or hints to assist users in recalling their password without compromising security, offering guidance without revealing full details.

6.1.5 Multi-Factor Authentication (MFA) Module:

Adds an extra layer of security by requiring users to authenticate via a second method, such as biometric verification (fingerprint) or a one-time password (OTP), alongside the graphical password.

6.1.6 Database Management Module:

Securely stores user credentials (images and patterns) using encryption techniques. The module also handles user session data and login attempts to maintain security and prevent unauthorized access.

6.1.7 Security Module:

Protects user data with encryption and hashing, defends against brute-force attacks, and detects smudge attacks (fingerprint traces on touchscreens) to ensure strong security during authentication.

6.1.8 Error Handling and Feedback Module:

Provides real-time error messages if authentication fails, guiding users to correct mistakes. It also handles account lockouts and helps users recover from errors securely.

6.1.9 User Interface (UI) Module:

Manages the design and layout of the authentication system, ensuring an intuitive, responsive experience across various devices (desktop, tablet, mobile), and supporting image selection and pattern drawing.

6.1.10 Backup and Recovery Module:

Provides recovery options for forgotten passwords, such as secondary authentication methods (biometrics or OTP). It ensures users can regain access securely without being locked out of their accounts.

CHAPTER 7

IMPLEMENTATION

7.1 System Architecture and Design

7.1.1. Overview of the Graphical Password System:

A graphical password is an authentication method that replaces traditional alphanumeric passwords with images or graphical elements. Instead of typing a password, users are required to select or interact with a series of images, regions of images, or graphical patterns in a specific sequence. The idea is that graphical passwords can be easier to remember and potentially more secure than text-based passwords, as they leverage the human ability to recognize and recall images or patterns.

7.1.2. System Architecture:

- **Client-side:** This includes the graphical user interface (GUI), where users can interact with images and select their password.
- **Server-side:** The backend, which stores the user credentials and handles authentication requests.

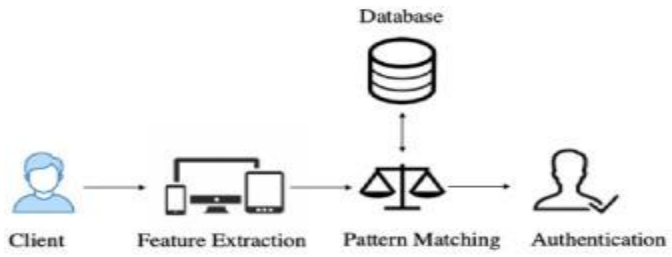

FIG 7.1 System Architectre

7.1.3. Technologies Used:

- **Programming Language**: Python
- **Libraries**:
    a) **Tkinter** (for GUI and canvas drawing)
    b) **hashlib** or **bcrypt** (for password hashing and security)
    c) **messagebox** (for pop-up messages)
- **Database**:
- **MySQL** or **MongoDB** (for storing user data and passwords securely)

7.2 System Flow

7.2.1 User Registration Process:

- Canvas Interaction: Users select points or images for their password.
- Password Storage: The selected password is hashed (for security) and stored.
- Confirmation: Users confirm their password by re-entering it.
- Database Storage: Password and user data are stored securely in a database.
- Final Confirmation: The system confirms successful registration and informs the user

7.2.2. Login/Authentication Process:

- Canvas Interaction: Users draw or select points/images to enter their password.
- Password Verification: The entered password (or its hash) is compared to the stored password.
- Authentication Result: If the password matches, the user is authenticated. Otherwise, an error is shown, and the user can retry.

7.3 Screenshots and Visual Representation

7.3.1 Login Screen:

The login screen will display an image grid, where users will select images (or spots) as part of their graphical password. The selected images will be stored as part of their password, and during login, users will be asked to repeat the selection to authenticate.

