Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, Issue 5, No. 4, May : 2023

TO AVOID SHOULDER SURFING USING GRAPHICAL PASSWORD

Dr. Atul B. Kathole, Associate Professor, Dept. Of Computer Science, Dr. D. Y. Patil Institute of Technology, Savitribai Phule Pune University, Pune – 411017
Email : atul.kathole@dypvp.edu.in
Mr. Atharv Jaiswal, Ms. Sejal Chaudhari, Mr. Aditya Kapile, Student, Dept. Of Computer Science, Dr. D. Y. Patil Institute of Technology,Savitribai Phule Pune University, Pune – 411017

Abstract
Stealing a person's personal information, such as their identification number or password, by looking over the victim's shoulder is known as shoulder surfing. A graphical authentication device has been developed so that customers can use a couple of images as passwords. In order to prevent this, a hacker can now use a video digital camera to actively report a person entering the password to access private banking or social networking software. On this mission, we are able to handle two different kinds of picture authentication: one is a photo splitting method in which we can install a matrix grid over the image and choose a grid based on the password. the second is the photo covering approach where a chain of randomized numbers is produced over the photograph. Every time a user attempts to log in, there is an additional two-tier security measure that requires the creation of a brief login password. The transient password is only available for a limited time and is generated most efficiently when the user covers the ambient sensor. the two kinds of verification gadgets give an agreeable way to get the right of section to the application and make it impractical for programmers to advantage get the right of passage.

Keywords: Data Encryption Standard (DES), Authentication, Pass Points, Cued-Click Points (CCP), Graphical Passwords

Introduction

An alternative method of authentication that substitutes images or graphics for conventional alphanumeric passwords is known as graphical passwords. This approach expects to upgrade security by making it more challenging for aggressors to acquire the secret word through shoulder surfing, keylogging, or different types of perception. Attackers use shoulder surfing to look over the shoulder of the user as they enter sensitive information in order to obtain passwords or other information. When using graphical passwords, the user creates a password by selecting a sequence of images or clicking on particular areas of an image. This makes it more difficult for an attacker to observe the precise sequence of clicks. In a variety of applications, such as mobile devices, online banking, and e- commerce, the use of graphical passwords as a means of authentication is growing in popularity. This method not only improves security, but it also makes the authentication process easier to understand and use, which is especially helpful for people who have trouble remembering alphanumeric passwords. Cued Click Points (CCP)-based graphic passwords are a novel authentication method that addresses the shoulder surfing vulnerability of conventional alphanumeric passwords. Using a series of images and clues, this method creates a unique password that is hard for an attacker to see or copy. A series of click points within an image are selected for CCP graphical passwords based on predetermined prompts or cues. A user might be asked, for instance, to select all of the images that contain a particular color or shape, or to click on a particular area of an image. The mix of these snaps and prompts makes an extraordinary secret word that is challenging for an aggressor to figure or notice, regardless of whether they are watching the client enter the secret word. There are a number of advantages that CCP graphical passwords have over standard alphanumeric passwords. They are more secure and less prone to shoulder surfing attacks, first and foremost. Because they can use images and cues that users find meaningful, they are also easier for users to remember. Additionally, users with disabilities who may have difficulty using conventional alphanumeric passwords may find that CCP graphical passwords are more user-friendly.

Literature Survey

Graphical passwords are a better option than traditional text-based passwords because they are easier to use, easier to remember, and more resistant to dictionary attacks. In any case, one critical drawback of graphical passwords is that they are defenseless against shoulder riding assaults, where an aggressor can notice a client entering their secret phrase by investigating their shoulder or from a good ways. Researchers have proposed a variety of strategies for graphical passwords that are resistant to shoulder surfing attacks as a solution to this problem.

