WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

A Review on Cued Click Points Graphical Password Authentication in Web Security

S. Dhivyalakshmi Narayanan [a], Dr. S. Prabhu [b]*

[a] *PG Scholar, Department of Computer Science and Engineering, Nandha Engineering College (Autonomous), Erode, Tamilnadu, India*
[b] *Associate Professor, Department of Computer Science and Engineering, Nandha Engineering College (Autonomous), Erode, Tamilnadu, India*

A B S T R A C T

Cued Click Points (CCP) is a graphical password authentication technique which comes under Authentication a subdomain of web security.The key area in security research is authentication which determine of whether a user should be allowed to access the given system . Authentication is a process of a system which verifies the identity of a user. Authentication is generalized by saying “to authenticate” means “to authorize”. A graphical password is an authentication system which makes the user select images in a specific order that presented in a graphical user interface. Textual alphanumeric password are alternated by Graphical Password s. Graphical password are easy to remember but hard to guess. An important goal for authentication system is to support the users in selecting the better password, thus increasing security .In Cued Click Point, the Users click on one point per image of a sequence of images. The next image will be displayed based on the previous click-point. It improves the performance in terms of speed, accuracy, and number of errors. Cued Click Points (CCP) provides high security because the sequence of images increases the workload for attackers. In increasing the number of images and number of grids in Password , the security and efficiency will be very high.

Keywords: Authentication, Graphical Password, Cued Click Points

1. Introduction

Web Security

Web Security is very important nowadays. Websites are always prone to security threats/risks. Web Security deals with security of the data which is being transferred to the internet. When data is transferring between client and server and the data have to protected that security of data is web security.Hacking a Website may result in the theft of Important data like credit card details or the login information. it can bring destruction of one’s business like propagation of illegal content to the users or steal important data of the customer through the website . Therefore, security are highly considered in the context of web security.

Authentication

Authentication technology provides access control for the systems by checking user's credentials matches with the credentials in a database of authorized users. Authentication assures secure systems, processes and enterprise information security. Authentication enables system to keep their networks secure by permitting only authenticated users . Authentication may includes in computer systems, networks, databases, websites and other network-based applications or services.

Graphical Password Authentication

In the graphical password authentication, the user selects points of images in a specific order presented in a graphical user interface (GUI). According to a study, the human brain has a greater remembering of what they see(pictures) rather than alphanumeric characters.Graphical passwords is used to overcome the disadvantage of textual alphanumeric passwords. Cued Click Points technique (CCP) is an alternative to the Pass Points technique. In CCP, users click one point on each image unlike Pass Points in which five points is clicked on one image. It alerts the users if they make any mistake while entering.

2. Literature Survey

2.1 Cued Click Points Password Authentication using Picture Grids

The main problem with password authentication is that users tend to use simple, easy-to-remember passwords rather than strong passwords. Passwords that are hard to remember. Users typically write down their passwords and share them with others, use the same password on multiple systems, and

possibly add extra digits end. This makes it easier for attackers to guess passwords. To get around this you should use a picture password .An alternative to alphanumeric passwords where the user clicks on an image/grid to authenticate. Instead of 5 click points (pass point system) he on the image uses 1 click cued click points (CCP). Dots on 5 different images. The input image is first split into equal numbers of rows and columns. Password setting. Registration is 3 clicks away. That's the click point for each image. assign image Each grid path in 3 steps. Three photos are displayed in succession. User will see the following image Creates a path through a series of images based on previously entered click point locations. user Only select images until the click point determines the next image. create something new Password users use different image sequences with different click points. is displayed when you log in The unrecognizable image warns the user that the previous click point was wrong and allows the user to restart Enter password. Explicit indication of authentication errors is provided only after the last click point. Protection against incremental guessing attacks.

