e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:06/Issue:04/April-2024 Impact Factor- 7.868 www.irjmets.com

WEB BASED GRAPHICAL PASSWORD AUTHENTICATION SYSTEM

Mrs. M Swarnanjali[*1], Burgula Vijay Prasanth[*2], Santelly Pavan[*3], Syed Wajid[*4]

[*1]Assistant Professor, Department Of Information Technology Malla Reddy College Of Engineering & Technology Hyderabad, India.

[*2,3,4]Final Year Student Department Of Information Technology Malla Reddy College Of Engineering & Technology Hyderabad, India.

ABSTRACT

This paper presents a project Medical Authentication dependent on passwords is utilized generally in applications for security and protection. Still, human actions, as an example, choosing bad passwords and contributing passwords in square measures are viewed as "the most fragile connection" in the Authentication chain. Algorithm used in this project is “persuasive cued click point algorithm” Maybe than discretionary alphanumeric strings, clients will pick passwords either short or significant for simple memorization.

To avoid this sort of issue, we need another method of confirmation. Here, we can choose a graphical authentication method. The image password offers the best approach to sign on that is simpler than recollecting and composing along with simple passwords. You can sign in by tapping the right points or creating the right gestures over an image that you just select in advance.

I. INTRODUCTION

The landscape of data analysis in the realm of the Olympic Games has evolved rapidly, with an increasing volume of complex and diverse datasets becoming available for exploration. Traditional methods of data analysis, though robust, often struggle to effectively communicate intricate patterns and trends inherent in Olympic data. The identification of crucial insights, which is essential for understanding the factors influencing countries' performances and contributions to the Games, can be hindered by the limitations of conventional approaches.

The primary objective of our research is to overcome the limitations posed by traditional data analysis methods and enhance the communicative potential of complex Olympic data. Through the development of a web application, we intend to empower users to interactively engage with the data, uncovering insights into the performance dynamics of countries in the Olympic Games.

II. LITERATURE REVIEW

[1] Graphical Authentication by Dhamija and Perrig :

Dhamija and Perrig proposed a technique for graphical passwords authentication where the user has to identify the defined images to prove their authenticity. In this, the user has to select set of images from a set of random images during registration and then during login the user has to identify those preselected images for authentication. This system is vulnerable to shoulder-surfing.

[2] Draw - a - Secret By Jermyn, et al:

Jermyn, et al. had proposed a method known as“Draw- a Secret” (DAS) where the user has to re-draw the predefined picture on a 2D grid and if the drawn picture touches the same grids in the same sequence, then the user is said to be authenticated. But this DAS scheme is vulnerable to shoulder surfing too.

[3] Passface Authentication :

Passface [2] is a technique developed where the user has to see a grid of nine faces and selects one face previously chosen by them. The user chooses four images of human as their password and the users have to select thei preselected image from eight other set of images. As there are four user pass images it is done for four times.

[4] Convex Hull for Graphical Password Authentication byWiedenback [3]:

Wiedenback et al [8] has proposed a graphical password entry scheme using convex hull method against shoulder surfing attacks. User must be able to recognize pass objects and click inside the convex hull formed by these pass objects. If user wants to make the password hard to guess, large set of objects can be used but it will

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:06/Issue:04/April-2024 Impact Factor- 7.868 www.irjmets.com

make the images look very crowded the objects almost indistinguishable. Using fewer objects may lead to a smaller password space resulting convex hull to be large.

[5] Blonder [5] has designed a graphical password scheme

where the user has to click on the approximated areas of pre-defined locations on particular image. Passlogix [6] elaborated this scheme by allowing the user to click on various objects in correct and ordered sequence to prove their authenticity. Haichang et al [7] also proposed a new scheme which was resistant to shoulder surfing where the user needs to draw a curve cross their password images sequentially instead of clicking them directly. The graphical scheme is combination of DAS and story schemes which provides authenticity to the user.

III. PROPOSED SYSTEM

At the time of registration, a user creates a graphical pass-word by first entering a picture he or she chooses. The user then chooses several point-of-interest(POI) regions in the picture. Each POI is described by a circle (center and radius).For every POI, the user types a word or phrase that would be associated with that POI. If the user does not type any text after selecting a POI, then that POI is associated with an empty string. The user can choose either to enforce the order of selecting POIs (stronger password), or to make the order insignificant.