Here are some papers that discuss graphical password techniques for avoiding shoulder surfing:

1. **"A Semantic Differential-Based Graphical Password Scheme for Enhanced Security and Usability"** by M. Mahbubur Rahman et al. This paper proposes a new graphical password scheme that uses a semantic differential approach, where users select images that best represent their feelings about a given concept. The scheme is designed to be resistant to shoulder surfing attacks by requiring users to select images from different categories and by introducing noise into the image selection process.
2. **"IrisCode: A Shoulder-Surfing Resilient Graphical Password System based on Iris Recognition"** by Y. Zhang et al. This paper presents a graphical password scheme that uses iris recognition technology to enhance security and resistance to shoulder surfing attacks. Users select a series of iris images from a set of pre-registered images to create their password, and the system is designed to prevent shoulder surfing attacks by requiring users to select iris images from different angles.
3. **"GraSP: A Graphical Password Scheme with Privacy Protection and Shoulder-Surfing Resistance"** by S. K. Samanta et al. This paper proposes a graphical password scheme called GraSP that provides privacy protection and resistance to shoulder surfing attacks. The scheme uses a grid of images, and users select a series of images to create their password. The system is designed to prevent shoulder surfing attacks by requiring users to select images from different quadrants of the grid and by introducing random perturbations into the image selectionprocess.
4. "**Evaluating the Security of PassMatrix: A Shoulder-Surfing Resilient Graphical Password System**" by M. S. Islam et al. This paper evaluates the security of PassMatrix, a graphical password scheme that uses a grid of images and requires users to select a series of images to create their password. The system is designed to be resistant to shoulder surfing attacks by requiring users to select images from different rows and columns of the grid, and by introducing noise into the image selection process.
5. **"GazeGesture: A Gaze-Based Graphical Password Scheme Resilient to Shoulder-Surfing"** by S. M. R. Islam et al. This paper proposes a graphical password scheme called GazeGesture that uses gaze tracking technology to enhance security and resistance to shoulder surfing attacks. Users select a series of images from a grid, and the system tracks their gaze to determine which images they are looking at. The scheme is designed to prevent shoulder surfing attacks by requiring users to look at different regions of the grid and by introducing noise into the gaze tracking process.
6. **"Pass-Go: A Direction-Based Graphical Password System Resilient to Shoulder Surfing"** by Jianwei Zhang et al. This paper proposes a graphical password system where users select a sequence of directions on a grid to create their password. The system is designed to be resistant to shoulder surfing attacks by requiring users to enter the directions in a random order and by using a feature called "multi-level protection" that adds an additional layer of security.
7. **"A Graphical Password Scheme Resilient to Shoulder Surfing"** by Jinwei Zhang et al. This paper presents a graphical password scheme where users select a series of images from a large set of images to create their password. The system is designed to be resistant to shoulder surfing attacks by requiring users to select images from different regions of the screen and by using

feature called "image selection confusion" that makes it difficult for an attacker to determine the correct password.

8. **"Ripple Password: A Graphical Password Scheme Resilient to Shoulder Surfing Attacks"** by Lei Hu et al. This paper proposes a graphical password scheme where users select a series of points on a grid to create their password. The system is designed to be resistant to shoulder surfing attacks by using a feature called "ripple effects," which makes it difficult for an attacker to determine the correct password by observing the user's movements.

9. **"Memorability and Security: An Analysis of a Graphical Password System Resilient to Shoulder-Surfing"** by Arun Vishwanath and Sarah Edenhofer. This paper presents a study of a graphical password system called Passfaces, which requires users to select a series of faces from a large set of images to create their password. The study evaluates the system's memorability and security, as well as its resistance to shoulder surfing attacks.

10. **"Security Analysis of Two Graphical Password Schemes Resilient to Shoulder-Surfing"** by Sze Yan Chan et al. This paper analyzes the security of two graphical password schemes called PictureGrid and Picture Gesture Authentication (PGA). Both schemes use a grid of images, and users must select a series of images to create their password. The paper evaluates the schemes' resistance to shoulder surfing attacks and other security risks.

These papers demonstrate that researchers continue to explore new techniques and technologies to enhance the security and resistance to shoulder surfing attacks of graphical password systems.