2.2. User Authentication Through Cued Click Points Based Graphical Password

User authentication is a fundamental component in most computer security contexts. lastly For many years, computer and network security have been viewed as technical issues. Critical Areas of Security Research is authentication, which determines whether a user is allowed access to a particular data source. system or resource. In this respect, authentication is the process by which a system confirms the identity of an individual user. Authentication can also be generalized to say "authenticate" means "authorize". user They tend to choose passwords that are easy to guess. But if the password is hard to guess this is It is often difficult to remember. To address this issue, some researchers have developed authentication. A method of using images as passwords, so-called graphical passwords. Users preferred her CCP over Passpoint. For each frame user selects only one point that is easy to remember and that it triggers seeing each frame A memory of where the corresponding points were. In Cued's click-based graphical password The image is displayed on the screen by the system. The image is no secret and has no other role. Help users remember click points. Every pixel in the image becomes a candidate click point. To sign in, The user must click again near the selected points in the specified order. because it's almost impossible The system is error tolerant so that a human user can repeatedly click on the exact location. Click position. This is done by quantizing (discretizing) the click position using three different squares grid.

2.3. Three Factor Graphical Authentication Mechanism

Proposing a new graphical password authentication technology that is resistant to shoulder surfing Other types of attacks are also possible in part. This is a combination of detection and memory An approach designed to reduce and reduce patterns.PCCP (Persuasive Cued Click Points) Take advantage of hotspots for attackers. Instead of his sequence of 5 click points on the image, PCCP uses this. Click points on 5 different images displayed in sequence.The image below is based on The previously entered click point. Create a password with different click points to get a unique picture sequence. User's e-mail Enter her address. Select 4 images in the order you selected them when registering. Select a click point from two images. In the image grid, select and enter the position of the 1st and 4th images Text box. When a user enters an incorrect password he enters 3 times, an email should automatically be sent to the specific user and the password should be reset. Therefore, the main advantage of PCCCP is that it is possible to attack the system. It's very difficult because the attacker can't tell if he tries the order of the click points. No warnings are issued for illegal image sequences, so the registered image sequences are deleted

2.4. Graphical Based Authentication Using Cued Click and Binary OTP

The user registers by entering the required data and the required click points on the image. Registration: When a user registers, they are prompted for a username and receive an OTP by email. When emailed, the user has to click the selected area on the image according to her OTP. After entering If it matches the registered data, registration is successful. By chance it shows the wrong random image when clicked appear. This means that authentication will be denied. In this project, users will implement random images. Click the wrong area. The user must log in again for authentication to succeed.

2.5. Preventing Shoulder Surfing Attack in graphical password authentication scheme

During the registration phase, users provide their information, name, You have to choose 6 images from the image set provided as her passport, such as phone number and email address. Image after the information is saved in the system database. The system stores 6 images of her in the following formats: Use a 2x3 matrix as template A. The user then also selects three more images and the system saves them to: As template B he creates a 3x1 matrix. Multiply the matrix from template A by the matrix from template B. Form a 2x1 matrix M in the database. Multiplication of two matrices is made possible by the following numbers: The number of columns in matrix A equals the number of rows in matrix B. During authentication, if the user chooses to Log in using the password/PIN generated during registration. The system provides a random set of images It also includes the image you selected during registration. User must be cognitively active in making choices The photo is used as a password/PIN and there is a certain amount of time during which the user can complete the login operation. A user named If a user cannot complete the login operation within a certain period of time, the system will automatically log out the user. The system first validates the image submitted for registration and the user's email address to see if there are any similarities. between them. Finally, the system uses the six selected images to form matrix A, and the three selected images of her. Form a matrix B from the image, then multiply matrix A by matrix B to form a matrix. of Next, the system checks whether the matrices formed during registration match. Matrix formed during authentication. This is true if there is a relationship between the M reg and the user. If not enabled, users will be denied access. The shoulder surf attack has been eliminated. Opponents can only see her two matrices. H. Matrix A and Matrix B, but the result of multiplication The Matrix M reg remains invisible to the attacker. Therefore, it is difficult for attackers to find relationships Between M reg and M auth