1. Cued Click Points:

- Description: Users select a set of images, and each image has predefined click points. The order and location of the clicks become the password.
- Advantages: Combines the recognition of images with the precision of click points, potentially more secure.
- Disadvantages: Usability may vary, and users must remember both the images and click points.

2. Grid-Based Recognition:

- Description: Users select a grid of images, and the system validates the order in which the user clicks on certain portions of the images.
- Advantages: Provides a combination of image recognition and spatial memory.
- Disadvantages: Complexity may impact usability, and the system must be designed to prevent brute-force attacks.

3. Story-Based Authentication:

- Description: Users create a story by selecting images that represent elements of a narrative. The order and combination of images create a unique password.
- Advantages: Engaging and memorable, potentially more resistant to guessing.

IV. METHODOLOGY

A. Public Module:-

It is the overall viewing end of an individual website. Anyone with the URL can access this module. It is public however they can't change or alter the information.

B. User Module:-

The registered users are the part of user module. The user module consists of 2 functionalities - Registration and Login. During Registration, the system collects the basic details of the user like name, mobile and email, textual password, and graphical password. These all are encrypted and stored in the database. During the login phase, the user will give the username, textual password, and image password for accessing the resource. It compares the given values with data already given by the user at the registration phase. If it matched, then he/she will be logged into the page.

C. Account and Settings

This is the third module that contains the client' srecords and different settings of the computerized web stage. There is a link between the user module and the account module, If the user completes the registration, then the account will be created on the database. Also, the users can change their passwords at any time. Sign-in data, privacy and security choices, and so on are a benefit of it. Furthermore, clients can get warnings and request support from this part.

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:06/Issue:04/April-2024 Impact Factor- 7.868 www.irjmets.com

The image presents a detailed screenshot of a computer interface, likely from a specialized software application focused on security or encryption. The interface is divided into several sections, each containing different elements related to user authentication and system settings. Notably, there are fields for entering a "USER" name and "Password," alongside options for "Graphical Password" and an "ENCRYPT/DECRYPT" function, indicating a robust security feature that possibly involves image-based authentication methods. A section labeled "IMAGE SLICING ALGORITHM" suggests advanced security protocols or data handling processes are in place, potentially for enhancing the security of graphical passwords. Additionally, there are navigational elements for "Dashboard," "ACCOUNT & SETTINGS," and "HOME," along with a "PUBLIC REGISTER" option, which could imply that the software is designed for both individual and organizational use. The interface is predominantly white with text and icons suggesting a user-friendly and accessible design. The presence of "SQL" in the interface hints at database interaction or management capabilities within the software. Overall, the screenshot captures a comprehensive view of a sophisticated computer application that prioritizes security and user management, employing both traditional and graphical password systems

ALGORITHM;-

Image-based authentication:

This approach allows users to select images or graphical elements as their passwords. These images could be anything from photographs to abstract patterns.

Algorithms for processing and analyzing images play a crucial role in extracting meaningful features or patterns from the selected images.

Computer vision techniques are often employed to preprocess and analyze user-provided images. This may include tasks such as edge detection, feature extraction, and image segmentation.

Once the images are processed, the system may use algorithms to compare the features extracted from the user-selected images with the stored representations to authenticate the user.

Image-based authentication offers a visually intuitive way for users to authenticate themselves, and the use of images can potentially enhance security by making passwords more memorable and difficult to guess.

Graphical password schemes:

Graphical password schemes introduce alternative methods for users to authenticate themselves using graphical elements rather than traditional text-based passwords.

These schemes often involve specific interaction patterns or rules that users must follow to create and authenticate their passwords.

For example, Pass Points requires users to select a sequence of points or areas on an image as their password. The system then verifies the user's input by comparing it with the stored password template.

ClickText, on the other hand, requires users to click on specific words or letters within a grid of text. The sequence of clicks is then used to authenticate the user.

Algorithms for verifying graphical passwords in these schemes typically involve pattern matching, geometric calculations, or other techniques tailored to the specific requirements of each scheme.

