EasyChair Preprint

№ 12539

Graphical Password Authentication

Venkata Siva Rama Krishna Bandaru, Saviour Badugu,
Deepak Bangi, Ch Bala Murali Krishna and Bhagyesha Pandhi

March 18, 2024

GRAPHICAL PASSWORD AUTHENTICATION

1st Venkata Siva Rama Krishna
Parul institute of Engineering and Technology
Parul University
Vadodara, India.
200303124131@paruluniversity.ac.in

2nd Saviour Badugu
Parul institute of Engineering and Technology
Parul University
Vadodara, India
Savisavi2@gmil.com

3rdBangi Deepak
Parul institute of Engineering and Technology
Parul University
Vadodara, India
deepakbangi18@gmail.com

4th Ch. Bala Murali Krishna
Parul institute of Engineering and Technology
Parul University
Vadodara, India
chbmuralikrishna4@gmail.com

5thBhagyeshaPandhi
Assistant Professor
Parul institute of Engineering and Technology
Parul University
Vadodara, India
bhagyesha.pandhi24831@paruluniversity.ac.in

I. ABSTRACT

Authentication is the approach for granting users access to framework objects in light of the client's uniqueness. If the code matches, the interaction will be completed, and the client will receive authorization to access the framework. Text-based secret word plots follow certain standards, such as having at least 8 characters in length. ought to join capitalized and lower-case and digits. Client have issue to recollect their convoluted secret phrase over the long haul because of the restriction of human mind, client will generally disregard their secret phrase. Client will generally utilize something similar secret key for all kind of record. Thus, assuming one record is hacked, the chances of another record being hacked are substantial. Other than that, picking the straightforward printed based secret word may build its weakness for assaults or interruptions. Thus, graphical secret key confirmation by utilizing passpoints conspire has been presented in this venture. Graphical secret key validation by utilizing passpoints plot is a model to recognize the most probable areas for client to click to make graphical secret word. The activity of the purposed conspire is basic and simple to learn for client since they recognizable with printed graphical secret word conspire. All in all, this graphical secret key plan will make it more straightforward for client to do their validation cycle since it is not difficult to recollect also, difficult to figure by others. Graphical Secure key approval by using passpoints plot is a model to perceive the most plausible regions for client to snap to make graphical mystery word. The action of the purposed system is essential and simple to understand for the client since it is prominent with printed graphical mystery word contrive. With everything taken into account, this graphical mystery key arrangement will make it more clear for client to do their approval cycle since it is easy to remember additionally, challenging to figure by others.

II. INTRODUCTION

Graphical Password confirmation is a technique for verification where clients are expected to utilize graphical components, like pictures, images, or shapes, rather than customary alphanumeric passwords. This technique has acquired consideration as an option in contrast to customary text based passwords because of its capability to be more significant and simpler to utilize Research on Graphical Password Authentication. Studies have demonstrated that graphical passwords are simpler to recall than typical text-based passwords, particularly for persons who are more visually oriented. However, users tend to choose simple and predictable images, which can make their passwords more vulnerable to guessing attacks. Usability Graphical passwords can be more user-friendly than text-based passwords, especially for users who have difficulty remembering complex passwords. However, the usability of graphical passwords can be influenced by parameters such as picture grid size, image count, and task difficulty. The security of graphical passwords can be influenced by a variety of factors, including the type of images used, their arrangement, the number of login tries permitted, and the complexity of the password. Some research have found that graphical passwords are more susceptible to shoulder surfing and smudge assaults than text-based passwords. Graphical password authentication is a topic that can be explored in various ways, with different levels of complexity and scope depending on the objectives and goals of the project. Here are some possible areas of focus for a graphical password authentication project: Design and assessment of graphical password schemes: creating and placing to the test novel graphical password schemes may be part of this project. It could include designing new types of images, icons, or symbols that users could use to create passwords. The project could also evaluate the usability, security, and memorability of the new graphical password schemes through user studiesandexperiments.