Problem Statement

The goal of using graphical passwords to avoid shoulder surfing is to provide users who are concerned about others seeing or guessing their passwords with a more secure and user-friendly method of authentication. Shoulder surfers, who observe the user's keystrokes or screen to guess or steal their password, are able to attack traditional text-based passwords. On the other hand, graphical passwords rely on images, shapes, or patterns for authentication, making them more challenging for shoulder surfers to guess or observe. The point is to make a secret key validation strategy that is both secure and simple for clients to recollect and utilize. Because they can be more difficult for shoulder surfers to guess or observe, graphic passwords can offer a higher level of security than conventional text- based passwords. Because they can associate their password with a visual cue, users may be less likely to forget it if they choose a more complicated image or pattern to create their password. Generally, graphical passwords are a possible answer for the issue of shoulder surfing, however they likewise require cautious thought and testing to guarantee they give satisfactory security and ease of use to all clients.

Motivation

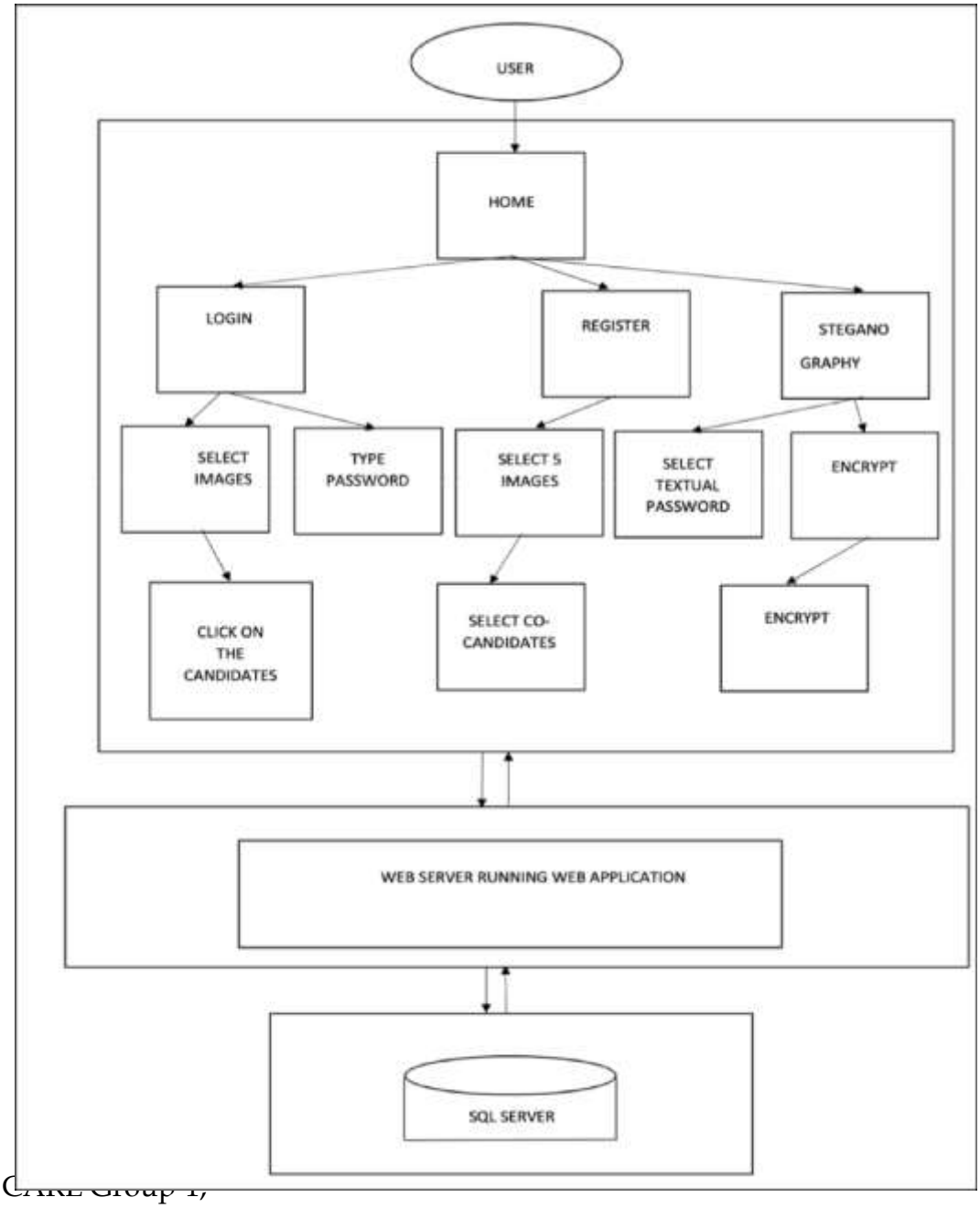
Due to the limitations of traditional text-based passwords, graphical passwords that are resistant to shoulder surfing attacks were developed. Text-based passwords can be effectively compromised in the event that an assailant can notice or get the secret key, either by investigating the client's shoulder, utilizing a camera or other reconnaissance innovation, or through friendly designing assaults. Graphical passwords, as opposed to conventional text-based passwords, may offer a number of potential advantages. They may, for instance, be simpler to remember and more challenging for intruders to guess. They can likewise give safer confirmation to clients who experience issues recollecting complex passwords. However, shoulder surfing attacks can still target graphical passwords. An attacker still has the ability to observe the user as they enter the password, allowing them to obtain the password and gain access to the user's account without authorization. Generally, the inspiration for creating graphical passwords that are impervious to bear riding assaults is to give clients a safer and dependable method for validating themselves without the gamble of their passwords beingundermined by aggressors.