Probabilistic password guessing:

Probabilistic password guessing involves assessing the security of graphical passwords by estimating the likelihood of successful guessing attacks.

These attacks may involve various strategies, such as brute-force attacks, dictionary attacks, or pattern-based attacks.

Algorithms for probabilistic password guessing analyze factors such as the complexity of graphical passwords, the number of available password choices, and the effectiveness of defense mechanisms against guessing attacks.

Machine learning techniques, such as Markov models or neural networks, may be used to model the behavior of attackers and predict the success rates of different attack strategies.

By quantifying the security of graphical passwords and identifying potential vulnerabilities, these algorithms help system designers optimize security parameters and implement effective defense mechanisms.

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:06/Issue:04/April-2024 Impact Factor- 7.868 www.irjmets.com

The Persuasive Cued Click Point (PCCP) algorithm is a graphical password scheme that aims to improve both security and usability by incorporating persuasive design principles. Let's delve deeper into its components and advantages:

1. User Interaction:

- In the PCCP algorithm, users interact with a grid of cells, each associated with a specific cue, such as a word or an image. These cues serve as hints or prompts for the user to remember their password sequence.
- During enrollment, users select a sequence of cells by clicking on them in the correct order based on the cues provided. This sequence becomes their graphical password.
- During authentication, users are presented with the same grid of cells and prompted to click on their pre-defined sequence of cells in the correct order to authenticate.

2. Persuasive Design Principles:

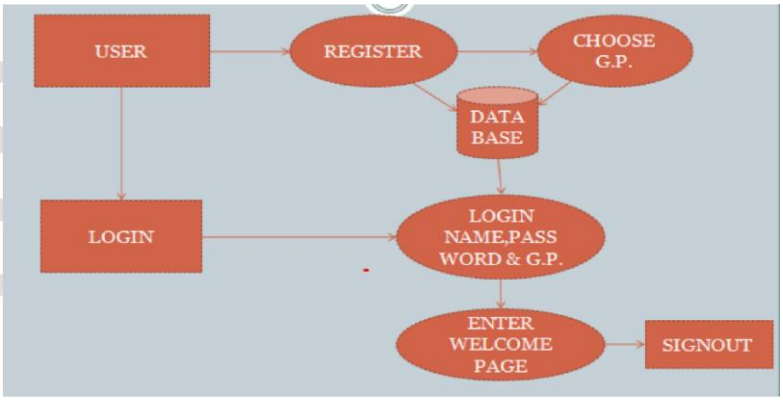
- **Salient Cues**: The cues associated with each cell are carefully chosen to be meaningful and memorable for the user. This makes it easier for users to recall their password sequence.
- **Progressive Disclosure:** The system may initially reveal only a subset of cues within the grid, gradually disclosing more cues as the user interacts with the system. This approach engages users and encourages exploration of the image, aiding in password creation and recall.
- **Feedback and Reinforcement**: Immediate feedback is provided to users during password entry, indicating whether each click is correct or incorrect. Positive reinforcement, such as visual cues or messages, is employed to reward correct actions and motivate users.

3. Security Measures:

- **Randomization:** To enhance security, the cues and their corresponding positions within the grid are randomized for each authentication attempt. This makes it difficult for attackers to predict the password sequence.

V. ARCHITECTURE

The architecture follows a modular and scalable design to accommodate various stages of data processing, model training, and evaluation, as well as deployment in real-world clinical settings.



The provided description paints a vivid picture of a meticulously crafted diagram illustrating the user login sequence. The diagram's primary function is to guide users through the process of accessing a system, starting with the decision-making path of choosing between "USER" or "REGISTER." This initial branching sets the tone for the user's journey, offering clear options for both new and returning users.

As the user progresses through the diagram, they encounter key steps such as selecting a "G.P." (graphical password) and interacting with a "DATA BASE" to authenticate their credentials. This process underscores the importance of security measures, such as the utilization of graphical passwords and interaction with a secure database, to ensure a robust authentication process.

