**CHAPTER 1**

# INTRODUCTION

## 1.1 Abstract

The traditional text-based authentication systems, such as password or PIN entry, are increasingly vulnerable to attacks like phishing, brute-force attempts, and social engineering. In response to these limitations, graphical-based authentication systems have gained attention as a more secure and user-friendly alternative. This Graphics Based Parser Authentication System (GPAS) proposes an Authentication System that leverages visual patterns and images for user verification, making it more resistant to common attack vectors and enhancing usability

As we know that our human brain can easily store or recall an image or image-based password. So, we propose graphical password for users to register randomly with high secured passwords and there is no difficulty to recall the graphical password. Authentication is a data access point that manages consumer security assurance.

In addition, scientist is saying that it’s easy to remembered a picture for human brain than text. The human brain can easily process visuals and visuals-based passwords, it is resistant to dictionary attack, keylogger, social engineering etc. Alphanumeric password is an old traditional common authentication method.

Practically this traditional method is too unsecure system. For example, attacker may easily guess user’s password unless it is not very special password. These are all unsecure characteristic for normal users and authentication is one of the important security points where user has active responsibility for their personal information security. Generally graphical password techniques are two types: recognition-base and recall based graphical techniques. In recognition-based techniques. User has to authenticated by choosing one or more visuals that are selected during the registration time. In recall-based techniques is a process that user has to remember that was done during registration time.

ST. PHILOMENA’S COLLEGE, MYSORE 1

## 1.2 Introduction to System

The GBPAS introduces a new authentication method where users are required to interact with a graphical interface, parsing predefined visual elements such as RGB shapes, colors, and spatial relationships to authenticate themselves. The system utilizes a combination of image segmentation, pattern recognition and user behavior analysis, ensuring that each authentication session is unique and difficult to replicate by unauthorized parties. The user’s interaction with the graphics serves as a multi-factor authentication (MFA) layer, integrating cognitive and behavioral patterns into the security process.

The proposed system uses visual parsing algorithms to convert graphical inputs into unique user profiles, which are then compared to stored templates. The integration of machine patterns techniques allows the system to improve over time, detecting anomalies in user behavior and adapting to different usage patterns. Moreover, the visual nature of the authentication process makes it more intuitive and engaging, leading to a reduction in user error rates and improved overall user experience.

This approach aims to enhance security by eliminating reliance on traditional password-based systems, offering a more robust solution against common attack methods, while also providing a more accessible and user-friendly authentication method. The system's potential for application spans across various domains, from online banking to mobile device access, and can be implemented in both low and high-security environments.

Through this innovative combination of graphics, pattern learning, and parsing techniques, the GPAS System offers a promising step forward in user authentication, balancing both security and convenience.

ST. PHILOMENA’S COLLEGE, MYSORE 2

# CHAPTER 2

# LITERATURE SURVEY

A literature survey or a literature review in a project report shows the various analyses and research made in the field of interest and the results already published, taking into account the various parameters of the project and the extent of the project.

A literature survey includes the following:

* Existing theories about the topic which are accepted universally.
* Books written on the topic, both generic and specific.
* Research done in the field usually in the order of oldest to latest.
* Challenges being faced and on-going work, if available.

Literature survey describes about the existing work on the given project. It deals with the problem associated with the existing system and also gives user a clear knowledge on how to deal with the existing problems and how to provide solution to the existing problems.

## 2.1 Survey Papers

**[1] Title: Recognition-Based Graphical Password Algorithms**

Year:2020

Author: Jiya Gloria Kaka; Oyefolahan O. Ishaq; Joseph O. Ojeniyi

**ABSTRACT:** User Authentication is an important aspect of information security. Alphanumeric passwords are the most common and widely adopted means of user authentication. Nevertheless, there are several disadvantages attached to the alphanumeric forms of authentication. Example, users choose passwords that are easy to guess (dates of births, their names, car plate number) in other to remember them, because difficult passwords are not easily remembered. This brought about the alternative of graphical passwords because research have been carried out to proof that humans find it easier to recall images. This paper reviews 10 recognition-based graphical password algorithms, and the common usability and security threats of these systems based on these algorithms were analyzed. This paper also suggests future research directions.

### [2] Title: A Captcha-Based Graphical Password with Strong Password Space and Usability Study

Publisher: IEEE

Year: 2021

Author: Altaf Khan; Alexander G. Chefranov

**ABSTRACT:** Security for authentication is required to give a superlative secure users' personal information. This paper presents a model of the Graphical password scheme under the impact of security and ease of use for user authentication. We integrate the concept of recognition with re-called and cued-recall based schemes to offer superior security compared to existing schemes. Click Symbols (CS) Alphabet combine into one entity: Alphanumeric (A) and Visual (V) symbols (CS-AV) is Captcha-based password scheme, we integrate it with recall-based n ×n grid points, where a user can draw the shape or pattern by the intersection of the grid points as a way to enter a graphical password. Next scheme, the combination of CSAV with grid cells allows very large password space (2.4 ×10 4 bits of entropy) and provides reasonable usability results by determining an empirical study of memorable password space. Proposed schemes support most applicable platform for input devices and promising strong resistance to shoulder surfing attacks on a mobile device which can be occurred during unlocking (pattern) the smartphone.

### [3] Title: Enhancement of Password Authentication System Using Vector (Graphical) Images

Publisher: IEEE

Year: 2023

Author: Karan Pandey; Amitesh Singh; Ashutosh Anand; Abhishek Kaushik; Shiv Narain Gupta

**ABSTRACT:**  In this paper, an improved password authentication system using images is presented. This research data focuses primarily on the concept of graphical password systems using vector images. This is supported by using persuasive queued click points for authentication purposes. The basic concept of this system is that the user manipulates a sequence of images. The underlying goal of this system is to attain higher security in a simpler manner that is easy for the user to use and harder for hackers to guess. This vector-based authentication system is the best alternative for text passwords. With the help of Persuasive Cued Click Point (PCCP), we will be able to make it more secure. PCCP is a combination of click points on five specific images. Persuasive cued click points are click points on an image that appear one after the other in random or sequential order. Persuasive clicked points provide a series of images, thus giving intruders more work and improving security. In this essay, PCCP is merged using modern innovations like mobile devices and email.

## 2.2 Existing System

Existing authentication systems are designed to verify the identity of a user before granting access to sensitive information or systems. The core principle behind these systems is to ensure that the user is attempting to access a system that is authorized:

* Password-Based Authentication is the most common and widely recognized traditional method of verifying user identity. This system relies on users choosing a secret word or phrase (the password), which they must input to gain access to a system, application, or service.

* PIN-Based Authentication (Personal Identification Number) involves the use of a short numeric code that a user must enter to authenticate themselves. PINs are typically shorter than passwords, consisting of 4 to 6 digits.

* Security Questions involve asking the user to answer a set of predefined questions, often chosen by the user when creating an account. These questions typically involve personal information, such as the user’s mother's maiden name, the name of their first pet, or the name of their high school.

**Disadvantages Of Existing System:**

* Limited Memorability: While traditional passwords may be easier to guess with brute-force attacks and they can be challenging for shorter pins, especially if users struggle with spatial memory, this can lead to forgotten passwords and potential usability issues.
* Susceptibility to Shoulder Surfing: Depending on the design of the passwords, users may inadvertently reveal their password patterns to shoulder surfers while inputting their passwords. This can compromise security and increase the risk of unauthorized access.

* Complexity of Creation: Creating a strong and secure password may require more effort and thought than creating a text-based password. Users may find challenging to generate complex passwords or select memorable passwords with compromising security.

* User Training and Support: Users may require additional training and support to understand how to create, remember, and securely use passwords effectively. Without proper education and guidance, users may struggle to use the system correctly, leading to security risks and usability issues.

## 2.3 Proposed System

The Graphics Based Parser Authentication System (GPAS) as a proposed system aims to combine advanced security measures with user-friendly features, providing a highly secure and intuitive authentication method for various platforms and devices. The system leverages graphical patterns or images as the core mechanism for password creation and verification.

**Advantages Of Proposed System (Objectives):**

* Usability: GPAS can be more user-friendly, especially for users with spatial memory loss, remembering complex alphanumeric passwords. The process of visuals or selecting patterns may feel more intuitive and natural than traditional passwords.

* Implementation complexity: Implementing cued image-based passwords requires additional functionality to store, present, and verify cues associated with each image, adding secured complexity to the authentication system
* Enhanced Memorability: By associating visuals with personal cues or hints, users are more likely to remember their passwords, reducing the risk of resetting the passwords.

* Resistance to Dictionary Attacks: Graphical passwords are less susceptible to dictionary attacks, where attackers use precomputed lists of common passwords or phrases to guess user credentials. Since graphical passwords are not based on words or phrases, they add an extra layer of complexity for attackers

* Potential for Increased Security: Depending on the implementation, visual-based passwords may offer additional security features such as the requirement to select visual in a specific sequence or to interact with specific areas within the visual.

# CHAPTER 3 SYSTEM ANALYSIS

## 3.1 Feasibility Study

In this phase, we conduct a comprehensive analysis to assess the feasibility of the project and develop a business proposal that outlines a general plan and cost estimates. The primary objective during the system analysis stage is to evaluate the feasibility of the proposed system and ensure it does not impose an undue burden on the company.

Conducting a feasibility analysis involves gaining a clear understanding of the major system requirements. This step is crucial in determining whether the proposed system aligns with the company's capabilities and resources. By carefully assessing the feasibility, we can evaluate the project's viability and make informed decisions regarding its implementation.