III. Literature Review

The research paper titled “Graphical Password Based Authentication Based System for Mobile Systems” by DAV University, Jalandhar, Punjab, India in 2019. [1] The study explains that the main advantage of graphical passwords is that they are easier to remember than text-based passwords. The study also identified some challenges to the implementation of the web-based platform, including limited access to internet and digital devices among some members of the community, a lack of awareness about the platform. [1]The paper provides an overview Graphical passwords provide a user-friendly alternative to traditional text-based passwords, but their usability and security aspects should be carefully considered and balanced for effective authentications. [1]Cued Click Points is an effective graphical password scheme that offers high memorability and resistance to shoulder surfing attacks, making it a viable option for enhancing user authentication. This study also attempts to establish the usability, efficiency, dependability, functionality, and portability of the proposed system once it has been deployed. Because the primary purpose of this research is to create a mobile and online application designed exclusively for user security and user friendly password to remember.

The research paper titled "Graphical Password scheme using color login" authored by H.Gao published in 2009. [2] The document offers a synopsis, Although graphical passwords are more accessible than conventional text-based passwords, their security and usability should be thoroughly considered in order to facilitate authentication is successful. During the login phase, four color pairs and an 8 by 8 matrix will be presented.[2]The password will be generated based on the user's color rating. A hybrid graphical password-based technique, which combines recognition and recall methods, has numerous advantages over existing systems and is more user-friendly.

The research paper titled "On the Usability and Security of Click-Based Graphical Passwords” by Springer in the Year 2020. [3]Click-based graphical passwords provide good usability and resistance against shoulder surfing, but their susceptibility to smudge attacks and pattern recognition attacks should be addressed for improved security. [3]Developing a graphical password type this helped to create some other types of graphical password authentication methods.Recall and recognition-based graphical password schemes offer varying levels of usability and security, and their strengths and weaknesses should be considered based on the target user population and threat model. [3]The methodology using pattern recognition and recall based techique for this authentication purposed and we are also used and implemethod this proposed flow.

The research paper titled "Graphical Passwords: A Survey by Blonder et al” published by IBM Thomas J. Watson Research Center in the Year 2020. [4] This preliminary survey article examines the concept of graphical passwords and their possible benefits over regular text-based passwords. [4]It discusses several graphical password methods, including their security, usability, and implementation issues. The report establishes the groundwork for future research in this area. [4]This paper introduces PassFaces, a graphical password authentication system that utilizes faces as authentication tokens.The authors discuss the usability and security of the system and provide insights into the human factors aspect of graphical passwords.

The research paper titled "Cued Click-Points: A Grid-Based Authentication Method” by Wiedenbeck et al” published by Springer in the Year 2019. [5]Proposed a grid-based graphical authentication method called Cued Click-Points. Users select specific points on an image to create a password.The paper discusses the security and usability aspects of this approach and compares it to other graphical password schemes.Discusses the integration of graphical passwords with smartcards for secure authentication. [5]Highlights the potential benefits of combining smartcards and graphical passwords.Reviews a decade of research in graphical passwords, including vulnerabilities and attack strategies.Identifies potential future research directions to enhance graphical password security.

The research paper titled "A Survey of Graphical Password Systems” by Dunphy and Yan published by Springer in the Year 2021. [6]Categorizes graphical password systems into recognition-based,recall-based,andcued-recall-based schemes.Evaluates the strengths and weaknesses of different types of graphical passwords. [6]Introduces a novel approach that combines biometrics with graphical passwords.Discusses the potential for improved security and usability in this hybrid authentication method.

The research paper titled "The Usability and Security of Gestural Passwords” by Jansen and Chiasson, Published by ACM (Association for Computing Machinery) in the Year 2022. [7]Focuses on gestural passwords, where users create passwords by drawing gestures on a touch screen.Analyzes the usability and security aspects of gestural password systems and potential challenges.Introduces Pass-Go, a graphical password system designed to enhance usability while maintaining security[7].Discusses how Pass-Go simplifies the password creation process while maintaining security. Focuses on the usability of graphical passwords on mobile devices, providing user-centered design recommendations. [7]Provides insights into the trade-offs between security and usability for different schemes.