The diagram then intricately details the steps for logging in, requiring the input of "NAME, PASSWORD & G.P." as credentials. This emphasis on multiple layers of authentication highlights the commitment to safeguarding user data and preventing unauthorized access. The sequential flow of the text elements suggests a logical order, guiding users through each step of the login process with clarity and precision.

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:06/Issue:04/April-2024 Impact Factor- 7.868 www.irjmets.com

VI. RESULT

Fig 1: Image of Overall Analysis

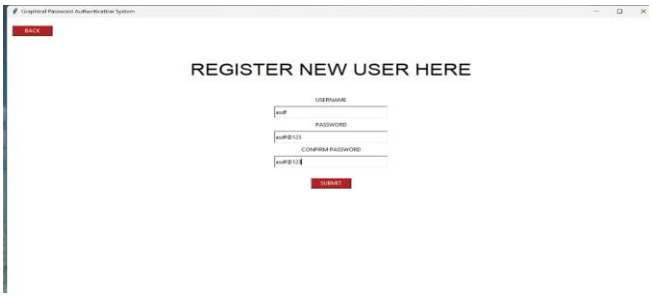


Fig 2: Image of login credentials

VII. CONCLUSION

To protect users digital property, authentication is required every time they try to access their account and data. Conducting the authentication process in public might result in potential shoulder surfing attacks. Using traditional textual passwords or PIN method, users need to type their passwords to authenticate themselves and thus these passwords can be revealed easily if someone peeks over their shoulder or uses video recording devices such as cell phones. To overcome this problem, we proposed a shoulder surfing-resistant authentication system based on graphical password. The past decade has shown a growing interest in using graphical passwords as an alternative to the traditional text based passwords. In this paper, we have conducted a comprehensive survey of existing graphical password techniques. Although the main use for graphical passwords is that people are better at memorizing graphical passwords than text-based passwords, the existing user studies are very limited and there is not yet convincing evidence to support this argument. Our preliminary analysis suggests that it is more difficult to break graphical passwords using the traditional attack methods such as brute force search, dictionary attack, or spyware. Overall, the current graphical password techniques are still immature. Much more research and user studies are needed for graphical password techniques to achieve higher levels of maturity and usefulness.

ACKNOWLEDGEMENT

The group express our gratitude most sincerely to our guide Mrs M. Swarnanjali who guided and motivated us in this course of time of understanding the concepts. We are grateful for the insightful comments offered by the peer reviewers.

VIII. REFERENCES

[1] Wantong zheng, Chunfu Jia, CombinedPWD: A New Password Authentication Mechanism Using Separators Between Keystrokes: 2017 13th International Conference on Computational Intelligence and Security (CIS).

[2] Salisu Ibrahim Yusuf, Moussa Mahamat Boukar, User Define Time Based Change Pattern Dynamic Password Authentication Scheme, 2018 14th International Conference on Electronics Computer.

[3] Yang Jingbo, Shen Pingping, A secure strong password authentiction protocol, 2010 2nd International Conference on Software Technology and Engineering.

[4] Hua Wang, Yao Guo, Xiangqun Chen, DPAC: A Reuse-Oriented Password Authentication Framework for Improving Password Security, 2008 11th IEEE High Assurance Systems Engineering Symposium.

[5] Salah Refish, PAC-RMPN: Password Authentication Code Based RMPN, 2018 International Conference on Advanced Science and Engineering (ICOASE).

[6] M Hamza Zaki, Adil Husain, M Sarosh Secure pattern-key based password authentication scheme2017 International Conference on Multimedia, Signal Processing and Communication Technologies (IMPACT).

[7] Vasundhara R Pagar, Rohini G Pise, Strengthening password security through honey word and Honey encryption technique, 2017 International Conference on Trends in Electronics and Informatics (ICEI).

[8] S. Sood, A. Sarje, and K. Singh, Cryptanalysis of password authentication schemes: Current status and key issues, in Methods and Models in Computer Science, 2009. ICM2CS 2009. Proceeding of International Conference on, Dec 2009, pp. 17.

[9] S. Gurav, L. Gawade, P. Rane, and N. Khochare, Graphical password authentication: Cloud securing scheme, in Electronic Systems, Signal Processing and Computing Technologies (ICESC), 2014 International Conference on, Jan 2014, pp. 479483