JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Enhanced Authentication Security: A Color- Assisted Text-Based Graphical Password Scheme"

Parsha Sravanthi Asst.Professor

Dept of Software Engineering ,

Balaji Institute of Technology and Science, Warangal, Telangana, India parshasravanthi1@gmail.com

Abstract:
Conventional password schemes are vulnerable to **shoulder surfing attacks**, where an adversary observes a user's login process to steal credentials. To mitigate this, many **graphical password schemes** have been proposed. However, since users are generally more familiar with **textual passwords** than purely graphical ones, **text-based graphical password schemes** have gained attention.
Unfortunately, existing text-based shoulder surfing-resistant schemes often lack **either efficiency or sufficient security**. In this project, we propose an **improved text-based graphical password scheme** that incorporates the use of **colors** to enhance both **security** and **usability**.
The proposed scheme allows users to log in **quickly and intuitively**, while maintaining strong resistance to **shoulder surfing** and reducing the risk of **accidental logins**. We further analyze the **security** and **usability** of the system, demonstrating its robustness against observational attacks and its practicality for real-world use.

Keywords: *Graphical Password,Text-Based Authentication,Shoulder Surfing Resistance,Color- Coded Login Scheme, Secure Authentication, Usability*

I. INTRODUCTION

1. *INTRODUCTION*

User authentication is a fundamental aspect of computer security, with alphanumeric passwords remaining the most widely used method. However, this traditional approach presents several challenges—most notably, the inherent trade-off between memorability for users and resistance to guessing or attacks. This paper explores the intricacies of user authentication, highlights the limitations of alphanumeric password schemes, and examines graphical password techniques as a promising alternative to enhance both security and usability**.**

The Significance of User Authentication

User authentication plays a critical role in ensuring that only authorized individuals can access computer systems, applications, and online services. Serving as the first line of defense, it verifies a user's identity before granting access to sensitive information or functionalities. For decades, alphanumeric passwords—comprising combinations of letters, numbers, and special characters—have been the most common method of authentication due to their simplicity and user familiarity. However, their extensive use has also revealed significant security vulnerabilities, including susceptibility to brute-force attacks, phishing, and shoulder surfing.

.**The Conflict Between Rememberability and Security**: One of the core issues with alphanumeric passwords is the inherent tension between two essential requirements:

1. Easy to Remember: Passwords should be easy for users to remember to minimize the risk of forgetting or recording them insecurely.
2. Hard to Guess: On the other hand, passwords should be difficult for potential attackers to guess or crack, making brute force and dictionary attacks less likely to succeed.

Unfortunately, many users prioritize rememberability over security, resulting in the creation of weak passwords that are easily guessable. Common examples include using "password" or simple phrases, birthdates, or easily accessible information.

The Consequences of **Weak Passwords**: Weak passwords represent one of the weakest links in computer security systems. They expose systems and user accounts to various risks, including unauthorized access, data breaches, and identity theft. Attackers often employ password-cracking techniques, such as dictionary attacks, brute force attacks, and password spraying, to exploit weak passwords and gain unauthorized entry. Additionally, compromised accounts can be used for launching further attacks, such as phishing and social engineering.

Proposed Solutions and the **Role of Graphical Passwords**: To address the vulnerabilities associated with traditional alphanumeric passwords, researchers and security experts have proposed various solutions. One notable alternative is graphical passwords. Graphical passwords involve users selecting images, patterns, or other visual elements as a means of authentication.

Graphical passwords aim to strike a **balance between usability and security**. They can be more memorable than complex alphanumeric strings while offering resistance to common guessing attacks. Users may choose from a predefined set of images or draw a unique pattern, making it harder for attackers to predict or crack the authentication method.

Benefits of Graphical Passwords: Graphical passwords offer several advantages:

1. Memorability: Users find it easier to remember images or patterns compared to random character combinations.
2. Resistance to Guessing Attacks: Predicting or guessing a graphical password is considerably more challenging for attackers.
3. Reduced Risk of Dictionary Attacks: Since graphical passwords do not rely on words or phrases, they are not susceptible to dictionary attacks.
4. User Engagement: The interactive nature of graphical password creation can enhance user engagement and satisfaction.

2. *PURPOSE*

The purpose of graphical passwords is to provide an alternative and more securemethod of user authentication compared to traditional text-based passwords. Graphical passwords use images, patterns, or drawings instead of alphanumeric characters to verify a user's identity. Their primary objectives and purposes include:

Enhanced Security: Graphical passwords are designed to offer a higher level of security compared to text- based passwords. They are often more resistant to bruteforce attacks, dictionary attacks, and password guessing, as the visual elements used can be more complex and harder to predict.

Mitigation of Shoulder Surfing: One of the key purposes of graphical passwords is to reduce the vulnerability to shoulder surfing attacks. Observers find it challenging to replicate or capture graphical patterns, making it harder for malicious individuals to steal passwords by simply watching users enter them.