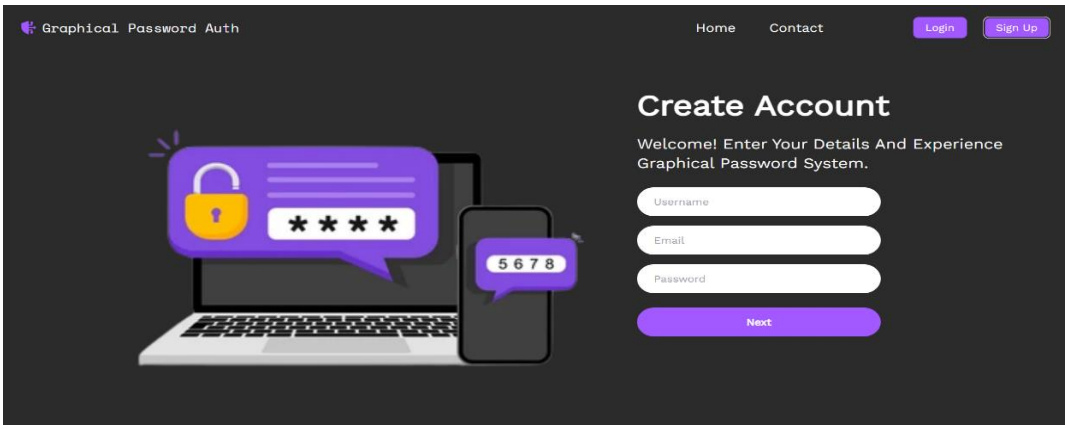

FIG 7.2 Login page

7.3.2 Password Creation:

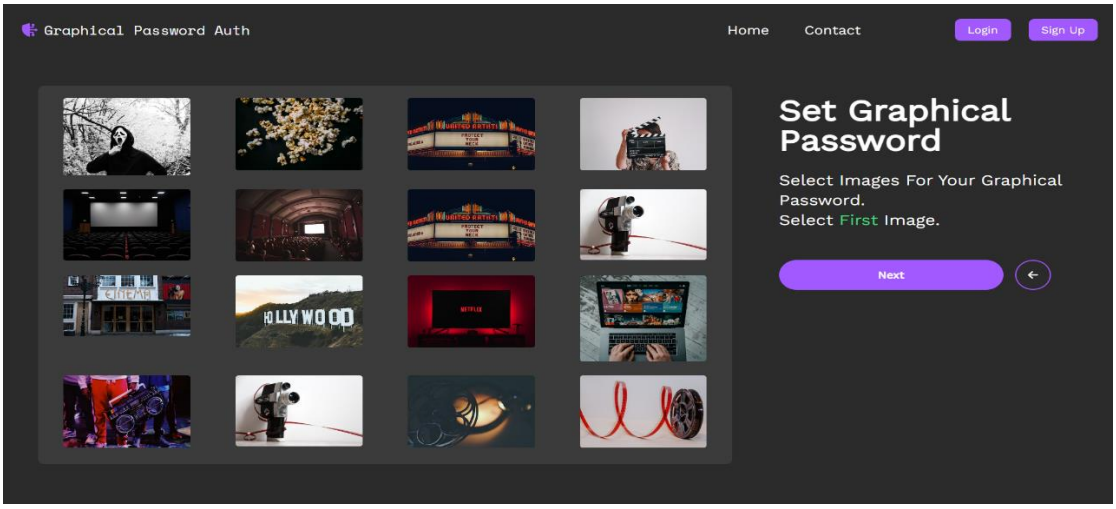

FIG 7.3 Password Creation

7.3.3 Successful/Failed Login:

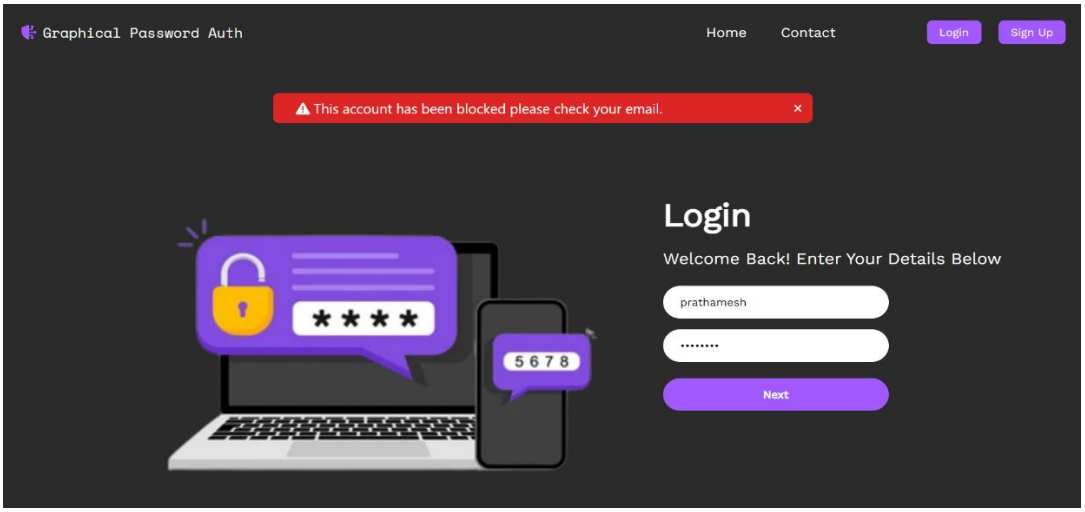

FIG 7.3 Account Blocked

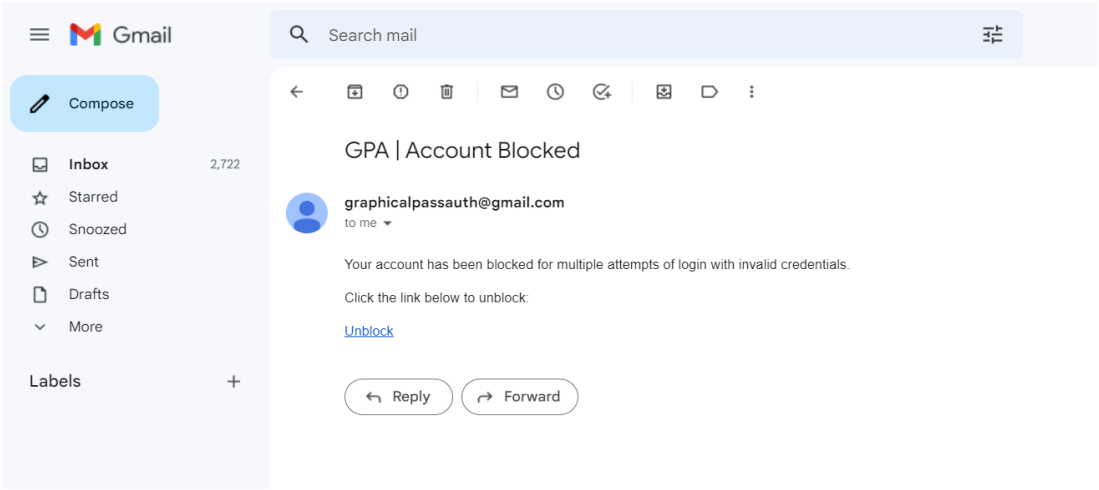

FIG 7.4 Notification Email

CHAPTER 8

CONCLUSION AND FUTURE OUTLOOK

8.1 CONCLUSION

Graphical Password Authentication is an innovative approach to securing user accounts by using visual patterns, images, or drawings instead of traditional alphanumeric passwords. The primary advantage of this system lies in its ability to leverage the natural human ability to remember images or graphical patterns, as opposed to relying on complex and often hard-to-remember text-based passwords.

Throughout the development and implementation of this system, several benefits and challenges were identified. One of the most prominent advantages of graphical password systems is the ease with which users can recall visual patterns compared to numeric or alphabetic strings. Furthermore, graphical passwords have been found to be more resilient against traditional attacks such as brute force, dictionary, or phishing attacks, especially when combined with advanced techniques like image grids or drawn patterns.

The graphical password system also improves usability, as it often requires fewer cognitive resources for the user to create and recall the password. This aspect makes the system more accessible to users of varying technical backgrounds, thus enhancing its potential for widespread adoption.

However, despite its benefits, the graphical password system is not without its challenges. The complexity of the graphical password can be a double-edged sword; while more intricate patterns offer enhanced security, they may also become burdensome to recall over time, leading to potential usability issues. Furthermore, concerns regarding shoulder surfing and other forms of observation attacks are still

relevant, as users may be vulnerable to having their graphical passwords captured by a third party.