During the feasibility analysis, various factors such as technical, economic, operational, and scheduling considerations are taken into account. These factors help us determine the system's practicality and its potential impact on the company's operations and resources.

### 3.1.1 Technical Feasibility

The technical feasibility study aims to evaluate the system's technical requirements. It is essential that the system does not place excessive demands on the available technical resources, which could strain the client. To ensure technical feasibility, the developed system has been designed with modest resource requirements. Implementation of this system would necessitate minimal or no significant changes, minimizing disruptions and resource constraints.

* **System Design**: Graphical authentication systems can be categorized into:
  + Recognition-Based Authentication: Users identify pre-selected images from a set during login
  + Recall-Based Authentication: Users reproduce a pattern or select images in a specific sequence.
* **Implementation Considerations**:
  + Platform Compatibility: Ensure the system is compatible across various platforms (web, mobile, desktop).
  + Technology Stack: Utilize technologies such as HTML5 Canvas, JavaScript, and secure backend frameworks.
  + Security Measures: Implement data encryption, secure image storage, and protection against attacks like shoulder surfing.

### 3.1.2 Economic Feasibility

The economic feasibility of implementing a Graphics Based Parser Authentication System involves evaluating both the initial development costs and ongoing maintenance expenses against the potential long-term benefits.

* **Development Costs**: Initial development costs include software development, graphical user interface design, system integration, and security implementation. these costs depend on the complexity of the system and the resources required, such as skilled labor and technology infrastructure. A ballpark estimate for development could range from 13,000 to 15,000, depending on the scale and features.

* **Operational Costs**: Ongoing costs for maintenance, system updates, user support, and security enhancements will be necessary to ensure the system remains secure and effective.

The system can lead to significant cost savings by reducing the risks associated with data breaches and improving overall security, thereby avoiding potential financial losses.

Additionally, enhanced user satisfaction and ease of use can increase productivity

While the initial development and operational costs may be significant, the long-term benefits—such as enhanced security, reduced security breaches, and improved user experience—suggest a positive return on investment (ROI), making the graphical password system economically feasible in the long run.

### 3.1.3 Schedule Feasibility

The schedule feasibility of implementing a Graphics Based Parser Authentication System examines whether the project can be completed within a reasonable timeframe, considering the project’s complexity and available resources.

**Project Timeline**: The estimated duration for the full development and deployment of the system could range from 3 to 4 months, depending on the scope and complexity of the system. This timeline would include the phases of requirement gathering, design, development, testing, and deployment.

* Requirement Gathering and Planning: 1–2 weeks Understanding the system requirements, gathering inputs, and defining the project scope.
* System Design and Architecture: 2–3 weeks Designing the graphical user interface, database structure, and security architecture.
* Development Phase: 8–10 weeks Coding and implementation of the system, including both the frontend and backend components.
* Testing and Debugging: 3–4 weeks Rigorous testing for bugs, security vulnerabilities, and usability issues.

The timeline of 3 to 4 months appears feasible for the implementation of a Graphical Password Authentication System, assuming that resources are available and there are no significant delays during development and testing phases. Timely execution will be crucial for the successful deployment of the system.

**3.1.4 Social Feasibility:**

Social feasibility evaluates how well the Graphics Based Parser Authentication System aligns with societal and organizational norms, and whether it can be accepted by users, employees, or any other stakeholders involved. This also includes how the system will affect user behavior, privacy, and accessibility.

**User Adoption and Behavior**: One of the key factors for the success of the system is user acceptance. Since graphical passwords are relatively new compared to traditional alphanumeric passwords, users might initially be hesitant or unfamiliar with this method. The system needs to be easy to use and provide a better user experience to ensure its adoption. If the system is too complex or perceived as difficult, users may resist it. Additionally, for users accustomed to typing passwords, there could be a learning curve to shift to an image-based system.

**Privacy Concerns**: Since graphical passwords rely on selecting images or image regions, there are potential concerns about privacy, especially if the images contain sensitive or personal data. The system must be designed with strong privacy protections, such as encryption and secure storage of user credentials, to prevent unauthorized access or leakage of sensitive information. Addressing these concerns and ensuring that user data is handled securely will be important for building trust.

The Graphics Based Parser Authentication System is socially feasible, but its success depends on the system’s ability to ensure user adoption, maintain privacy, and provide accessibility for all users. Proper training, addressing cultural and individual needs, and ensuring user-friendly design will be essential for the system’s acceptance. Ensuring that the system aligns with societal norms and concerns will foster broader usage and trust.

# CHAPTER 4

# SOFTWARE REQUIREMENT SPECIFICATION

## 4.1. Functional Requirements

These requirements describe the system’s functionality and behavior, focusing on what the system should do:

### 1. User Registration

* Description: The system should allow users to register by selecting a set of images or regions within images that form their graphical password.
* Input: User details (e.g., name, email), selection of images or regions.
* Output: Confirmation of successful registration and graphical password storage.
* Feature: The system must ensure that images selected by the user are unique and securely stored with encryption.

### 2. User Authentication

* Description: The system must authenticate users based on their selected graphical passwords.
* Input: User's identification (e.g., username) and graphical password (image selection or click pattern).
* Output: Successful login or authentication failure notification.
* Feature: The system must validate the image-based password and provide real-time feedback if the entered password is incorrect.

### 3. Password Recovery

* Description: In case users forget their graphical password, they should be able to recover or reset it using an alternate method, such as email verification or security questions.
* Input: User identification and alternative recovery option (email/phone).
* Output: Password recovery link or instructions for resetting the password.
* Feature: Ensure secure password recovery options are available.

### 4. Image-Based Authentication (First Step)

* Description: The first step in the authentication process requires the user to select specific images they had chosen during registration from a set of images displayed.
* Input: A set of images is displayed, and the user selects the ones they had previously chosen during registration.
* Output: If the image selection is correct, the user proceeds to the next step (color-based authentication).
* Feature: The system must verify that the selected images match the user's registered image choices and ensure the image selection process is intuitive and responsive.

### 5. Color-Based Authentication (Second Step)

* Description: In this step, the user must select specific colors that were associated with their account during registration. These colors may be displayed in random order or as part of a color grid.
* Input: A color grid or selection of colors, from which the user must select the ones they previously chose.
* Output: If the user selects the correct colors, the system moves to the next step (cued recall authentication).
* Feature: The system should ensure that the colors are securely stored, and there is no risk of accidental selection due to color overlap or display issues.

### 6. Cued Recall Authentication (Third Step)

* Description: In this step, users must recall a predefined sequence of images or colors, which they had registered. The system provides cues (e.g., a hint image or a color) to help users remember their original selections.
* Input: A cue is displayed (e.g., an image or color), and the user must correctly recall and select the corresponding item from the set.
* Output: If the user recalls and selects the correct items, authentication is successful and they are granted access to the system.
* Feature: The system should securely handle the cued recall challenge and verify that the correct sequence is followed.

### 7. Authentication Flow

* Description: The three-step authentication process (image-based, color-based, and cued recall) should be performed sequentially. The user must successfully complete all steps to gain access to the system.
* Input: User inputs (image selection, color selection, and cued recall selection).
* Output: Successful login or failure notification if any step is incorrect.
* Feature: After three consecutive failed attempts, the system should temporarily lock the user out and initiate a recovery process.

## 4.2 Non-Functional Requirements

These requirements define the system's quality attributes, such as performance, security, and usability.

### 1. Performance Requirements

* Description: The system should be capable of handling a large number of simultaneous authentication requests without significant performance degradation.
* Requirement: The system must support at least 1,000 simultaneous users and ensure that the authentication process completes within 3 seconds for each user.

### 2. Security Requirements

* Description: The system must ensure the privacy and security of user data, especially their graphical passwords.
* Requirement: All graphical passwords should be encrypted and stored securely.

Password recovery mechanisms must be secure and prevent unauthorized access.

### 3. Usability Requirements

* Description: The system must be easy to use and intuitive for end-users of all technical skill levels.
* Requirement: The graphical password creation and authentication process should take no more than 5 minutes for new users to complete.

### 4. Availability Requirements

* Description: The system should be available and operational for users at all times.
* Requirement: The system must have an uptime of 99.9%, with maintenance scheduled during off-peak hours.

### 5. Compatibility Requirements

* Description: The system should be compatible with a variety of devices and platforms.
* Requirement: The graphical password system must function on major web browsers (Chrome, Firefox, Safari) and mobile platforms (iOS, Android).

## 4.3 Software Requirements

**4.3.1 Client-Side Tools and Technology Used for Project Integration**

### 1. HTML (Hypertext Markup Language)



HTML is the foundational language for structuring web pages. It defines the elements on the page such as headings, paragraphs, forms, images, links, and buttons. In the Graphical PasswordAuthentication System, HTML will be used to create the structure of key pages, such as the registration page, login page, and password recovery interface.

Purpose in the project: It structures the layout of the user UI, enabling the system to display input fields, buttons, and error messages to guide the user through the authentication process.

Key Features:

* Creates form elements to capture image selections, colors, and cued recall input.
* Organizes the page into sections (e.g., step-by-step authentication).

### 2. CSS (Cascading Style Sheets)



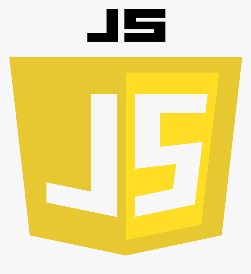
CSS is used to control the appearance and layout of the HTML elements. It defines the design, such as colors, fonts, spacing, and positioning of elements on the page. CSS will be utilized to make the Graphical Password Authentication System visually appealing and responsive.