2.6. Graphical based Authentication System using Keystroke Parameters and Cued Click- Points

The goal of this system is to develop a graphic-based dynamic authentication system with password keying. of this system provides better protection and confidentiality. User authentication based on typing rhythm user's. If you click rhythmically, the mouse makes sounds that annoy others. You can easily see and hear your click rhythms and imitate their speed and tempo. Pretend to be a user. The user then specifies a checkpoint for each image. B. For specific images If the partition is 3, the image is divided into her 3x3 matrices and the checkpoint is a combination of these. Rows and columns (1,2), (2,2), etc. Images and their respective control points are saved in the database. KDA More Parameters can be measured by down-up time (DU), down-down time (DD), up-down time (UD), and upup time. (UU) time, down-up 2 (DU2) times. During registration, the system compares registered parameters. If the keypress parameters at login match, graphical password authentication opens. window. After the user enters the click point (specified during registration), the system checks in. The database uses CCP. If the checkpoint for each image matches the checkpoint stored in the database, the user Registration was successful.

2.7.Web Application Authentication Using Visual Cryptography and Cued Clicked Point Recall-based Graphical Password

Visual cryptography is a cryptographic technique that allows the processing of visual information (images and text). It is encoded and decoded in such a way that the decoded data is displayed as a visual image. Here is the binary image: It can be split into parts and stacked to resemble the original image. data completed It cannot be recognized if it is hidden behind another image (so-called shared). At this stage, the user is asked to upload an image of their choice. This uploaded image is encrypted and converted into two images. Share images using visual encryption technology. The user will be prompted to download and save the file. Between these two images. These generated images are saved in a database for further use. data is retrieved The phase gets user details such as user id, email id, password, full name and phone number. Do you get itIn the data phase, user details such as user id, email id, password, full name and phone number are captured. The user is presented with a 2x2 image grid of her, from which they click on an image point. rear

This requires the user to select a different image and click on a 2x2 image grid of her generated.

2.8.Cued Click Point Based Authentication

Structuring framework using pixels of graphic images. The password depends on the client being validated. We encourage our customers to use her CCP framework Choose stronger passwords and make password choices increasingly difficult. especially, When the customer entered the password, the image was slightly shaded except for one random character . Positioned viewport are placed haphazardly and not specifically to maintain strategic alignment. Remove known hotspots. Such data can be used by attackers to improve their inferences, so It may also encourage the establishment of new hotspots. The viewport size is It has many distinctive points, but at the same time spreads only a small part of the whole possible point. The size of the viewing window depends on the resistor selected by the customer. customer The click point had to be selected within this highlighted viewport and was not allowed to click outside this viewport. In case you were hesitant or unable to select a click point in that district, By pressing the Revive button, you can freely change the position of the viewport. While the customer was allowed Rearranging passwords as often as necessary interferes with the entire password creation process. Viewport And then an encouraging catch appeared during password creation. Happens between password confirmation and registration Images were displayed regularly without shading or viewports, and customers could click anywhere. If the customer misses a point, a new image will be displayed as needed Please request separately at registration. Additionally, the customer has to click the image again.

2.9.Graphical Password System Using Cued Points

Cued Click Points (CCP) have been proposed as an alternative to pass points. In CCP, the user clicks the c = 5 images instead of 5 points on one image. Provides cued recall and introduces visual cues If the last click point (at what point) is entered incorrectly, notify the valid user immediately. You can abort the attempt and start over. Also performs attacks based on hotspot analysis It gets more sophisticated, as we'll see later. It will show the next image on every click and actually redirect the user. Clicking a series of points follows a "path". Wrong clicks lead to wrong paths Explicit display of authentication error only happens after the last click. Users can only select their own images As long as the click determines the next image. If you don't like the resulting image, Create a new password with different click points and get different images. Each of the following 1200 The image has a tolerance square of 1200, so we need 1200 subsequent unique images. the number of The image quickly becomes quite large. Therefore, I propose to reuse image sets across stages. through reuse For images, there is a small chance that users will see duplicate images. During the five phases of password creation

The image indices i1,...,i5 of the images in the password sequence are in the range $1 \leq ij \leq 1200$. If the computation of the next picture index is iterative (that is, if k < j, then ij equals ik), The following picture selection function f is deterministically perturbed to select a particular picture. User's initials The image is chosen by the system based on user properties (used as an argument to username). The sequence is spontaneously regenerated by the function each time the user enters the password. If the user enters the wrong click point, the image sequence will change from that point false , so the login attempt fails. For attackers who don't know the correct order Pictures, this tip does not help

2.10.Graphical Password Authentication System

A password is constructed by clicking a different image five times in a row. user can Select any pixel in the image as the click point for the password. To login, repeat the following sequence: Clicks in the correct order within the system tolerance squared for the original click points. A text file is used to

store the information in the image. The form requires her two pieces of information: name and password. Then upload the image in the image box and set the password in the position where you clicked the image in the image box.