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, Issue 5, No. 4, May : 2023

Proposed Methodology

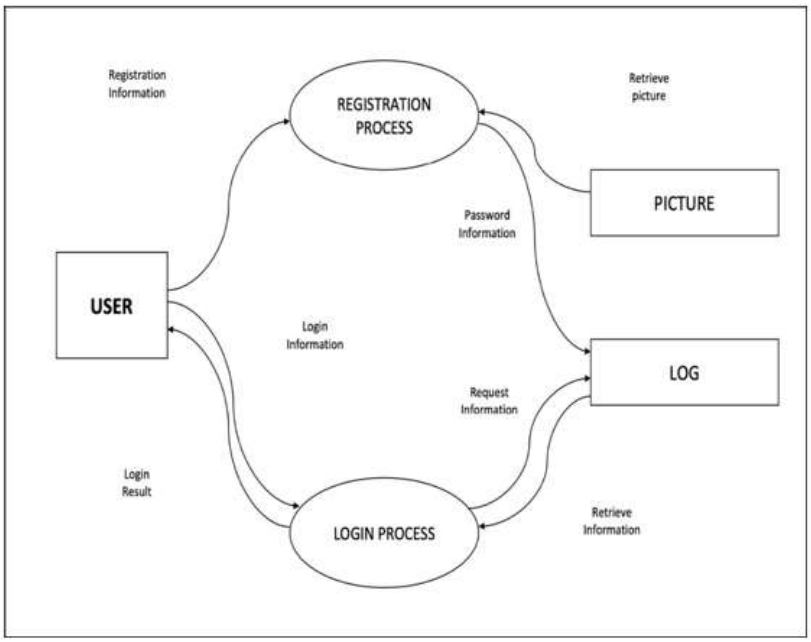
Cued Click Points (CCP)-based graphic passwords are a novel authentication method that addresses the shoulder surfing vulnerability of conventional alphanumeric passwords. Using a series of images and clues, this method creates a unique password that is hard for an attacker to see or copy. A series of click points within an image are selected for CCP graphical passwords based on predetermined prompts or cues. A user might be prompted, for instance, to select all of the images that contain a particular color or shape, or to click on a particular area of an image. The mix of these snaps and prompts makes an extraordinary secret word that is challenging for an aggressor to figure or notice, regardless of whether they are watching the client enter the secret word. There are a number of advantages that CCP graphical passwords have over standard alphanumeric passwords. They are more secure and less prone to shoulder surfing attacks, first and foremost. Because they can use images and cues that users find meaningful, they are also easier for users to remember. Additionally, users with disabilities who may have difficulty using conventional alphanumeric passwords may find that CCP graphical passwords are more user-friendly.