Purpose in the project: CSS ensures the system’s pages are clean and user-friendly by providing style and organization. It also handles responsiveness, ensuring that the authentication pages look good on different devices (desktop, tablet, mobile).

Key Features:

* Provides styling for the image grid, color selection boxes, and input fields.
* Controls the layout, such as ensuring the content is centered, and sections are visually distinct.
* Implements media queries to make the system responsive across various screen sizes.

### 3. JavaScript (JS)



JavaScript is a powerful, high-level programming language that allows developers to add dynamic behavior to web pages.

Role in the Project: JavaScript will handle the core logic behind the three-step authentication process. It will manage user inputs, validate selections, and control the flow of authentication steps.

Key Features in the Project:

* Event Handling: JavaScript will handle events like clicks on images, colors, and form submissions. For instance, when the user selects an image, JavaScript will track the selection.
* Validation: The system must ensure that the user follows the correct order of selection for images, colors, and cued recall.
* Dynamic Content: JavaScript will dynamically display the images, colors, and form fields for each authentication step. It will also provide feedback to users (e.g., alerting them if they select the wrong image or color).
* Form Submission: JavaScript will manage the logic for form submissions, ensuring that users have entered all the required fields and that the authentication or registration is successful.

### 4. Bootstrap



Bootstrap is a popular open-source front-end framework that simplifies the process of designing responsive web pages. It provides a set of pre-designed UI components, a flexible grid system, and other features that can be easily integrated into any project.

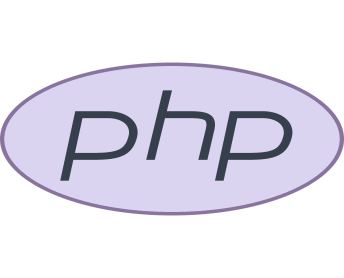
Role in the Project: Bootstrap will be used to ensure that the Graphical Password Authentication System is mobile-first and responsive, meaning it will work well on any device or screen size.

Key Features in the Project:

* Responsive Grid System: Bootstrap's grid system will help structure the layout of the authentication pages. It uses a 12-column system, allowing the design to adjust based on screen size (desktop, tablet, mobile).
* UI Components: Bootstrap includes a wide variety of pre-designed components like buttons, forms, alerts, modals, and navigation bars that will be used in the system. For example, you can use Bootstrap's form groups for the image, color, and cued recall fields, making them easy to style.
* Utility Classes: Bootstrap offers utility classes for spacing, alignment, colors, etc., which can be used to fine-tune the layout and design of the application without needing custom CSS for every small detail.

**4.3.2 Server-Side Tools and Technology Used for Project Integration**

### 1. PHP (Hypertext Preprocessor)



PHP is a server-side scripting language used for web development. It allows for dynamic content generation and is commonly used for handling form submissions, connecting to databases, and session management.

Role in the Project: PHP will be responsible for processing the data sent from the frontend (user inputs such as selected images, colors, and cued recall sequence). It will handle user registration, login authentication, session management, and interact with the database to store and retrieve authentication data.

Key Features in the Project:

* Form Handling: PHP will process the form data (image selections, color selections, cued recall sequences) submitted by the user.
* Database Interaction: PHP will interact with the MySQL database to store and retrieve authentication credentials (image, color selections, and cued recall sequences).
* Session Management: PHP will handle session management during user login to maintain authenticated states.

### 2. XAMPP



XAMPP is an open-source software package that includes Apache, MySQL, PHP, and Perl, making it easy to set up a local server environment for development purposes.

Role in the Project: XAMPP provides an easy-to-use local server environment for developing the Graphical Password Authentication System. It allows you to run Apache (web server), MySQL (database server), and PHP (scripting language) locally on your computer without needing to configure them separately.

Key Features in the Project:

* Local Server Setup: XAMPP simplifies the setup process by providing all necessary software in one package. It allows you to run your authentication system locally before deploying it to a live server.
* MySQL Database Management: XAMPP includes phpMyAdmin, a tool for managing MySQL databases easily through a web interface, where you can create and manage tables for storing authentication data.

### 3. MySQL



MySQL is an open-source relational database management system used for storing data in a structured manner.

Role in the Project: MySQL will be used to store user authentication data, including image selections, color selections, and cued recall sequences for each user. It will manage user data and ensure that only the correct combination of selections is allowed for successful authentication.

Key Features in the Project:

* Database Storage: MySQL will store user credentials securely in the database, including encrypted data for the graphical password selection.
* Querying: MySQL will handle database queries to validate the user’s authentication credentials during login and registration.

### 4. Apache



Apache is an open-source web server software used to serve web pages and handle HTTP requests from clients.

Role in the Project: Apache will be the web server that serves the frontend of the Graphical Password Authentication System. It will handle HTTP requests from users, directing them to the appropriate PHP scripts for processing.

Key Features in the Project:

* Web Hosting: Apache will host the Graphical Password Authentication System, serving

HTML, CSS, JavaScript, and PHP files to the client’s browser.

* Request Handling: Apache will handle incoming requests from users, executing PHP scripts on the server and sending the responses back to the client (e.g., login results or registration confirmations).
* URL Routing: Apache can handle URL routing and map incoming requests to the correct PHP files for the appropriate actions (login, registration, etc.).

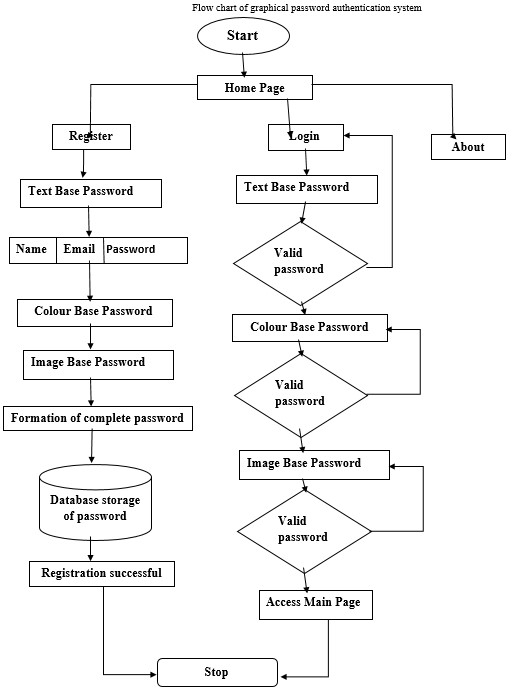
## 4.4 Hardware Requirements

|  |  |
| --- | --- |
| Processor | Intel Pentium IV 2.66 GHz or Dual Core |
| Main Memory (RAM) | 8GB |
| Hard Disk Capacity | 25GB |
| Keyboard | 101 Keys |
| Monitor | VGA with resolution |

# CHAPTER 5 SYSTEM DESIGN

## 5.1 DFD Diagram

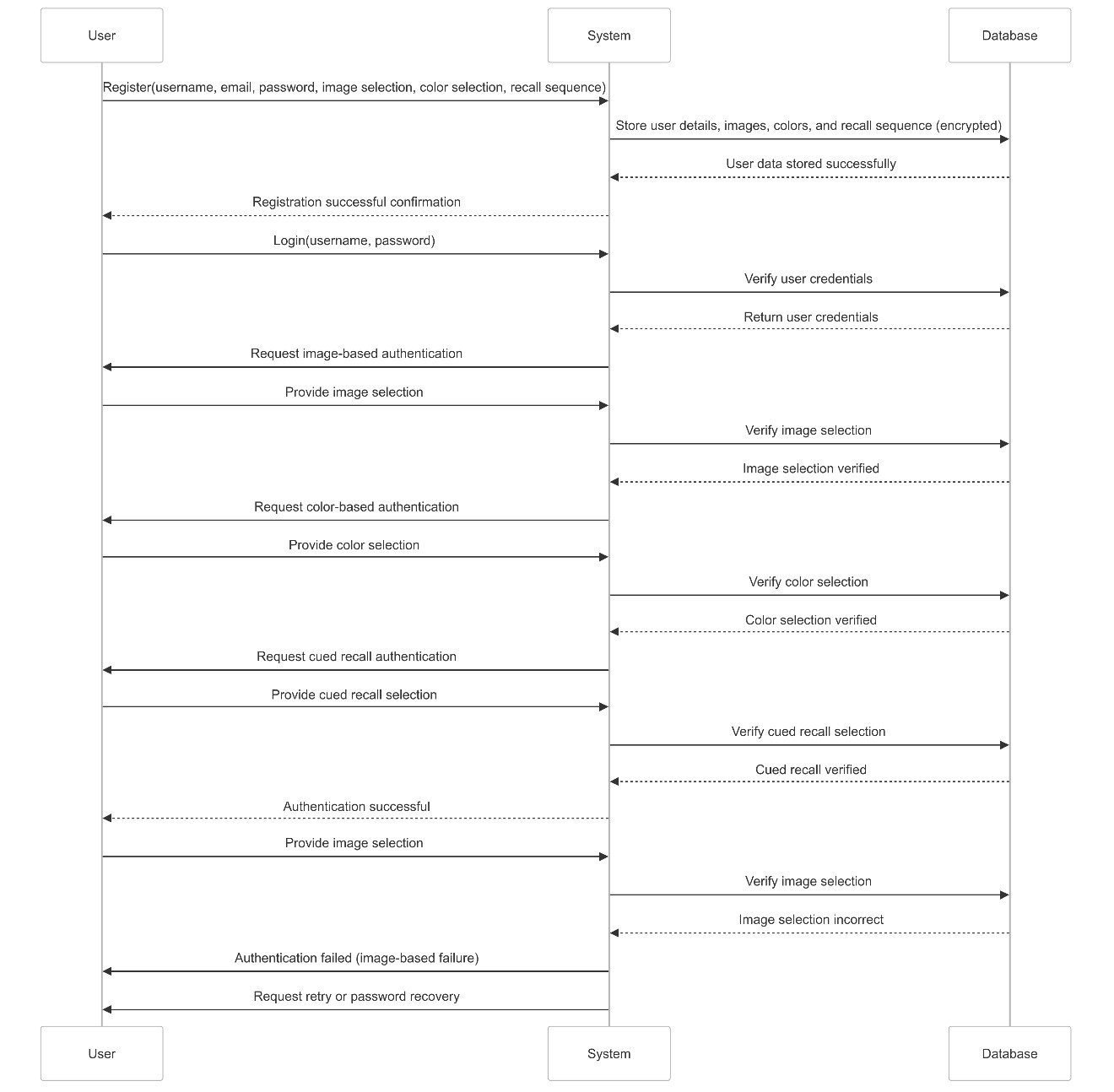
The Data Flow Diagram visualizes the flow of data within the system. It shows how data moves between the user interface, backend processing, and the database