Overall, the purpose of graphical passwords is to provide a secure and user friendly authentication option that addresses the limitations and vulnerabilities associated with traditional text-based passwords. They aim to enhance security while offering a more engaging and personalized user experience.

3. *SYSTEM ANALYSIS*

After analysing the requirements of the task to be performed, the next step is to analyse the problem and understand its context.

Analysis Model;

The Model that is basically being followed is the WATERFALL MODEL, which states that the phases are organized in a linear order. First of all the feasibility study is done. Once that part is over the requirement analysis and project planning begins. If system exists one and modification and addition of new module is needed, analysis of present system can be used as basic model.

4. *Modules of the System*

The system after careful analysis has been identified to be presented with the following modules: The modules involved are:

- Administrator
- User

Admin Module

a. **User Registration:** Users register by providing their personal details, including a username, email address, and selecting a color for graphical password authentication.

This information

is stored securely in the system's database.

b. **Data Handling:** The admin has privileged access to the system and can view, manage, and modify user data as needed. This access allows the admin to assist users with any data- related issues or changes.

c. **Data Modification Requests:** Users who need to modify their registration data(e.g., change email address or update their chosen color) can make requests to the adminfor assistance.

d. **Admin Assistance**: When a user requests data modification, the admin can verify the user's identity through appropriate means (e.g., communication via a verified email address or secondary authentication). Once identity is confirmed, the admin can update the user's information in the system's database.

5. *GRAPHICAL PASSWORD REPRESENTATION:*

a. **Admin Interface:** The admin provides an interface within the system for users to set up their graphical passwords. This interface includes the option for users to select their color, which is a crucial element of the graphical password.

b. **Password Setup**: Users use the admin-provided interface to create their graphical password. They select a color and configure any additional graphical elements as required by the system.

c. **Secure Storage:** The system securely stores the graphical password information, associating it with the user's account.

d. **Authentication:** During login, users enter their username and the traditional password, and they adjust a color picker to match their chosen color, as previously described.

e. **Admin Support**: In case users encounter issues with setting up or using their graphical password, they can seek assistance from the admin.

f. **Security and Maintenance**: The admin is responsible for ensuring the security and reliability of the graphical password authentication system. This includes monitoring for any unusual activity or potential breaches.

It's important to implement strong security measures to protect user data, ensure secure authentication, and prevent unauthorized access to user information. Additionally, user privacy should be a priority, and data handling procedures must comply with relevant data protection regulations. Regular system maintenance and updates should also be carried out to keep the system secure and up-to-date.

USER MODULE :

1. **User Registration**: The user starts by providing the required registration details, which typically include personal information like name, email address, and username. This information is stored securely in the system's database.

2. **Password Setup**: During the registration process, the user is prompted to set up their password. This password is traditionally a combination of alphanumeric characters, special symbols, or other characters, similar to text-based passwords.

3. **Color Selection:** In addition to the password, the user is asked to select a color from a predefined set of colors. This chosen color will serve as the main key for future logins.

LOGIN:

a. **Username and Password:** To log in, the user provides their username (or email) and the traditional password they set during registration.

b. **Color Authentication**: After entering the username and password, the user is prompted to adjust a color picker or slider to match the chosen color they selected during registration. This is where the unique aspect of the system comes into play.

c. **Authentication Process:** The system compares the adjusted color value provided by the user with the color value associated with their account. The match must be sufficiently close to be accepted as a valid authentication.

d. **Successful Login:** If both the traditional password and the adjusted color match the stored values in the system's database, the user gains access to their account.

6. *EXISTING SYSTEM*

Visual or graphical password authentication system, which is a variation of traditional text based passwords. Instead of typing a password, users

select or interact with specific icons, images, or patterns to authenticate themselves. This approach is often used for enhanced security and usability. Here's how it generally works:

1. **Icon Selection:** During the initial setup, the user chooses a set of icons or images that will serve as their password elements. These icons could be anything, such as animals, objects, or symbols.

2. **Challenge Screen**: When the user wants to authenticate, a challenge screen is presented. This screen contains numerous icons and images, including the user's private password icons.

3. **Authentication Process**: To authenticate, the user must visually locate their chosen icons among the others on the screen and interact with them in a specific way. This interaction can vary depending on the system's design. For example, they might click or tap on their chosen icons in the correct sequence or drag and drop them into a designated area.

4. **Feedback:** The system provides feedback to the user to indicate whether they have successfully completed the authentication process. If they select the correct icons or perform the correct actions, they gain access. Otherwise, they may need to retry.

DISADVANTAGES:

a. **Memory Load:** Remembering the specific icons or images and their arrangement can be difficult for some users, especially if they choose a large set of icons or complex patterns.

b. **Shoulder Surfing**: Visual passwords are vulnerable to shoulder surfing, where an attacker can simply watch the user's interactions to learn their password. This is especially problematic in public settings.

c. **Reset Process**: Resetting a graphical password can be more complicated than resetting a traditional text-based password, as it may involve verifying the user's identity through other means.