1) Architecture

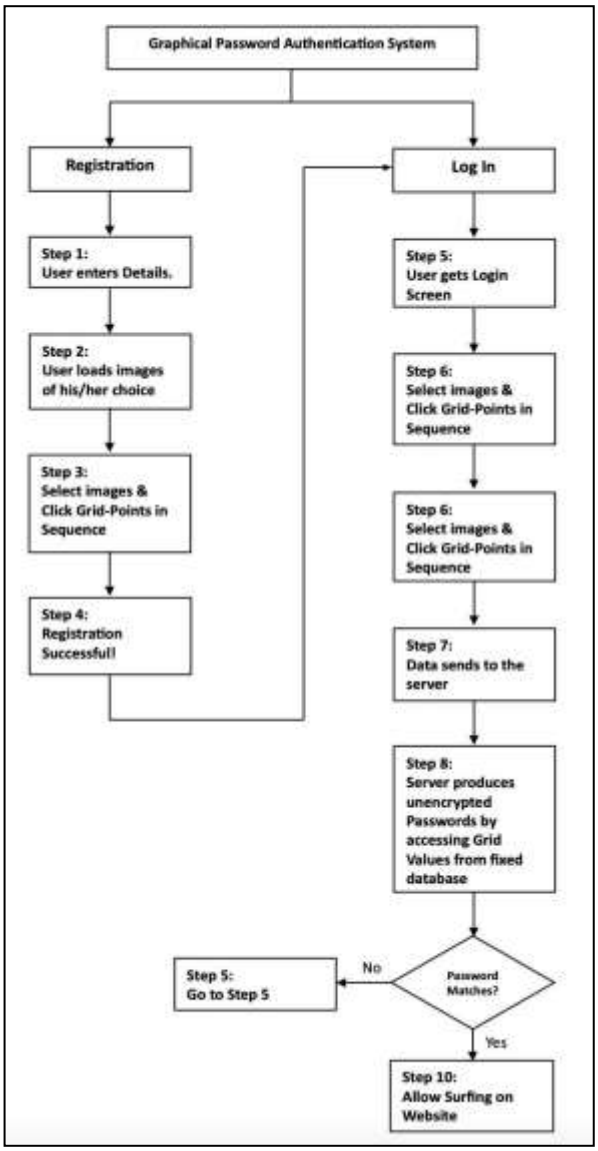


Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, Issue 5, No. 4, May : 2023

2) Plan of Execution



3) Flow Chart



Algorithm

Cued Click Point (CCP) Algorithm

A possible algorithm for a graphical password that is resistant to shoulder surfing attacks using CCP (Cued Click Point) could be as follows:

i. Create a pool of images: A set of images is selected from which the user will select an image to create their password. The images should be visually distinct and have a reasonable size to be easily recognizable by the user.

ii. Assign values to each image: Each image is assigned a value, typically an integer value,which is kept secret from the user.

iii. Select a click pattern: The user selects a pattern in which to click on the images. For example, the user may be asked to click on 3 images in a specific sequence.

iv. Determine click count values: For each image in the pattern, a click count value is calculated by multiplying the assigned value of the image by the position of the image in the pattern. For example, if the user selected a pattern of 3 images and the assigned values for the images were 2, 3, and 4, the click count values would be calculated as follows: (2 x 1) + (3 x 2) + (4 x 3) = 2 + 6 + 12 = 20.

v. Store click count values: The click count values are stored on the server side for authentication purposes.

vi. Authenticate user: To authenticate the user, the system displays a grid of images, with the user's selected images hidden among a larger set of decoy images. The user must click on their selected images in the correct pattern. Once the user has clicked on the correct images, the system calculates the click count values as in step 4, and compares them to the stored values on the server side. If the click count values match, the user is authenticated and granted access.