The research paper titled "Study of Usability parameter for graphical Based Authentication System” by Dept. Of Computer Engineering, Shri Chhatrapati College Of Engineering, Nepti, Ahmednagar, Maharashtra, India in the Year 2020. [8]This study provides a study recall-based graphical password authentication schemes. The researchers study aims to analyze the usability aspect in the existing recall based authentication systems. [8]This paper provided a study that comprises of comprehensive reswarch in the graphical password schemes and evaluates each of available schemes. [8] The research examines ten recognition-based graphical password algorithms, as well as the prevalent usability and security issues associated with these systems.

IV. METHODOLOGY

In The proposed system for developing a graphical password and authentication system typically follows a structured path. It begins with project planning and requirements gathering, where the objectives and scope of the system are defined, and user requirements are collected. Extensive research is conducted to explore potential graphical elements for passwords and security measures. Once the conceptualization is complete, the system's architecture and user interfaces are designed, taking into account security and usability considerations. The actual implementation involves creating interfaces for password creation, authentication logic, and user management, all while prioritizing security measures. Extensive usability testing is carried out to ensure that the system is user-friendly, and performance optimization is performed for efficient authentication. Security testing, documentation, and compliance checks are essential steps before deployment. Continuous maintenance, updates, and user training are necessary for long-term success, and a feedback- driven approach ensures that the system evolves to meet evolving user needs and security threats. Throughout the entire project, collaboration with experts in security, usability, and legal compliance is crucial to deliver a robust and user-friendly graphical password and authentication system.

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

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

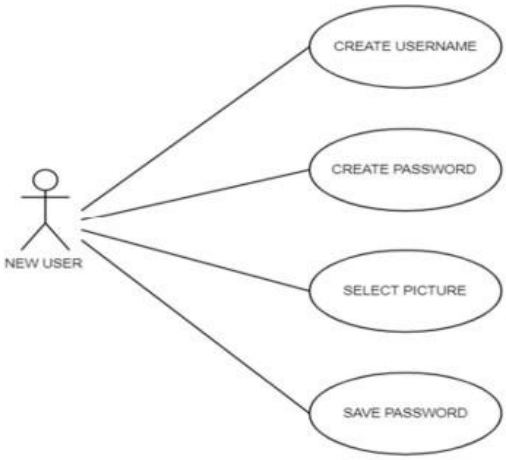
3. Admin Module:
In admin module, the administrator maintains the user details. The administrator maintains security to password.

4. Selection Method:
The user after registration has to choose his convinent type of graphical password that he has been need and liked.

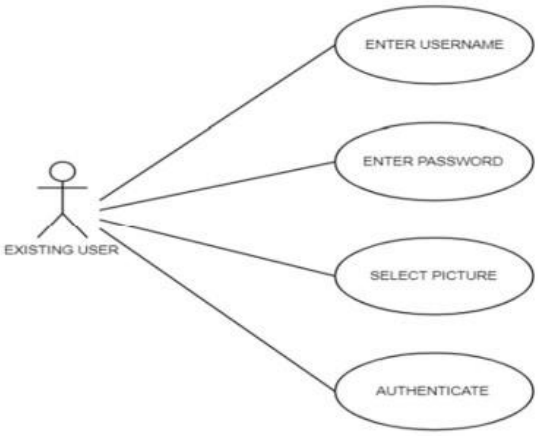
STEPS:

Step 1: Start the program.
Step 2: Select new user register.
Step 3: Fill your details.
Step 4: give your mail id.
Step 5: select the type of graphical password you liked.
Step 6: go on authentication process.
Step 7: verify the authentication process.
Step 8: if success it shows authentication successful.
Step 9: if not it won't allows to login.
Step 10: It makes the user alert.