7. *PROPOSED SYSTEM*

The login system described involves a circular interface with eight sectors, each containing different colored arcs. Within these sectors, 16 characters are randomly distributed. Users can interact with the system by rotating the characters either clockwise or counter clockwise into adjacent sectors. Let's break down how this systemworks:

AUTHENTICATION PROCESS:

1. **User Interaction**: When a user attempts to log in, they are presented with the circular interface containing the 8 sectors and the 16 characters distributed within thesesectors.

2. **Character Rotation**: To authenticate, the user needs to arrange the characters in a specific sequence or pattern within the sectors. They can achieve this by clicking buttons labeled "Clockwise" and "Anti-clockwise."

3. **Rotation Rules**: Clicking the "Clockwise" button once will rotate all the colors within the sectors in a clockwise direction. Clicking the "Anti-clockwise" button once will rotate them counter clockwise.

4. **Pattern Matching:** The user must rotate the characters in such a way that they align with a pre-defined pattern or configuration set during the initial setup. This pattern based on the colors of the arcs.

5. **Feedback:** The system provides feedback to the user, indicating whether the characters are correctly aligned according to the predetermined pattern. If the arrangement matches the required pattern, the user gains access. Otherwise, they may need to retry.

Advantages :

1. **Enhanced Security**: This system offers an alternative to text-based passwords,making it less susceptible to traditional password attacks like brute force.

2. **User Engagement**: The interactive nature of this authentication method canengage users and make the login process more interesting.

3. **Customization:** Users can set their own patterns or configurations based on thecolors of the arcs, increasing personalization and security.

7.FEASIBILITY STUDY

Feasibility study is a high-level capsule version of the entire process intended to answer a number of questions like: What is the problem? Are there any feasible solutions to the given problem? Is the problem even worth solving? Feasibility study is conducted once the problem is clearly understood. Feasibility study is necessary to determine that the proposed system is feasible by considering the technical, Operational, and Economical factors. By having a detailed feasibility study the management will have a clear-cut view of the proposed system.

Feasibility study encompasses the following thing:

1. Technical Feasibility
2. Operational Feasibility
3. Economical Feasibility

8. *SYSTEM DESIGN*

Software design sits at the technical kernel of the software engineering process and is applied regardless of the development paradigm and area of application. Design is the first step in the development phase for any engineered product or system.

UML diagrams

Use Case:

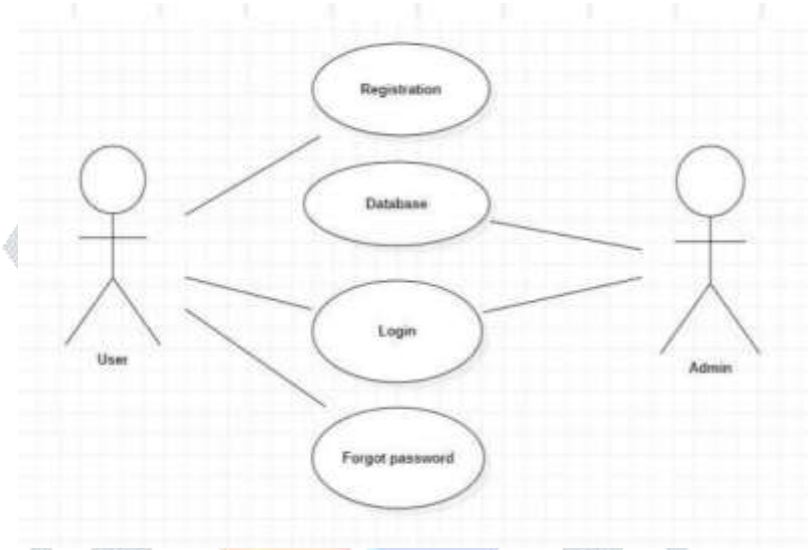
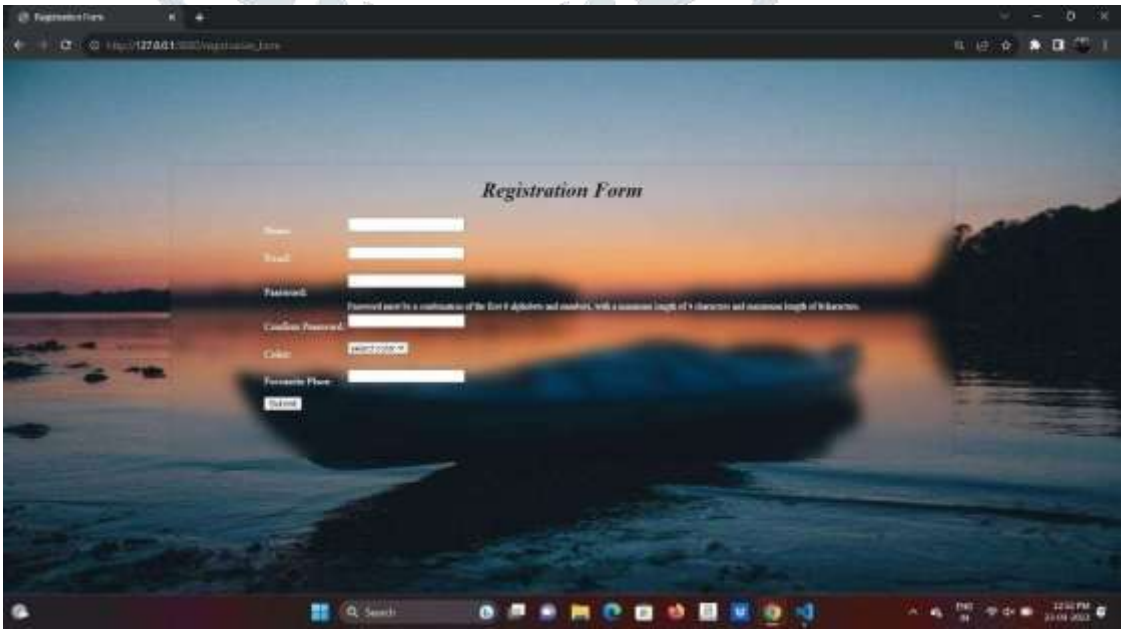