**Fig:5.1**

## .2 Sequence Diagram

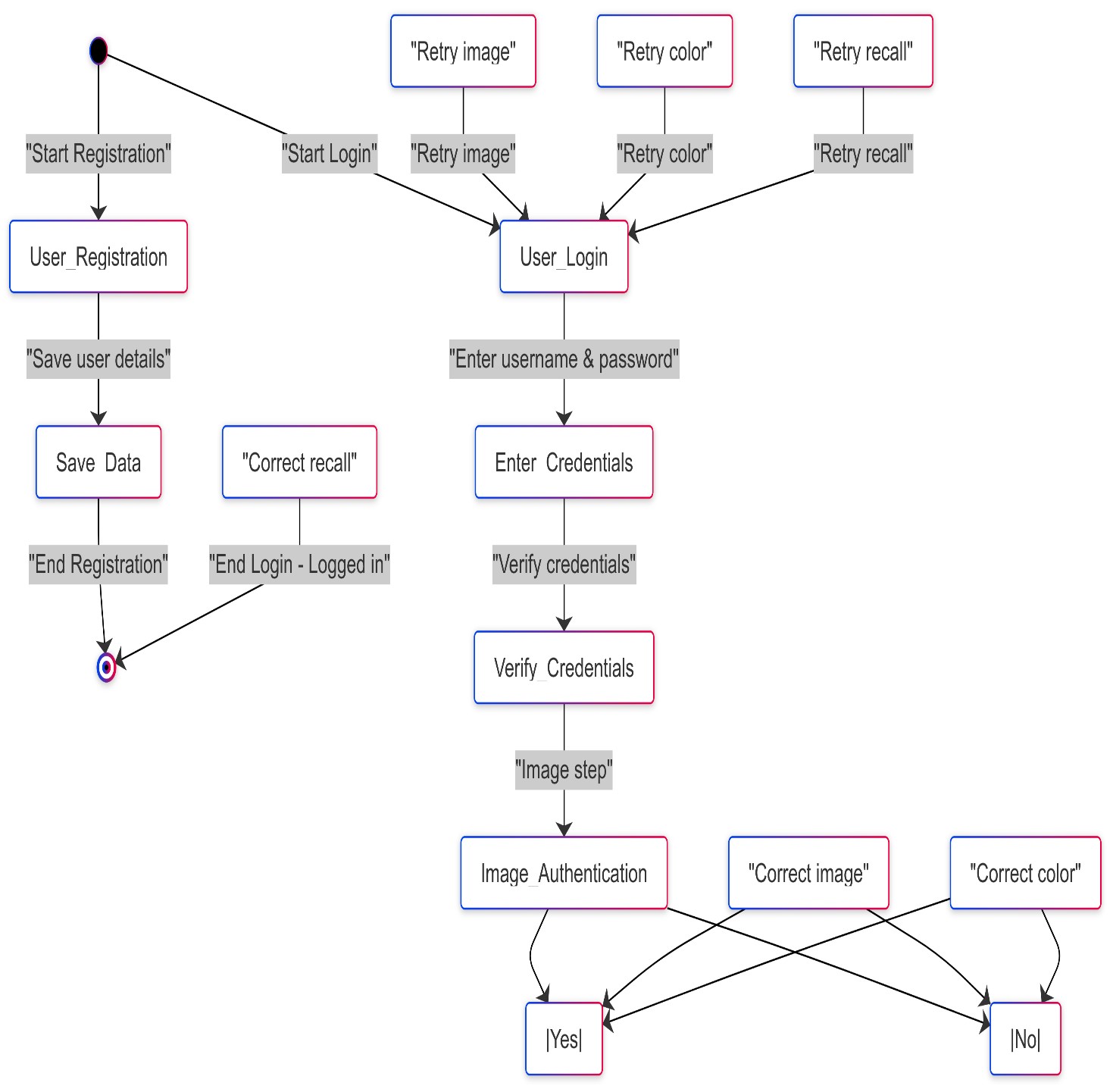
A Sequence Diagram is a type of UML diagram that illustrates how objects or components in a system interact with each other over time. It emphasizes the sequence of messages exchanged between entities, such as a user and a system, showing the flow of information and the order of operations. Each object is represented by a lifeline, and interactions are depicted as messages exchanged in a sequential order, allowing for a clear visualization of the process flow in time. Sequence diagrams are particularly useful for modeling the behavior of a system in response to user actions, such as logging in or making a purchase.



**Fig :5.2**

## .3 Activity Diagram

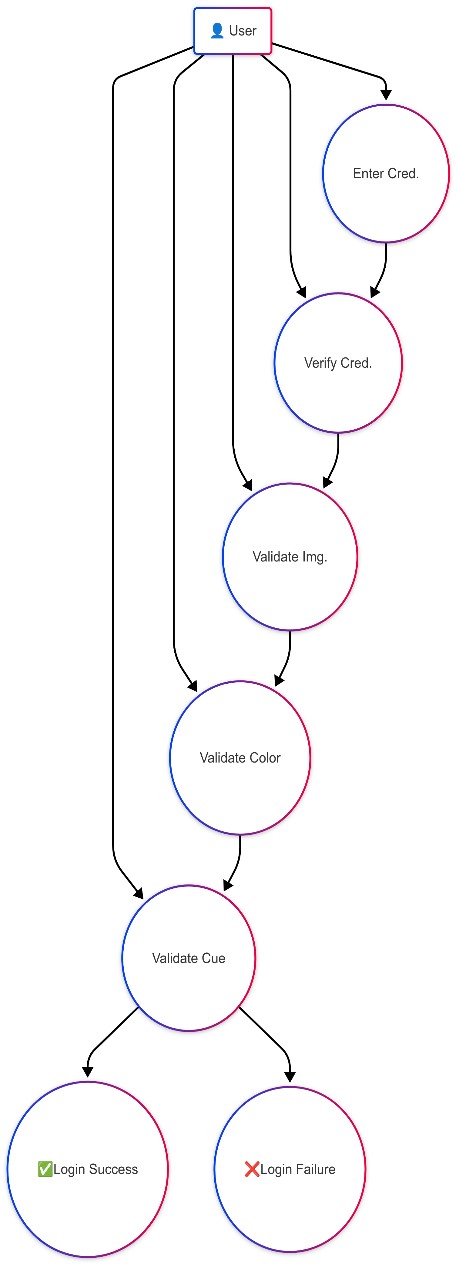
Activity Diagram represents the workflow or business process within a system. It is used to model the dynamic behavior of a system, focusing on the flow of activities or tasks. The diagram includes decision points, actions, and the sequence in which tasks are performed. Activity diagrams are excellent for showing parallel processes, conditional flows (yes/no), and how different activities are connected. They are ideal for illustrating processes like user authentication or multi-step operations, where decisions or branching occurs based on specific conditions. Both diagrams provide complementary views of system behavior, with sequence diagrams focusing on interactions and activity diagrams highlighting process flows.



**Fig :5.3**

## .4 Use Case Diagram

A Use Case Diagram is a visual representation of how users (actors) interact with a system. It shows the system's functionality through use cases, which are specific actions or processes the system performs. Actors, represented by stick figures or circles, interact with these use cases, depicted as ovals or ellipses. The diagram helps identify the system’s requirements and interactions, providing a clear overview of how users will engage with the system to achieve their goals. It’s commonly used in the early stages of development to clarify system functionality.



**Fig :5.4**

## CHAPTER 6

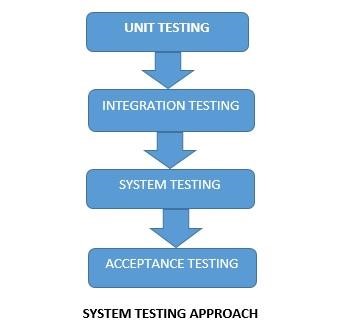
**IMPLEMENTATION AND TESTING**

### 6.1 Implementation

The implementation phase is the stage where the system is actually built based on the design and requirements gathered during earlier phases. For the Graphics Based Parser Authentication System, this phase involves several key steps. First, the development environment is set up, which includes configuring necessary software such as XAMPP for local server management, along with PHP for server-side scripting and MySQL for database management.

Next, the user interface (UI) is created using HTML, CSS, JavaScript, and Bootstrap, ensuring a responsive design for user registration, login, and authentication processes. The backend development involves coding the logic for handling user registration, storing graphical password details securely in the database, and authenticating users during login using the threestep process: image-based authentication, color-based authentication, and cued recall.