By using CCP, the graphical password is resistant to shoulder surfing attacks, as an attacker would not be able to observe the user's click pattern or the assigned values of the images. The use of decoy images further increases the security of the password, making it more difficult for attackers to guess the correctpattern

Confusion Matrix

In the case of a graphical password system to avoid shoulder surfing, the confusion matrix can be used to evaluate the accuracy of the system. Assuming that the graphical password system involves the user selecting a sequence of images from a grid of possible images, a confusion matrix for this system mightlook something like this :

	Shoulder surfer present	**No shoulder surfer present**
User authenticated	True Positive (TP)	False Positive (FP)
User not authenticated	False Negative (FN)	True Negative (TN)

In this table, TN represents the number of times the system correctly identified a negative (i.e., the user did not select the correct sequence), FP represents the number of times the system incorrectly identified a positive (i.e., the user did not select the correct sequence, but the system mistakenly accepted it), FN represents the number of times the system incorrectly identified a negative (i.e., the user selected the correct sequence, but the system mistakenly rejected it), and TP represents the number of times the system correctly identified a positive (i.e., the user selected the correct sequence).

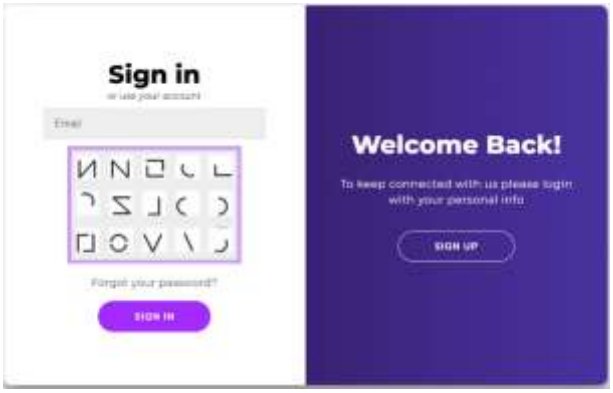
Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, Issue 5, No. 4, May : 2023

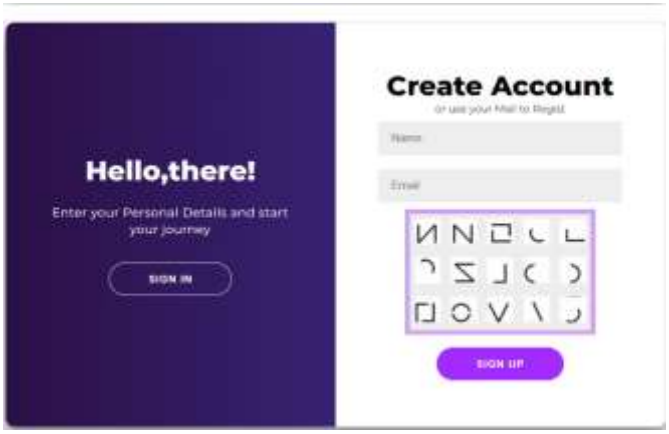
The accuracy of the system can be calculated as the sum of TN and TP divided by the total number of cases (TN + FP + FN + TP)

Future Scope

It has a wide future scope. It tends to be utilized wherever rather than text-based secret key or can be utilized as significant level security for text secret word moreover .We can expand the security of this framework by expanding the quantity of levels utilized, the quantity of resistance squares utilized. By and by there are numerous confirmation framework yet they enjoy their own benefits and hindrances. Biometric authentication can be more expensive, whereas a text password can be easily hacked using a variety of techniques. Old methods are more expensive and less secure than this system. Additionally, this system facilitates a system that is more dependable and user-friendly. Because of the way we've written it, this system might be better than a text password. It tends to be utilized wherever like guard administrations, banking areas and a lot more administrations to give best secret key system to client.