Fig1: Use Case Diagram

CLASS:



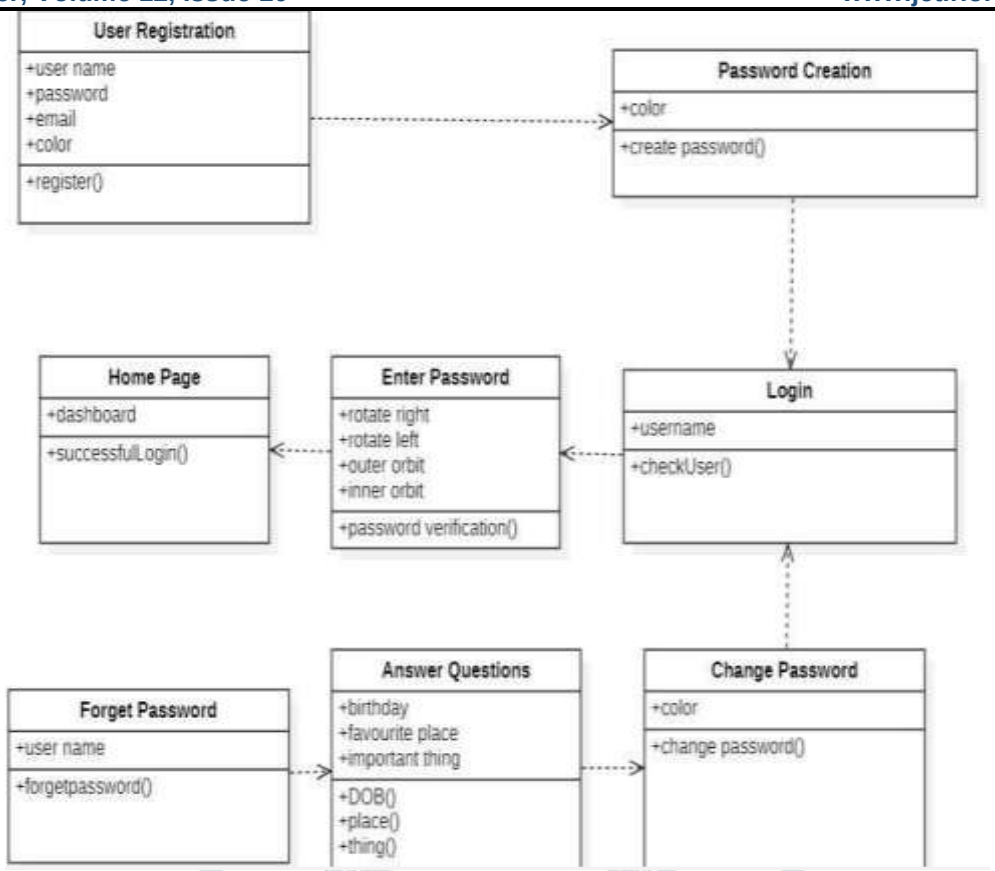


Fig2: Class diagram

Sequence Diagram:

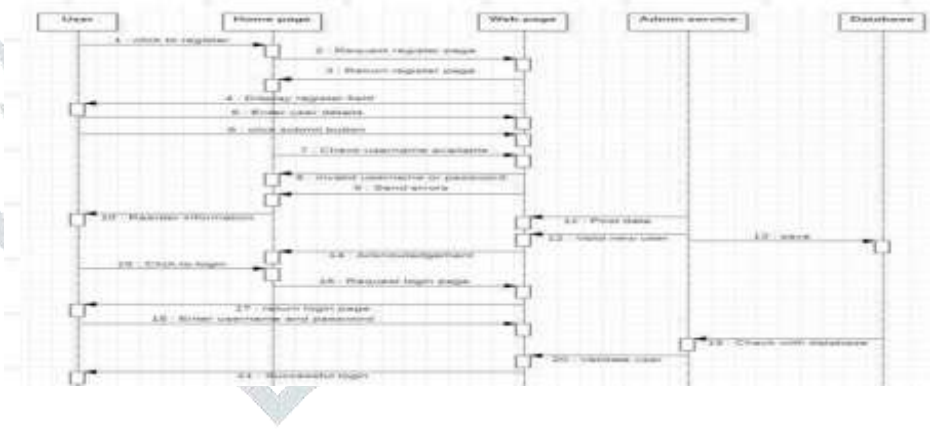
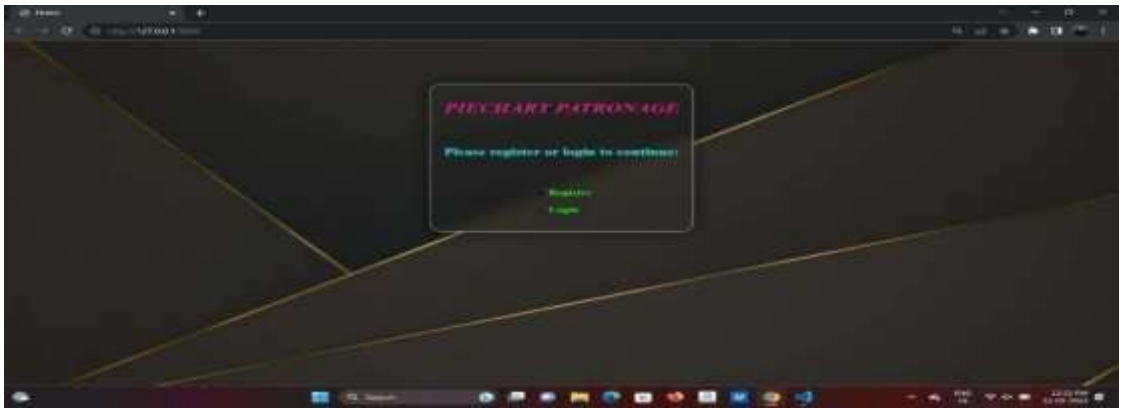