### 6.2 Testing Approach



#### 6.2.1 Unit Testing

Unit testingis a critical phase in software development that focuses on testing individual components or functions of the system to ensure each unit of the software works as expected. It helps identify bugs early in the development cycle, making it easier to fix issues before they escalate into larger problems. In the context of the Graphics Based Parser Authentication System, unit testing will focus on testing individual functions, such as password encryption, image validation, color validation, and user input validation.

#### 6.2.2 Integration Testing

Integration testing is a crucial phase of the software development lifecycle that focuses on testing the interaction between different components of the system. It ensures that various modules, when combined, work together as intended and that data flows smoothly across the system.

For the Graphics Based Parser Authentication System, integration testing aims to validate the communication between the front-end interface, back-end logic, and the database. This testing phase checks if the individual components that were unit tested work correctly when integrated into the overall system.

Additionally, integration testing will examine the communication between the PHP backend and the MySQL database, ensuring that user data such as image selections, colors, and hashed passwords are correctly stored and retrieved from the database. These tests will also ensure that the authentication process can handle multiple login attempts and sessions efficiently.

By conducting integration tests, the development team can identify issues that might occur when different system components interact with each other, ensuring the overall stability and functionality of the system before it is deployed for use.

#### 6.2.3 System Testing

System testing is a critical phase in the software development process where the complete system is tested as a whole to ensure that it meets the specified requirements and works as expected in the real-world environment. Unlike unit or integration testing, which focuses on individual components or interactions between components, system testing evaluates the behavior of the entire application when all its parts are integrated and working together.

In the case of the Graphics Based Parser Authentication System, system testing will involve testing the entire flow of the application from user registration to authentication, ensuring that all functionalities perform as expected. This phase will verify that the system as a whole works correctly and that it can handle various user actions, such as registering a graphical password, logging in, and recovering a password if forgotten.

#### 6.2.4 Acceptance Testing

Acceptance testing is the final phase of testing before the system is delivered to the client or end-users. It focuses on validating whether the system meets the specified requirements and satisfies the user's needs and expectations. The goal of acceptance testing is to ensure that the Graphics Based Parser Authentication System works as intended in a real-world environment and that it is ready for production use.

During acceptance testing, the system is tested from the perspective of the end user. The key focus is on validating whether the system functions according to the business requirements, as well as ensuring that the user experience is intuitive and seamless. this testing phase typically includes two main components: alpha testing (performed by the development team or internal testers) and beta testing (conducted by a select group of end-users or clients.

# CHAPTER 7

# RESULTS AND DISCUSSION

The outcome of using graphical password authentication, here are some potential results:

1. Improved User Experience: Users may find graphical password authentication systems more intuitive and user-friendly compared to traditional text-based passwords, leading to increased satisfaction with the authentication process.

1. Enhanced Security: Graphical password authentication systems can offer enhanced security features such as resistance to dictionary attacks, reduced vulnerability to keylogging, and increased privacy against shoulder surfing.

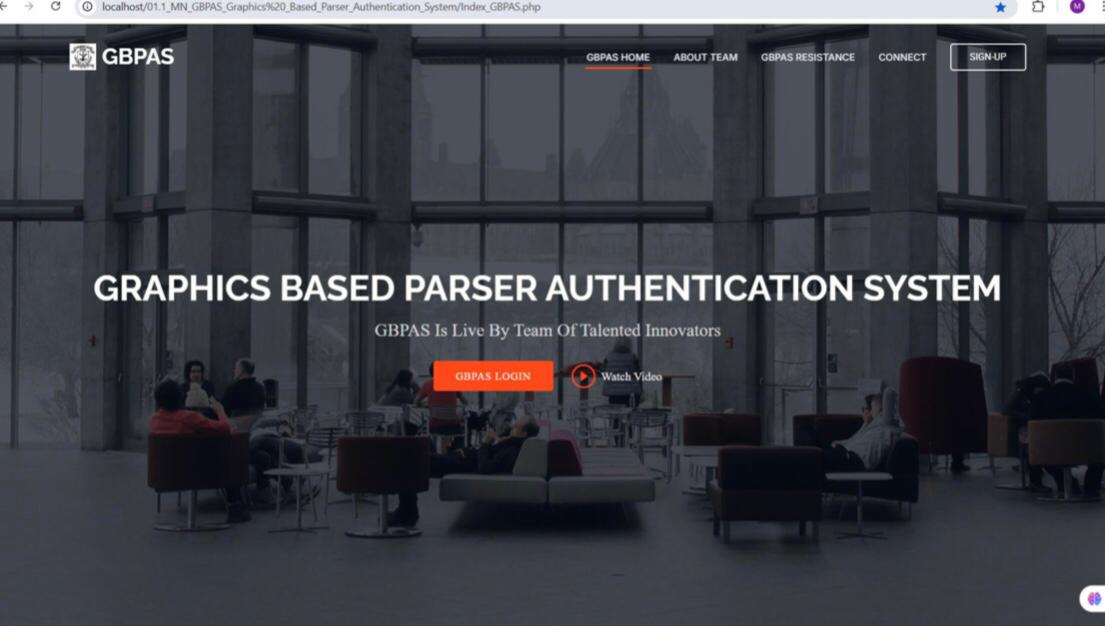
1. Reduced Password Fatigue: Graphical passwords may reduce user fatigue associated with remembering and typing complex alphanumeric passwords, potentially leading to fewer instances of forgotten passwords and password resets.

1. Increased Accessibility: Graphical password authentication systems can be more accessible to users with disabilities, offering alternative authentication methods that accommodate diverse needs and preferences.

1. Potential Challenges: However, there may also be challenges associated with the adoption of graphical password authentication, such as usability issues, training requirements for users, and the need for robust security measures to prevent attacks.

Overall, the results of using graphical password authentication can vary depending on factors such as system design, implementation, user acceptance, and security considerations. With careful planning and implementation, graphical password authentication systems have the potential to provide a secure and user-friendly authentication experience for a wide range of users.