In the context of the overall security landscape, graphical passwords offer an exciting alternative to traditional authentication methods. When combined with additional security layers such as multi-factor authentication (MFA) or biometric recognition, graphical passwords could become a vital part of the future of secure authentication systems, offering both ease of use and robust protection.

8.2 FUTURE OUTLOOK

The future scope of graphical password authentication is vast, and there are numerous avenues for improvement and exploration. As technology advances, graphical password systems can evolve to meet emerging security challenges while enhancing user experience.

- **Integration with Multi-Factor Authentication (MFA):** The integration of graphical passwords with multi-factor authentication (MFA) can enhance security by adding an extra layer of protection. For example, after the user enters a valid graphical password, they could be required to authenticate via a second factor, such as a one-time password (OTP) sent to their mobile device or biometric authentication (fingerprint or facial recognition). This would significantly reduce the likelihood of unauthorized access.
- **Adaptive Password Systems:** In the future, graphical password systems could become more adaptive, adjusting the difficulty level of the password based on the context. For example, based on the sensitivity of the application or the user's history, the system might offer more complex password options or employ dynamic image grids that change periodically to keep the password secure.
- **Biometric and Gesture-Based Authentication:** Another exciting development is the integration of biometric data into graphical password systems. Future graphical passwords could combine images with biometric features, such as

recognizing a user's unique gesture or drawing style. This would not only make the system more secure but also further enhance the user experience by allowing for natural, intuitive interaction with the system.

- **Mobile and Touchscreen Integration:** With the widespread use of mobile devices and touchscreen technology, graphical password systems will be able to take advantage of these devices' capabilities. Touchscreen devices can allow users to draw their passwords directly on the screen, making the system even more user-friendly. Further developments could introduce gesture recognition as part of the authentication process, where users can swipe, tap, or draw specific patterns to authenticate.
- **Gamification and User Engagement:** To address the issue of user fatigue with graphical passwords, the concept could be gamified to make password creation and recall a more engaging process. This could involve incorporating game-like elements where users perform actions like drawing patterns, solving visual puzzles, or interacting with virtual objects to form a password. This would not only increase security but also make the system more enjoyable, thus encouraging regular use.
- **Artificial Intelligence (AI) for Enhanced Security:** The use of artificial intelligence (AI) could be a game-changer for graphical password authentication. AI could be used to detect unusual patterns in how users draw or interact with the graphical password system, potentially identifying and flagging suspicious activity. Additionally, AI can be used to help generate more secure and unpredictable graphical passwords based on user behavior or environmental factors.
- **Cross-Platform Security:** As more applications and services move to the cloud and become cross-platform, graphical password systems must evolve to work seamlessly across various devices and platforms. Whether on a desktop, mobile device, or wearable, graphical passwords should remain consistent and secure. Future developments could focus on cloud-based password storage and

synchronization, allowing users to authenticate themselves across all their devices without compromising security.

- **Usability Improvements:** While graphical passwords are already more user-friendly than traditional alphanumeric passwords, there is still room for improvement. Future systems could incorporate better visual cues, such as highlighting or zooming in on selected points, making the authentication process even more intuitive. Additionally, machine learning could help in refining the user experience by analyzing user preferences and providing personalized guidance during the password creation and recall process.
- **Behavioral Biometrics:** Future systems could combine graphical password systems with behavioral biometrics, which track the user's unique interaction patterns with the system. This could include monitoring how a user draws the password (e.g., speed, pressure, angle) or how they interact with images. This data can provide an additional layer of security, making it harder for unauthorized users to replicate the behavior.