Result





Conclusion

Despite their effectiveness in preventing shoulder surfing, graphical passwords have their own set of difficulties. The possibility that users will select weak passwords that are simple to guess or duplicate is one cause for concern. Additionally, if they have multiple accounts with distinct password requirements, some users may have trouble remembering the images or patterns they chose as their passwords. Another cause for concern is the possibility that hackers might use social engineering or video recording to get users to reveal their graphical password. Additionally, a number of researchers have demonstrated that a variety of attacks may be used to guess particular

kinds of graphical passwords. Overall, graphical passwords can be a useful tool for preventing shoulder surfing; however, to provide the most robust protection for user accounts and devices, they should be used in conjunction with other security measures like two-factor authentication.

References

1. Ho Li, Yang, Xinyu Yun, Liming Fang, and Chunpeng Ge. 2021. "An Efficient Login Authentication System against Multiple Attacks in Mobile Devices" *Symmetry* 13 https://www.mdpi.com/2073-8994/13/1/125
2. Vaddeti, A.; Vidiyala, D.; Puritipati, V.; Ponnuru, R.B.; Shin, J.S.; Alavalapati, G.R. Graphical passwords: Behind the attainment of goals. *Secure. Priv.* 2020 https://www.ijsr.net/archive/v/11i2/SR22115013701.pdf
3. Yee, L.; Ku, C.S.; Ang, T.F. Preventing Shoulder-Surfing Attacks using Digraph SubstitutionRules and PassImage Output Feedback. *Symmetry* 2019 https://www.mdpi.com/2073-8994/11/9/1087
4. Fang, L.; Li, Y.; Yun, X.; Wen, Z.; Tanveer, M. THP: A Novel Authentication Scheme to Prevent Multiple Attacks in SDN-based IoT Network. *IEEE Internet Things J.* 2019 https://nesa.zju.edu.cn/download/THP_A_Novel_Authentication_Scheme_to_Prevent_Multiple Attacks in SDNbased IoT Network.pdf
5. Graphical Password Authentication, Mohini Patil, International Research Journal ofEngineering and Technology (IRJET), Volume: 06 Issue: 01 Jan 2019 https://www.irjet.net/archives/V6/i1/IRJET-V6I175.pdf
6. A Novel Hybrid Textual-Graphical Authentication Scheme With Better Security,Memorability, and Usability, March 26, 2021, IEEE,Shah zaman nizamani ,Syed raheel hassan ,Riaz ahmed shaikh ,Ehab atif abozinadah , Rashid Mehmood https://ueaeprints.uea.ac.uk/id/eprint/85251/1/A_Novel_Hybrid_Textual_Graphical_Authentication_Scheme_With_Better_Security_Memorability_and_Usability.pdf
7. g-RAT A Novel Graphical Randomized Authentication Technique for Consumer Smart Devices, M. A. Khan, U. Din, S. U. Jadoon, M. K. Khan, M. Guizani, K. A. Awan, IEEETransactions on Consumer Electronics, vol. 65, no. 2, pp. 215-223, 2019. https://sci-hub.se/10.1109/TCE.2019.2895715
8. TCpC: a graphical password scheme ensuring authentication for IoT resources, Priya Matta, Bhaskar Pant, International Journal of Information Technology, vol. 12, pp. 699-709, 2020, https://sci-hub.se/10.1007/s41870-018-0142-z
9. Jumbled pass steps: a hotspot guessing attack-resistant graphical password authentication scheme based on the modified pass matrix method, Jerome P. Songcuan, Ariel M. Sison, Proceedings of the 3rd International Conference on Cryptography, Security and Privacy, KualaLumpur, Malaysia, 2019 https://sci-hub.se/10.1145/3309074.3309099
10. Graphical Password to avoid Shoulder-Surfing,Bharathepudi Sri Himaja, Potluri Uday Teja, Maddirala Viswanadha Kashyap, Sajja Poorna Chand,Gogineni Krishna Chaitanya, Journal of Xi'an University of Architecture & Technology Volume XII, Issue IV, 2020 http://www.xajzkjdx.cn/gallery/531-april2020.pdf