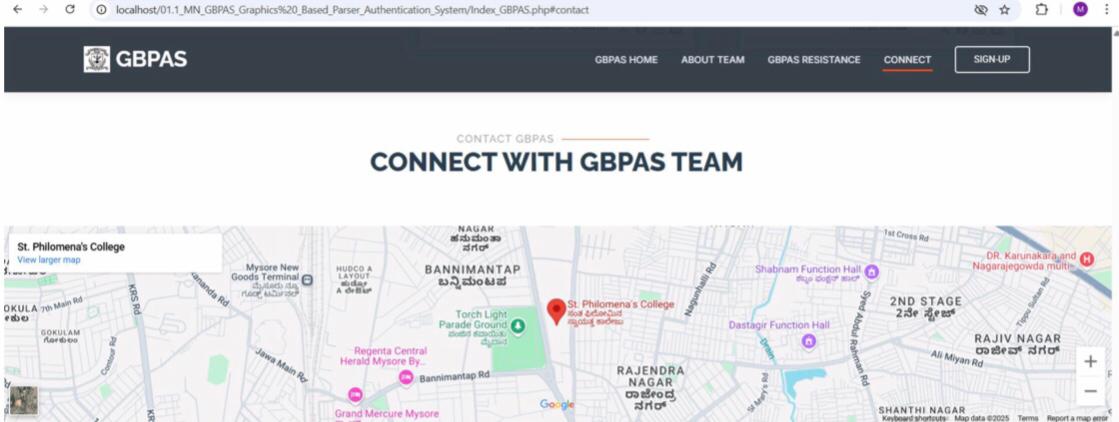
## 7.1 SNAPSHOTS



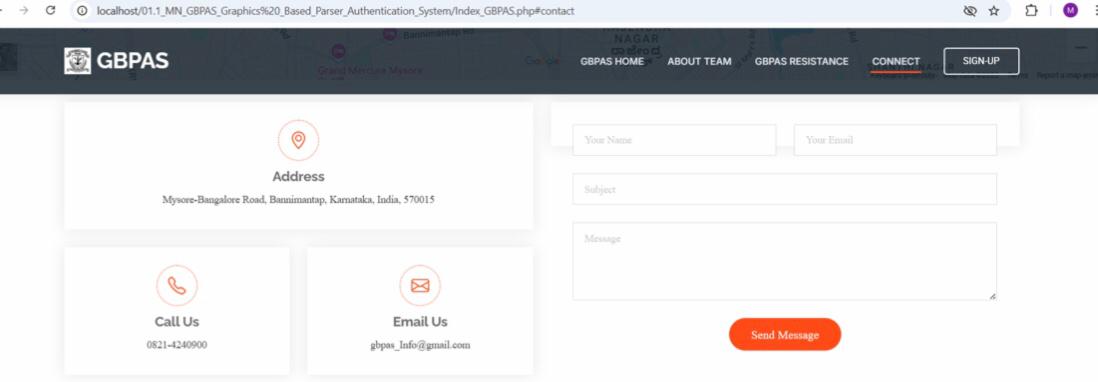
**FIG 7.1: DEVELOPMENT IN PROGRESS**



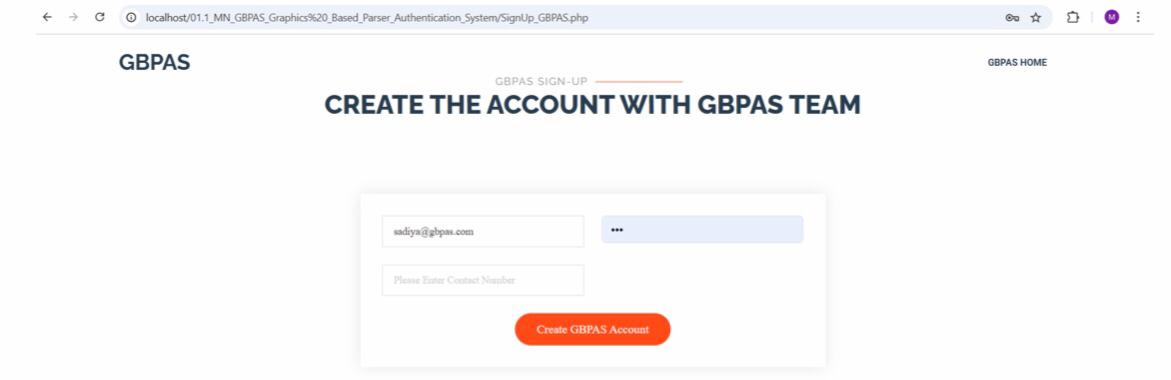
**FIG 7.2:**



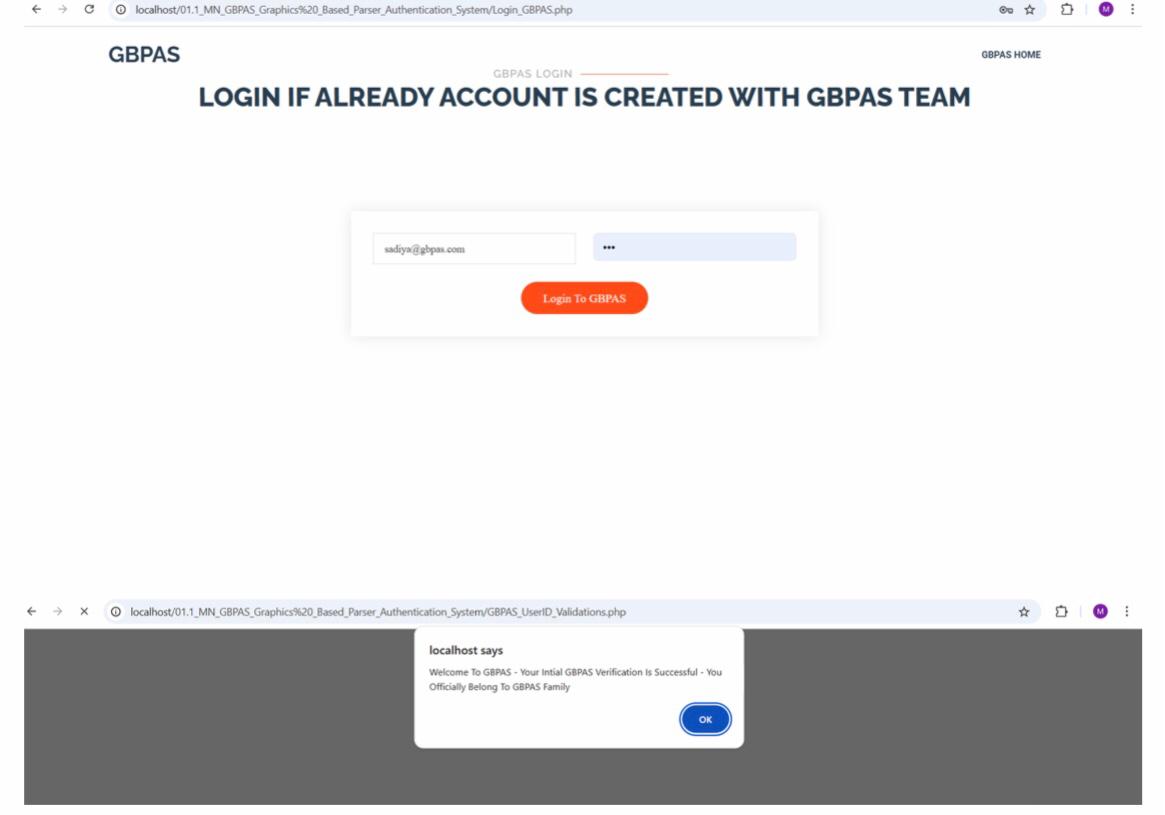
**FIG 7.3:**



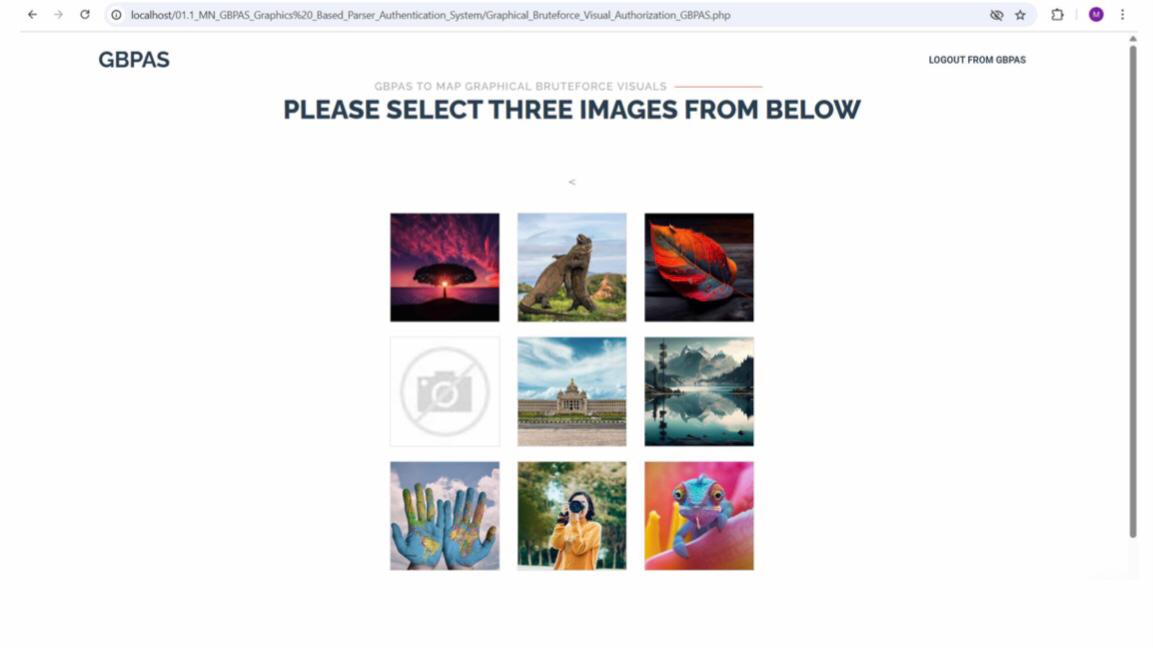
**FIG 7.4:**



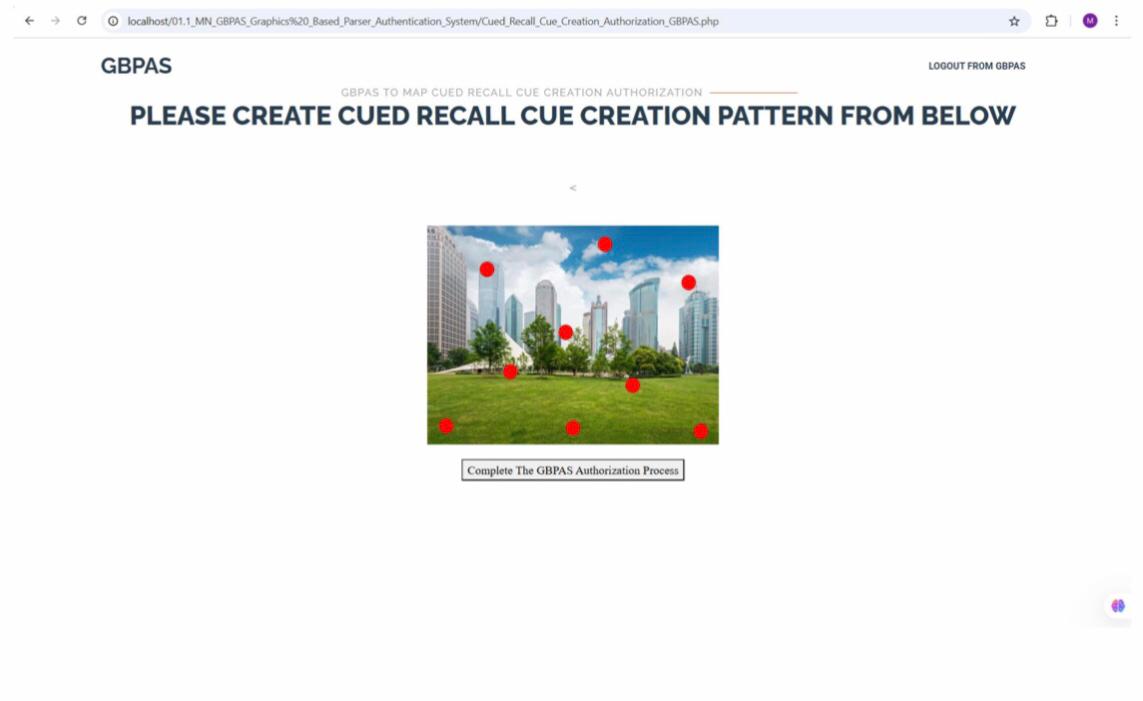
**FIG 7.5:**

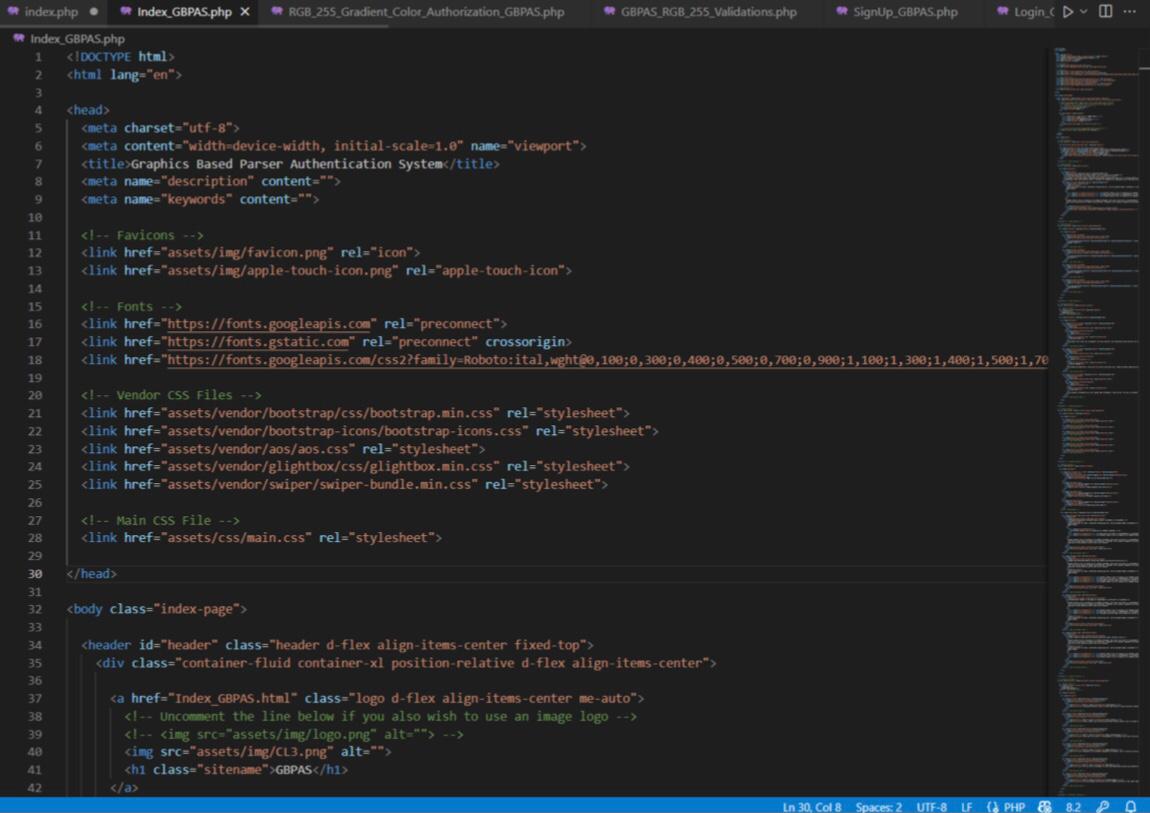


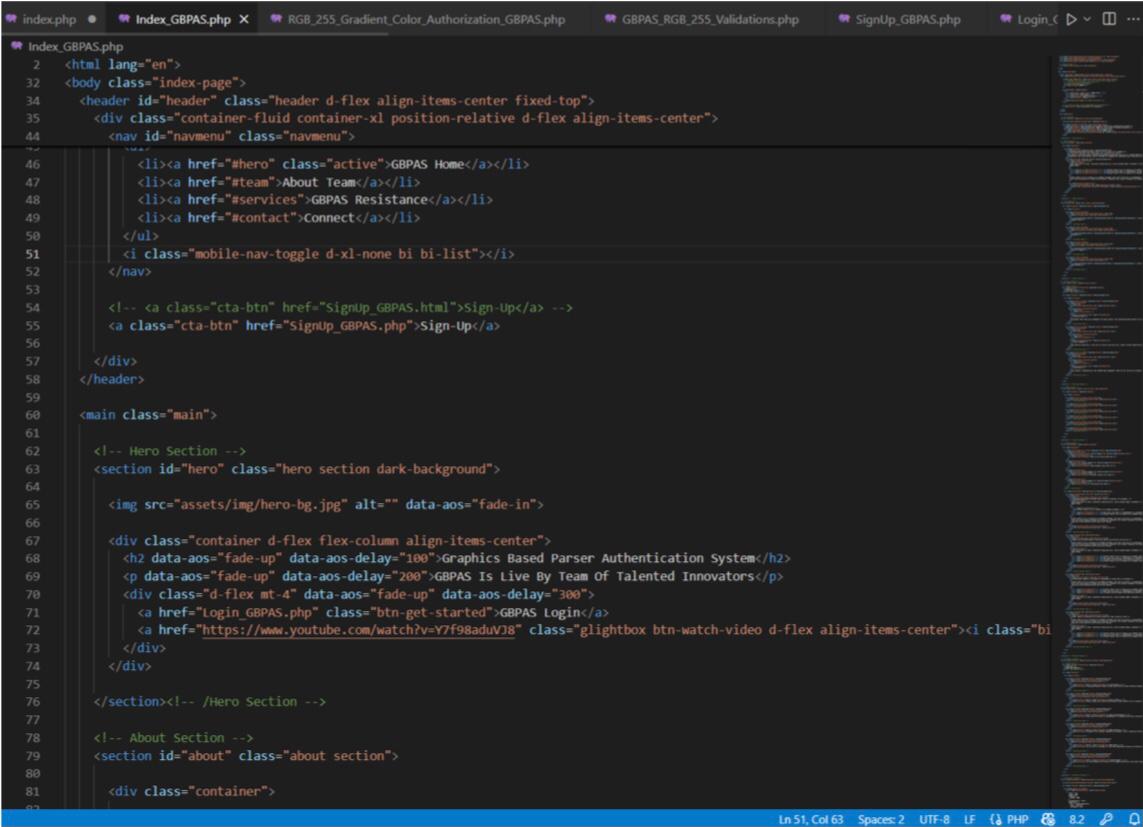
**FIG 7.6:**

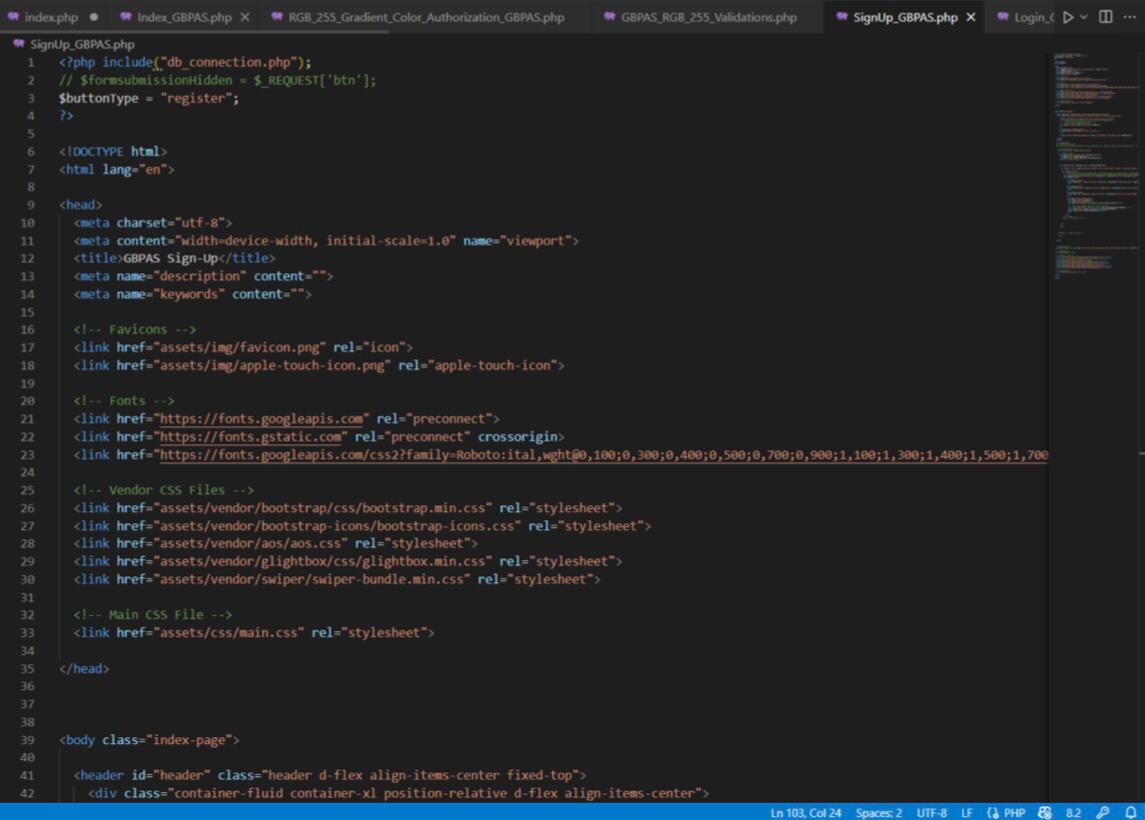


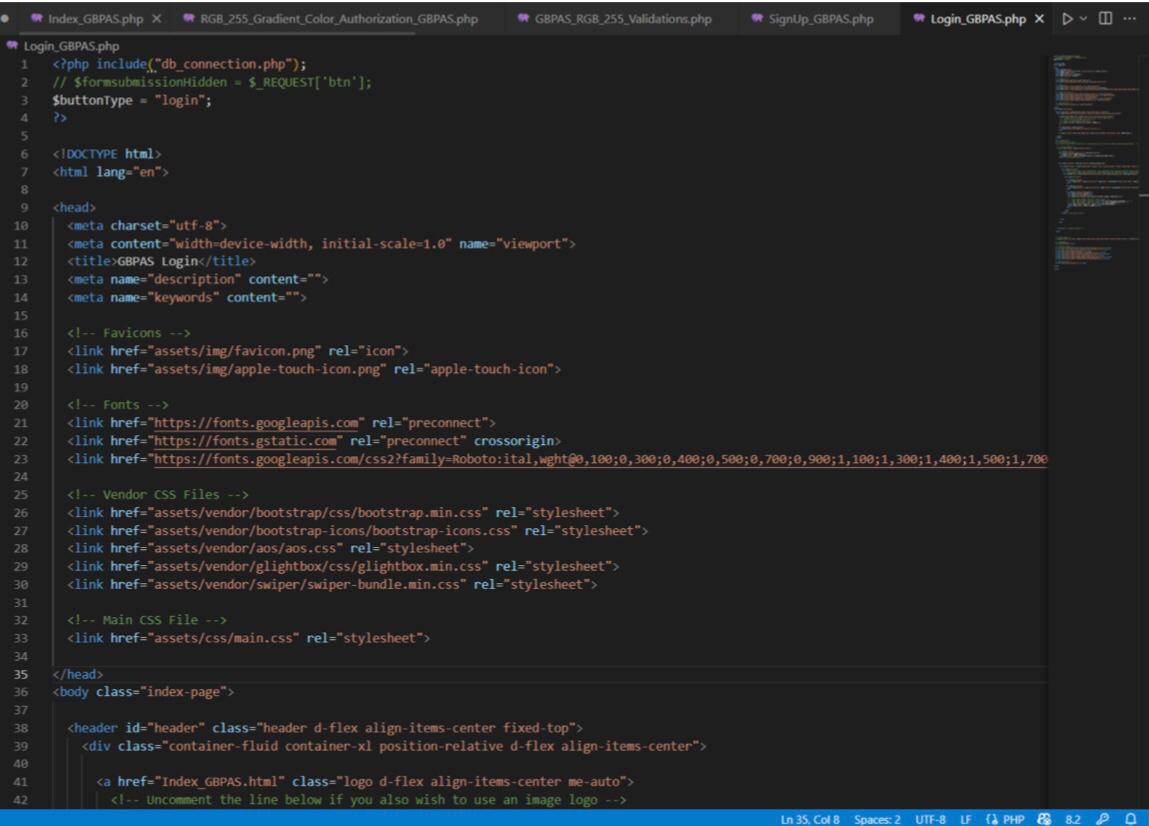
**FIG 7.7:**



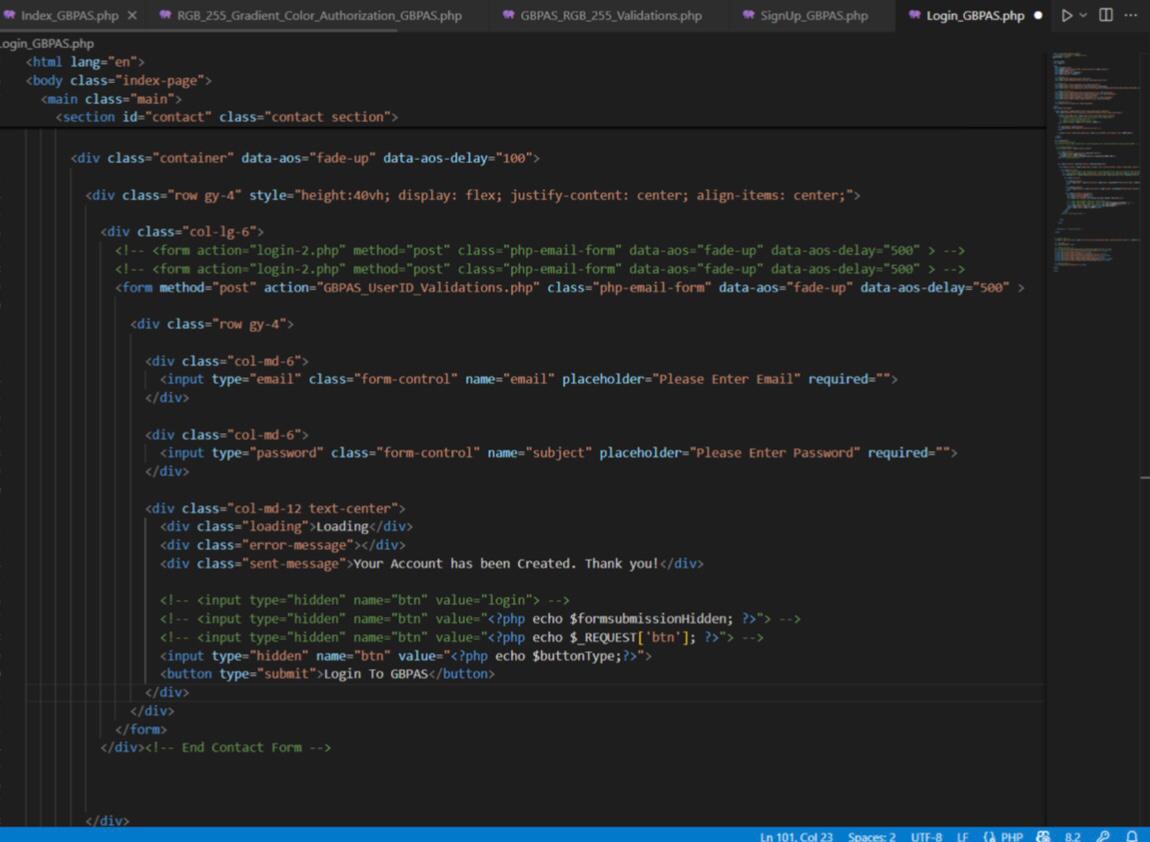


****





# 



# 

# CHAPTER 8

# FUTURE SCOPE

The future enhancement of Graphics Based Password Authentication Systems (GPAS) lies in improving both security and user experience. Integrating Multi-Factor Authentication (MFA) with biometric authentication, such as fingerprint or facial recognition, can provide an additional layer of security. Adaptive graphical interfaces, dynamic grid sizes, and touchscreen integration will make the system more user-friendly, while combining voice commands could further streamline the process.

GPAS can also become more contextually aware, using location-based and time-based restrictions, as well as environmental sensors to enhance security. To combat attacks, implementing techniques such as salting the graphical password and introducing dynamic elements like moving visuals will make the system more resilient.

To further enhance security, encrypted communications via HTTPS and Web Cryptography API could be leveraged to ensure that graphical passwords are transmitted securely and stored in an encrypted format on the server. The local Storage or Indexed DB APIs can be used for securely caching passwords on the user's device, allowing for a seamless experience even in offline modes.