APPENDIX

A1. SAMPLE CODE

```
import tkinter as tk
from tkinter import messagebox
class GraphicalPasswordAuth:
    def _init_(self, master):
        self.master = master
        self.master.title("Graphical Password Authentication")
        self.master.geometry("400x300")

        self.password = "1234"  # Set your password here
        self.canvas = tk.Canvas(self.master, width=400, height=300)
        self.canvas.pack()

        self.canvas.create_text(200, 50, text="Draw your password", font=("Helvetica",
16))

        self.canvas.bind("<Button-1>", self.start_line)
        self.canvas.bind("<B1-Motion>", self.draw_line)

        self.line_start = None
        self.line_end = None
        self.user_password = ""

    def start_line(self, event):
        self.line_start = (event.x, event.y)
    def draw_line(self, event):
        if self.line_start:
```

```
            self.canvas.delete("line")
            self.line_end = (event.x, event.y)
            self.canvas.create_line(self.line_start[0], self.line_start[1], self.line_end[0],
self.line_end[1],
                                    fill="blue", width=5, tags="line")
            self.line_start = self.line_end
    def authenticate_password(self):
        if self.user_password == self.password:
            messagebox.showinfo("Success", "Authentication successful!")
        else:
            messagebox.showerror("Error", "Authentication failed. Try again.")
            self.canvas.delete("line")
            self.user_password = ""
    def submit_password(self):
        self.master.bind("<Return>", lambda event: self.authenticate_password())
    def add_point(self, event):
        self.user_password += str(event.x) + "," + str(event.y) + ","
        print(self.user_password)
if _name_ == "_main_":
    root = tk.Tk()
    app = GraphicalPasswordAuth(root)
    app.submit_password()
    root.mainloop()
```

REFERENCES

[1] Rachna Dhamija and Adrian Perrig, "Deja Vu: A User Study. Using Images for Authentication" In Proceedings of the 9th USENIX Security Symposium, August 2000.

[2] Authentication:http://www.objs.com/survey/authent.htm

[3] Patric Elftmann, Diploma Thesis, "Secure Alternatives to Password-Based Authentication Mechanisms" Aachen, Germany October 2006.

[4] G. E. Blonder Graphical password, U.S. Patent 5559961, Lucent Technologies, Inc. (Murray Hill, NJ), August 1995.

[5] Approaches to Authentication: http://www.e.govt.nz/plone/archive/services/see/see-pki-paper/chapter6.html?q=archive/services/see/see-pki-paper-3/chapter6.html

[6] Ali Mohamed Eljetlawi, Norafida Ithnin. "Graphical password: comprehensive study of the usability features of the recognition base graphical password methods," Third 2008 International Conference on Convergence and Hybrid Information Technology. 1137-1143. 2008

[7] S. Wiedenbeck, J. Waters, J. C. Birget, A. Brodskiy, and N. Memon, "Authentication Using Graphical Passwords: Basic Results", In Human-Computer Interaction International (HCII 2005), Las Vegas, NV, 2005.

[8] "Persuasive Cued Click Point: Design, Implementation and Evaluation of a Knowledge-Based Authentication Mechanism", Sonia Chiasson, Member, IEEE, Elizabeth Stobert ,Student Member, IEEE Alain Forget, Robert Biddle, Member, IEEE, and Paul C, van Oorschot, Member, IEEE.

[9] Wiedenbeck, S., Waters, J., Birget, J.C., Broditskiy, A., & Memon, N. (2005). Pass Points: Design and evaluation of a graphical password system. Submitted

[10] X. Suo, “A design and analysis of graphical password”, Master's thesis, College of Arts and Science, Georgia State University, August 2006

[11] A.Perrig and D.Song, “Hash Visualization: A New Technique to improve Real-World Security”. In International Workshop on Cryptographic Techniques and E-Commerce, pages 131--138, 1999.

[12] S. Man, D. Hong, and M. Mathews,”A shoulder surfing resistant graphical password scheme", In Proceedings of International conference on security and management. Las Vegas, NV, 2003.

[13] Xiayuan Suo, YingZhu, G. Scott. Owen, “Graphical Passwords: A Survey”, In Proceedings of Annual Computer Security Applications Conference, 2005.

[14] Hafiz Zahid Ullah Khan, “Comparative Study of Authentication Techniques”, International Journal of Video & Image Processing and Network Security IJVIPNS Vol: 10 No: 04.

[15] Wing Ho Leung and Tsuhan Chen, “Hierarchical Matching For Retrieval of Hand Drawn Sketches”, In Proceeding of International Conference on Multimedia and Expo –Volume 2(Icme‟03), 2003