USECASE DIAGRAM

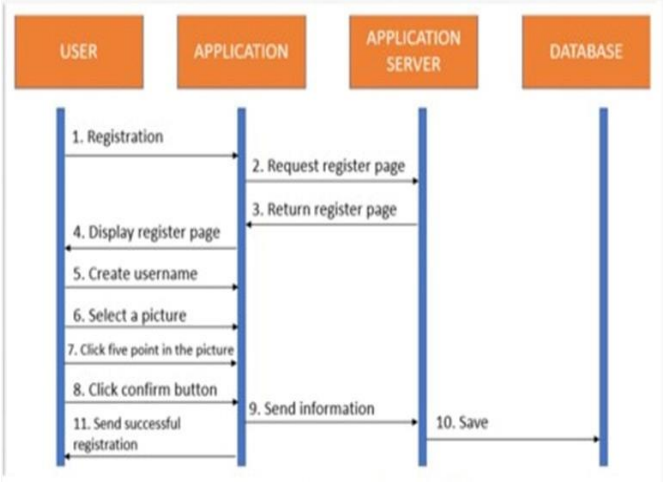


Use case diagram for new user

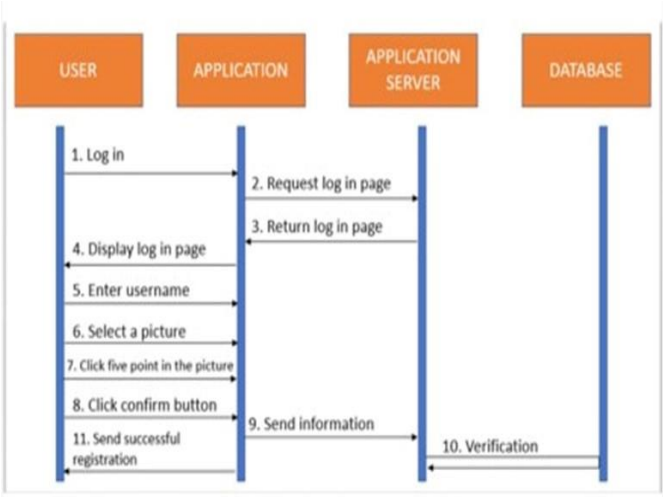


Use case diagram for exsisting user

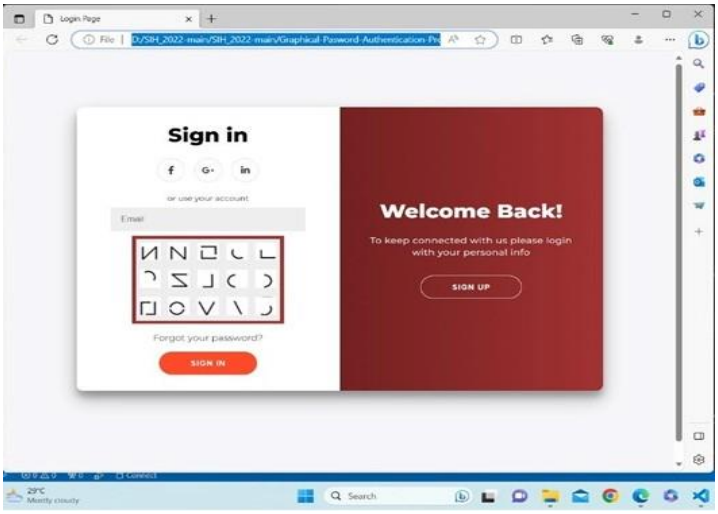
Sequence Diagram for Registration Page:



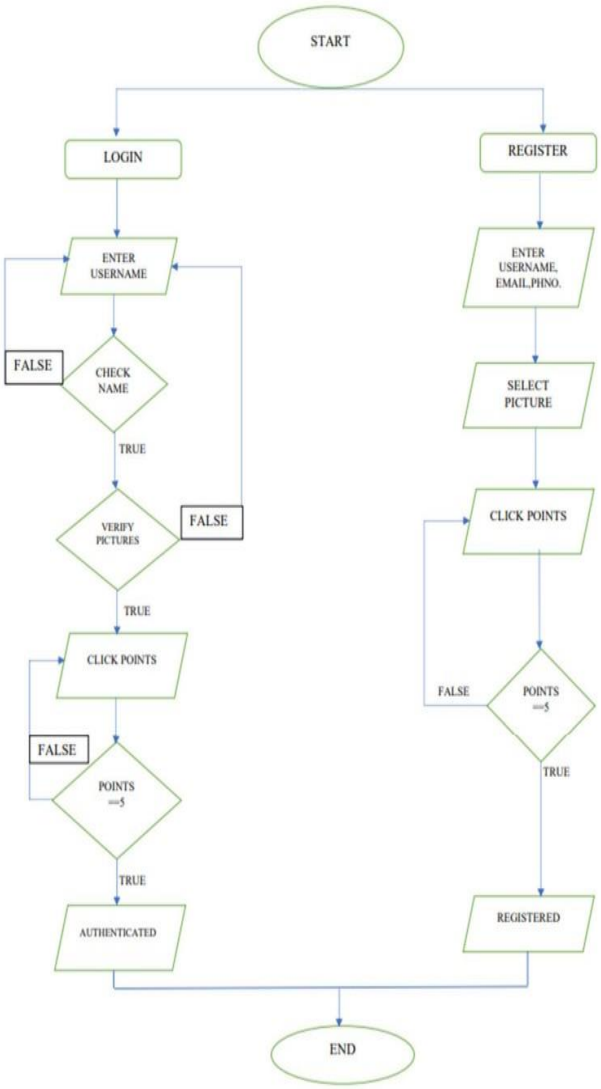
Sequence Diagram for Login page:



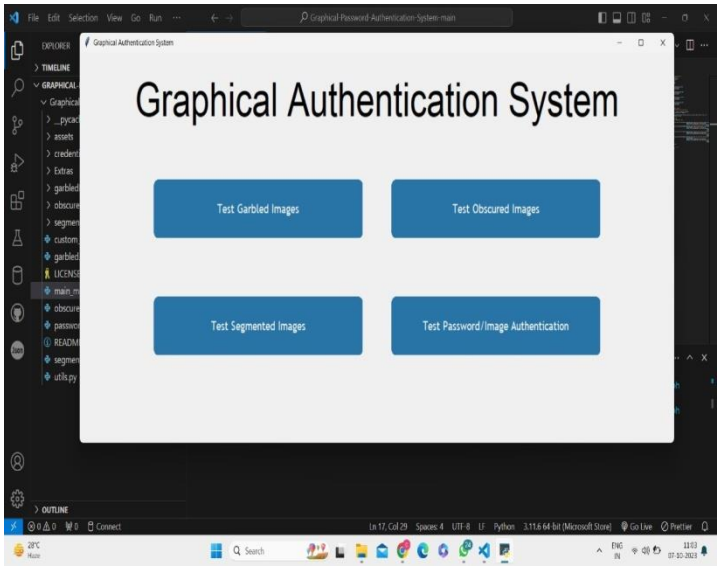
New User Registration:



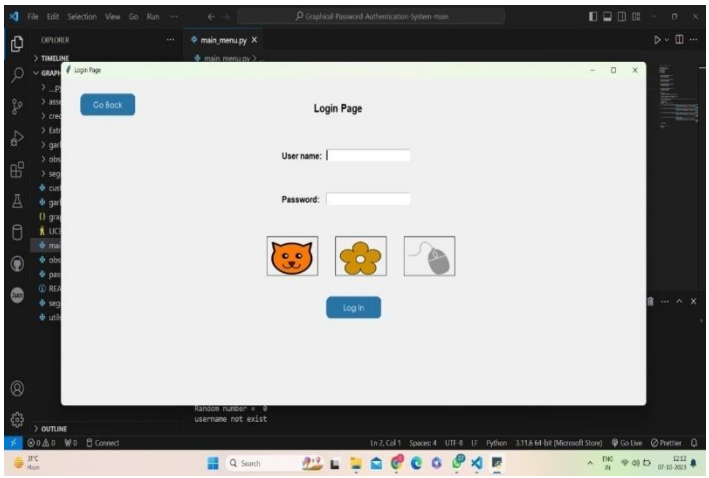
FLOW CHART:



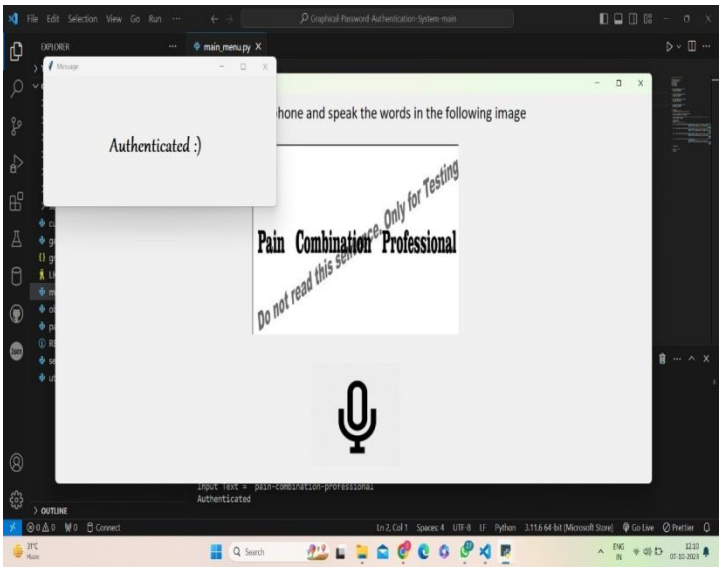
Graphical Password types:



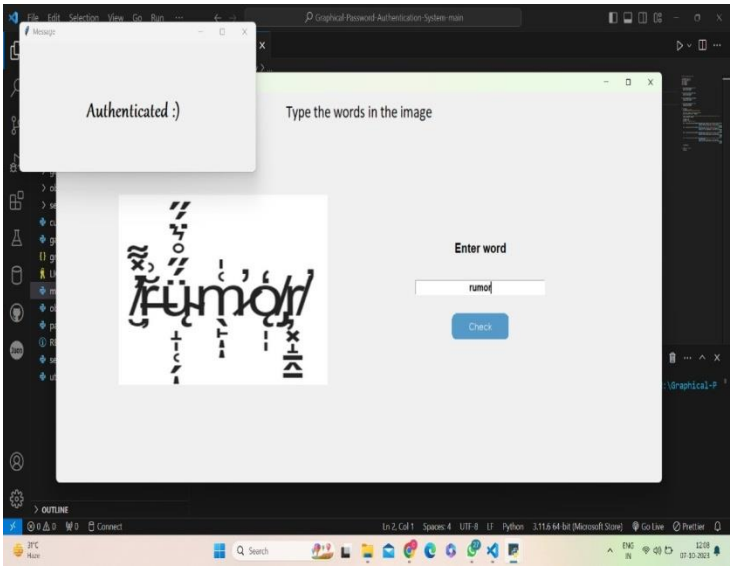
Test Password Image Authentication:



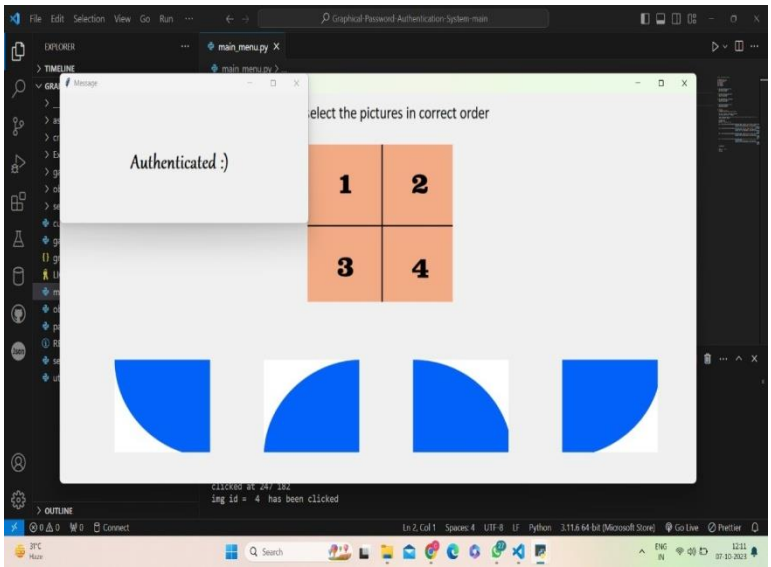
Test Obscured Image:



Test Garbled Image:



Test Segmented Image:



V. CONCLUSION AND FUTUREWORK

In conclusion, Graphical Password Authentication represents a promising and evolving approach to addressing the limitations of traditional text-based passwords. Over the years, extensive research has been conducted to explore various graphical password schemes, evaluate their usability and security, and propose innovative solutions to enhance user authentication.Graphical passwords offer several advantages, including the potential for increased security by leveraging users' visual memory and reducing vulnerability to dictionary attacks. Moreover, they have the potential to be more user-friendly and intuitive, particularly for individuals who struggle to remember complex alphanumeric passwords.However, the field of graphical password authentication is not without its challenges. Issues related to predictability, memorability, and the risk of shoulder surfing have raised concerns about the overall security of these systems. Additionally, achieving a balance between security and usability remains a key challenge, as more secure graphical password schemes tend to be less user-friendly, and vice versa. To advance graphical password authentication, ongoing research efforts are focused on addressing these challenges. These efforts include the development of hybrid approaches that combine graphical passwords with biometrics or other authentication factors, as well as the exploration of new graphical password schemes that strike a better balance between security and usability.As technology continues to evolve, graphical password authentication is likely to remain a relevant area of study and innovation. With the growing need for robust yet user-friendly authentication methods in an increasingly digital world, the continued exploration of graphical passwords offers the potential to provide secure and accessible solutions for users and organizations alike.

In Future we want to work in the field of graphical password authentication holds the potential for significant advancements in security, usability, and adaptability to emerging technologies. Hybrid Authentication Schemes: Investigate novel hybrid approaches that combine graphical passwords with other authentication factors, such as biometrics (e.g., fingerprint or facial recognition) or behavioral characteristics (e.g., keystroke dynamics). These hybrid systems can offer increased security while maintaining usabilits. Privacy-Preserving Graphical Passwords: Develop privacy-preserving graphical password schemes that protect user data and biometric infor Visual Cryptography: Investigate the use of visual cryptography techniques to enhance the security of graphical password authentication. Visual cryptography can provide a mechanism for securely splitting a password image into multiple shares.mation, ensuring that personal data is not exposed in case of system breaches. Multimodal Authentication: Research the integration of multiple authentication modalities, such as a combination of graphical passwords, biometrics, and traditional passwords, to create multi-layered security that is adaptable to different scenarios and threat levels. Continuous Authentication: Explore continuous authentication methods that continuously monitor user behavior and authenticate users based on ongoing interactions, reducing the risk of unauthorized access during a session.

REFERENCES

[1] Title: “graphical password scheme using color login”. Authors: H.Gao proposed paper Published: Journal of Cleaner Production, 2022.

[2] Title: Hybrid Textual Authentication Scheme. Authors: M. Sreelatha Published: The International Journal of Web-Based Learning and Teaching Technologies,2020.

[3] Title: “Graphical Password Based Authentication Based System for Mobile Systems”. Authors: Er. Aman Kumar, Er. Naveen Bilandi Published: Department of Computer Science and Engineering, DAV University, Jalandhar, Punjab.

[4] Title: “Password Authentication Using Text and Colors”. Authors: Miss.Swati Tidke, Miss Nagama Khan, Miss.Swati Balpande Published: Computer Engineering, RTM nagpur university, M.I.E.T Bhandara,.

[5] Title:, “Graphical Password as an OTP”. Authors: .Veena Rathanavel, Swati Mali Publisher:Department of Computer Engineering, K J Somaiya, College of Engineering Mumbai.Year:2021

[6] 6.Title:, “Color Shuffling Password Based Authentication”. Authors: Aayush Dilipkumar Jain, Ramkrishna Khetan Krishnakant Dubey, Prof. Harshali Rambade K. Elissa Publisher:Department of Information Technology Vidyalankar Institute of Technology, Mumbai, Year:2017.

[7] Title:”Towards Reliable Storage of Personal Identification Numbers and Passwords on Smartcards”. Authors: G. R. Blakley, P. D. MacKenzie, and W. D. Mills. Publisher:IEEE Transactions on Computers. Year:2021

[8]Title: ”PassFaces: A User Friendly Graphical Password System”. Authors: D. M. K. Jermyn,
A. Mayer, F. Monrose, M. K. Reiter, and A. D. Rubin . Publisher:USENIX Annual Technical Conference. Year:2018

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

[10] Title:”The Usability and Security of Gestural Passwords”. Authors: K. Jansen and S. Chiasson.Publisher:ACM Transactions on Computer-Human Interaction (TOCHI)Year:20