For increased contextual security, Geolocation APIs can be incorporated to restrict login attempts based on location, while Web Authentication APIs (Web Authn) could add a layer of biometric security, requiring users to authenticate with face or fingerprint recognition before accessing sensitive systems.

# CHAPTER 9

# CONCLUSION

The Graphics-Based Parser Authentication System (GBPAS) represents an innovative step forward in securing user identities by leveraging the power of graphical patterns, images, and user interactions instead of relying on traditional text-based methods. By utilizing visual cues and integrating advanced parsing algorithms, this system offers enhanced security, reduced vulnerability to common cyber-attacks such as brute force, phishing, and social engineering, and improved user experience.

The key strengths of GBPAS lie in its resistance to simple attack methods that target alphanumeric passwords and PINs. The graphical interface is inherently more difficult to guess or replicate, as it requires a higher degree of complexity and personal engagement, making it significantly more secure. Additionally, the system integrates a multi-layered approach to authentication, potentially incorporating image recognition, user behavior analytics, and machine learning, further enhancing both security and adaptability.

Moreover, the system addresses usability concerns by providing an intuitive and visually engaging method for authentication. The reliance on graphical elements allows users to bypass the cognitive load associated with remembering complex passwords while still maintaining strong security protocols.

In conclusion, the Graphics-Based Parser Authentication System offers a promising alternative to traditional text-based authentication methods. With ongoing developments in image recognition, pattern learning, and user behavior analysis, GBPAS could become a cornerstone in future authentication systems. Its ability to combine security with a more user-friendly interface presents a compelling case for adoption across various domains, from online banking to mobile security, ushering in a new era of more secure and intuitive authentication methods.

# REFERENCES

1. Graphical Password Authentication. ShraddhaM. Gurav Computer Department Mumbai University RMCET Ratnagiri, India. Leena S. Gawade Computer Department Mumbai University RMCET Ratnagiri, India, 2014 IEEE.

1. Enhancement of Password Authentication System Using Graphical Images. Amol Bhand,Vaibhav desale Savitrybai Phule Pune University, Swati Shirke Dept.of Computer Engineering NBN Sinhgad School of Engineering, Pune, Dec 16-19, 2015

1. The Shoulder Surfing Resistant Graphical Password Authentication Technique.

Mrs.Aakansha S. Gokhalea , Prof. Vijaya S.Waghmareb.

1. A New Graphical Password Scheme Resistant to Shoulder-Surfing. Uwe Aickelin School of Computer Science the University of Nottingham Nottingham, NG8 1BB, U.K.
2. A Graphical Password Against Spyware and Shoulder-surfing Attacks. Elham Darbanian Master of Engineering, College of e-learning Shiraz University, Gh. Dastghaiby fard Department of Computer science & Engineering, College of Electrical and Computer & Engineering Shiraz University,jun- 2015.

1. Text based Graphical Password System to Obscure Shoulder Surfing. Khazima Irfan, Agha Anas, Sidra Malik, Saneeha Amir Department of Computer Science COMSATS Institute of InformationTechnology Islamabad Pakistan, 13th January,2018.