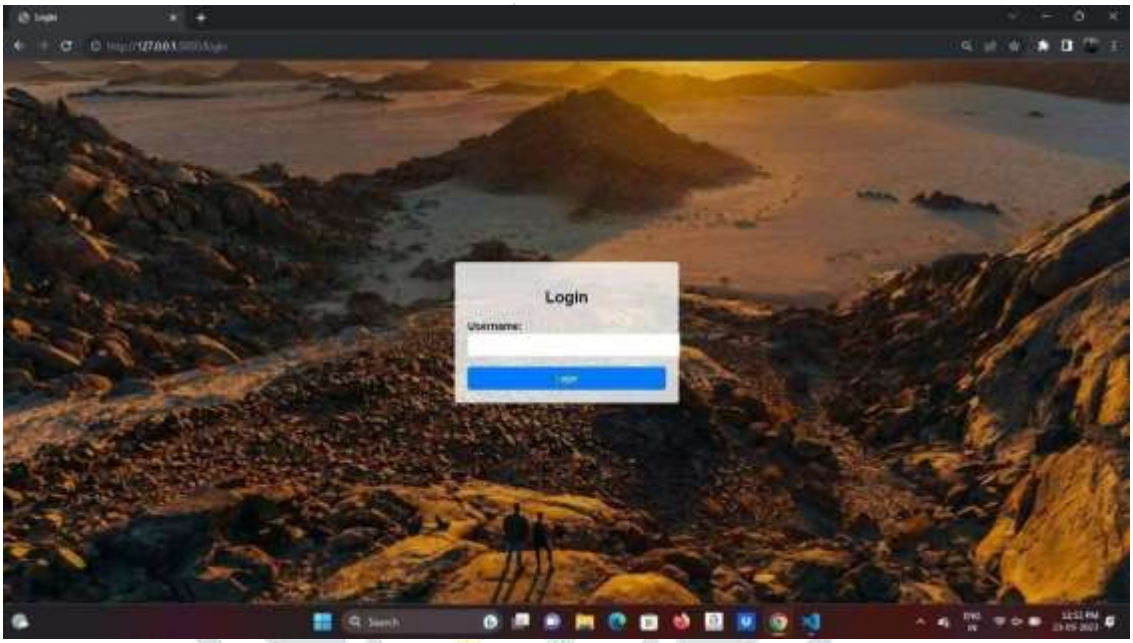
Fig 3: Sequence diagram

9. SCREENSHOTS

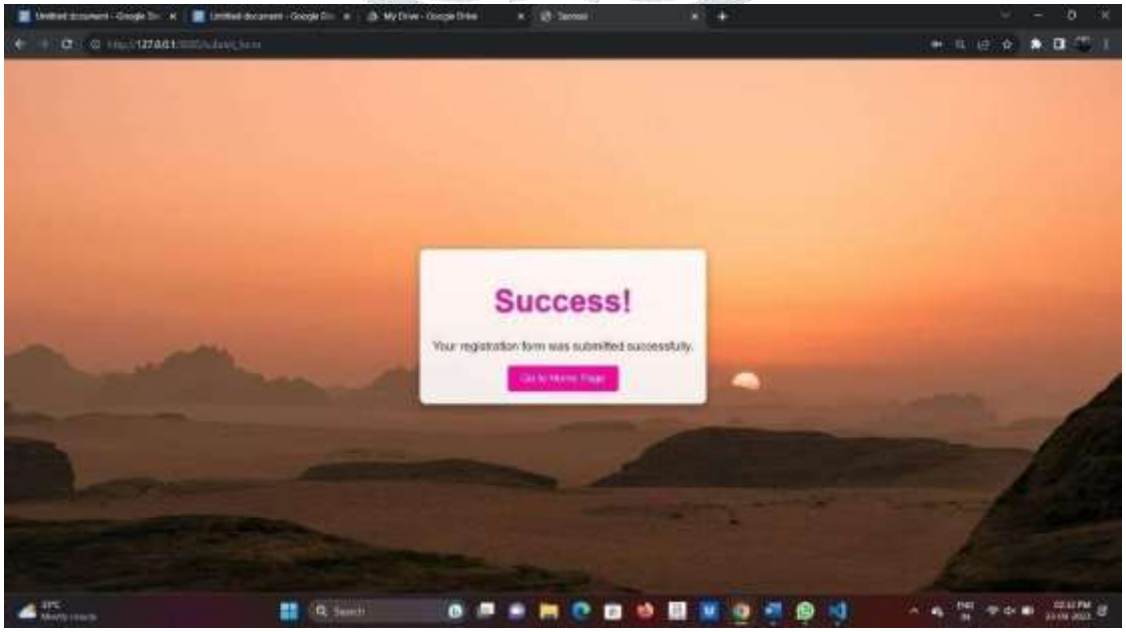
HOME PAGE:



Registration page: Login page:



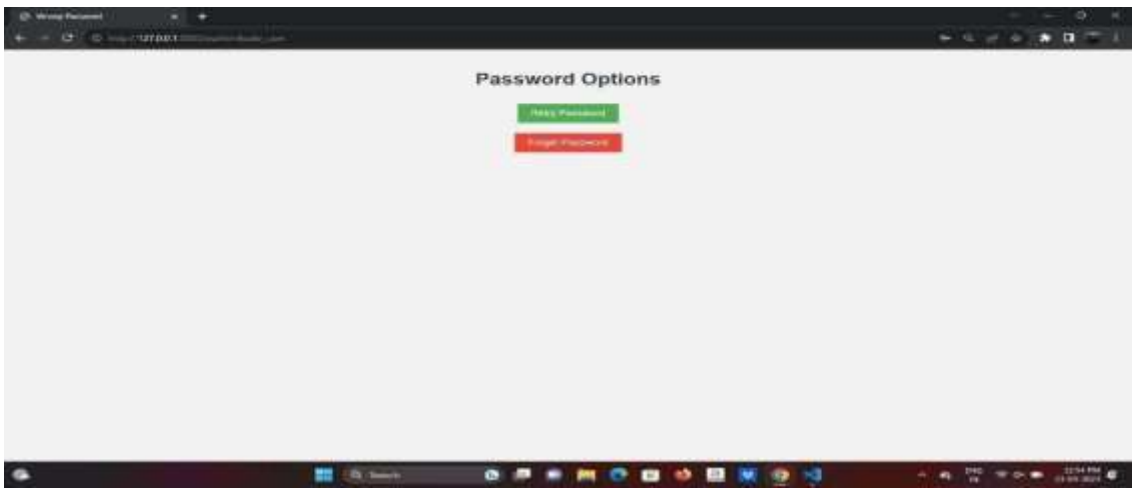
Successful page:



Password page:

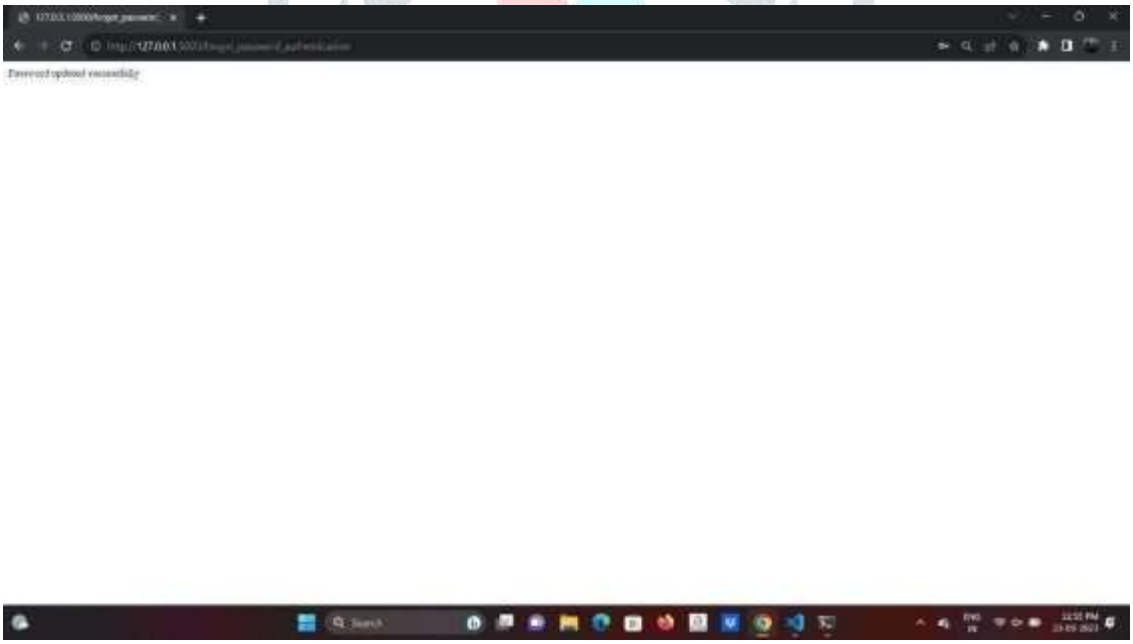
Login successful page:

Reset password:



Update password:

Password updated successfully:



Password not updated successfully:

10. *TESTING*

Software testing is a critical element of software quality assurance and represents the ultimate review of specification, design and coding. In fact, testing is the one step in the software engineering process that could be viewed as destructive rather than constructive. A strategy for software testing.

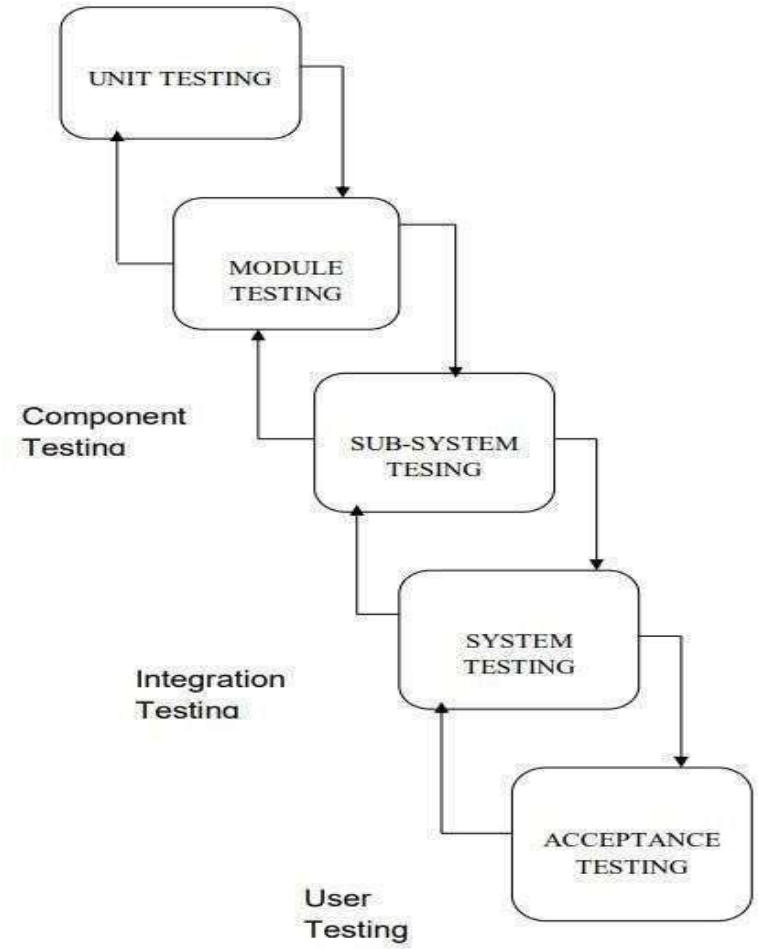


Fig: Software Testing Approach

11. *FUTURE ENHANCEMEMNTS*

1. *Biometric Integration:*

Integrating biometric authentication methods such as fingerprint recognition, facial recognition, or iris scanning alongside visual password authentication to provide an additional layer of security.

2. *Gesture-Based Authentication:*

Implementing gesture-based authentication, where users draw predefined patterns or shapes on the screen as part of their visual password.

3. *Machine Learning and AI:*

Leveraging machine learning and artificial intelligence algorithms to improve the recognition and validation of visual passwords, reducing false positives and enhancing security.

4. *Multi-Factor Authentication (MFA):*

Combining visual password authentication with other factors like something the user knows (traditional password) and something the user has (e.g., a mobile device) for stronger security.

5. *Augmented Reality (AR) Integration:*

Utilizing AR technology to enhance the visual password experience by allowing users to interact with 3D objects or holographic elements as part of their authentication process.

6. *Enhanced User Customization:*

Allowing users to customize their visual password environment further, such as choosing from a wider range of icons, themes, or visual elements for their authentication process.

7. *Behavioral Biometrics:*

Implementing behavioral biometrics, such as analyzing the way a user interacts with the screen or the timing of their interactions, to create unique patterns for authentication.

8. *Continuous Authentication:*

Moving beyond a one-time visual password entry and implementing continuous authentication methods that analyze user behavior throughout a session to detect anomalies or unauthorized access.

9. *Password less Authentication:*

Advancing visual password authentication to a completely password less model by relying on other user attributes or factors, like device identity and behavioral patterns.

10. *Usability Improvements:*

Focusing on improving the user interface and accessibility to ensure that users of all abilities can effectively use visual password authentication.

11. *Block chain Integration:*

Utilizing blockchain technology to enhance the security and integrity of visual password data storage and validation.

12. *Security Analytics and Threat Detection:*

Implementing advanced security analytics and threat detection mechanisms to detect and respond to unauthorized access or suspicious activity promptly.

13. *Compliance with Regulations:*

Ensuring that future enhancements align with evolving data privacy and security regulations to protect user data adequately.

14. *Cross-Platform Compatibility:*

Expanding the use of visual password authentication to various platforms, including mobile devices, IoT devices, and desktops, with seamless cross-platform compatibility.

15. *User Education and Training:*

Developing comprehensive user education and training programs to help users understand the importance of visual password security and best practices.

These future enhancements aim to make visual password authentication more secure, user-friendly, and adaptable to emerging technologies and user needs while ensuring robust protection against cyber threats.

12. *CONCLUSION*

Secure visual password system can be complex, as it requires a deep understanding of user behavior and potential threats.

Poorly designed systems may inadvertently introduce vulnerabilities.

Reset and Recovery: Resetting a visual password can be more complicated than resetting a traditional text-based password, as it may involve additional identity verification steps.

13. *FUTURE DIRECTIONS*

Visual password authentication has the potential to evolve and become more secure
and user-friendly. Future enhancements could include the integration of biometric authentication methods, advanced machine learning for better recognition, and improved accessibility features. Additionally, research into the development of standardized visual password frameworks could lead to more consistent and secure implementations.

In conclusion, visual password authentication presents an intriguing approach to user authentication, leveraging human visual memory. While it offers several advantages, including enhanced security and personalization, it also comes with notable challenges, such as susceptibility to shoulder surfing and usability issues. As technology and user expectations continue to evolve, the future of visual password authentication may see improvements in both security and usability, making it a more viable option for securing user accounts online. However, it's essential to consider the specific context and user base when deciding whether to implement visual password authentication or explore alternative authentication methods.

REFERENCE:

1. Piechart Patronage Bandi Krishna1 , Parsha Sravanthi 2 , Ramdas Vankdothu3 1,2,3 Dept of CSE, Balaji Institute of Technology and Science, Warangal, Telangana, India *https://doi.org/ 10.33472/AFJBS.6.Si2.2024.386-401* *Bandi Krishna / Afr.J.Bio.Sc. 6(Si2) (2024) 386-401* ISSN: 2663-2187

2. Ramdas Vankdothu, Dr.Mohd Abdul Hameed “A Security Applicable with Deep Learning Algorithm for Big Data Analysis”,Test Engineering & Management Journal,January-February 2020

3. Ramdas Vankdothu, G. Shyama Chandra Prasad “ A Study on Privacy Applicable Deep Learning Schemes for Big Data” Complexity International Journal, Volume 23, Issue 2, July-August 2019

4. Ramdas Vankdothu, Dr.Mohd Abdul Hameed, Husnah Fatima " Brain Image Recognition using Internet of Medical Things based Support Value based Adaptive Deep Neural Network" The International journal of analytical and experimental modal analysis, Volume XII, Issue IV, April/2020

5. Ramdas Vankdothu,Dr.Mohd Abdul Hameed, Husnah Fatima" Adaptive Features Selection and EDNN based Brain Image Recognition In Internet Of Medical Things " Journal of Engineering Sciences, Vol 11,Issue 4 , April/ 2020(UGC Care Journal)

6. Ramdas Vankdothu,Dr.Mohd Abdul Hameed, Husnah Fatima "Efficient Detection of Brain Tumor Using Unsupervised Modified Deep Belief Network in Big Data" Journal of Adv Research in Dynamical & Control Systems, Vol. 12, 2020.

7. Ramdas Vankdothu,Dr.Mohd Abdul Hameed, Husnah Fatima "Internet of Medical Things of Brain Image Recognition Algorithm and High Performance Computing by Convolutional Neural Network" International Journal of Advanced Science and Technology, Vol. 29, No. 6, (2020), pp. 2875 – 2881

8. Ramdas Vankdothu,Dr.Mohd Abdul Hameed, Husnah Fatima "Convolutional Neural Network- Based Brain Image Recognition Algorithm And High-Performance Computing", Journal Of Critical Reviews,Vol 7, Issue 08, 2020(Scopus Indexed)