2.11.Graphical Password Authentication Using Block chain Technology

The purpose of our system was to overcome the shortcomings associated with traditional web authentication. Techniques such as password cracking and the annoyance of remembering multiple passwords for different purposes account. We designed a graphical password system that is easy to remember and easy to use. Recognizable, but difficult for hackers to penetrate. Our system uses an advanced click point method An email notification system that identifies potential security risks and notifies users. in a fraudulent attempt When a hacker is detected, it will send an email notification without revealing the identity of the hacker. The system of the Chinese Communist Party A recognizable, clickable, easy-to-use and secure graphical password verification system. system Generates a password based on click points along the x and y axes on a user-selected image. The RGB values of these points determine the password. User can select an image An existing database and a large number of photos in various formats. The system will generate a text password. The user must enter at login based on the RGB values of the click points selected during registration. security is Powered by a second level key click point approach. Even if hackers try to crack the system, If the user enters the wrong click point three times, a warning message will be sent to the user's mobile device. Although this system has many advantages, it has one drawback. because we value it more Authentication as interface design lacks aesthetic appeal. The user selects at least four images and Users have to select specific sharing parts for each image and the data is stored on the blockchain. to disturb Specific attacks such as B. A shoulder attack during a login session to generate a user-chosen picture password Decrease opacity

2.12.Puzzle Based Password Authentication by using Grid Selection

Graphical password generation is the process by which the system randomly generates new keys. to eliminate conflicts. GPG is a puzzle where the user selects an image or uploads an image Let's make it a password-like puzzle. The login process requires the user to select a frame within the puzzle

That will be the password for all files. Generate a password using a graphical password generator (GPG). A puzzle used as an entry point into user documentation, etc. So the mystery is this Key used to authenticate the user. The designed grid size is displayed in the grid cell and activated by the user. Click to select the cell corresponding to the password. Click to select the desired cell. independence. In other words, each button intersection of rows and columns. Cells in the grid are represented by two indices representing rows. Index (R) and column index (C). The columns and rows of the grid are numbered (0-99). Number placement changes dynamically with each login, increasing resistance. Shoulder surfing attack. The relatively large grid size used makes password guessing very difficult. This also makes it more resistant to guessing attacks. users register with them Details (i.e. Name and Email ID). Processes are tracked using graphical passwords. Once the user has successfully logged in, they will be logged into the page. Enter the user's login information on the login page Your registered email ID and corresponding password. Passwords can be location-based or image- based. You can divide the image base into pixels and create puzzles for the user to solve on it. login page. Access is via the server (that is, via the administrator). admin is Check against the database to see if both are the same. If both are the same, access from: administrator

2.13.Cued Click Point Graphical Authentication

The proposed system is based on graphical password recognition as well as resisting users. Observation attacks and guess attacks as well as shoulder surf attacks. The proposed system is based on the WYSWYE strategy (what you see is what you type). The proposed system works in conjunction with image grids By doing so the user gets her two grids. One is a large grid containing images and the other is a small grid. User must be removed Repeat the same process for large grid rows and columns that do not contain passwords. It then matches the passwords in the smaller grid each time the order of the password images changes. Appears to users to withstand shoulder surf attacks.

2.14.Accessing and Study of Cloud Services using Graphical Password Authentication

Based on the username, a procedure is initiated on the server side. A set of images that become The information provided to the user is primarily based on calculated results. Server-side username location Alphabets are calculated in alphabetical order. All positions are then summed. first digit of This sum is used in similar subsequent calculations. Currently there are 26 letters in the alphabet alphabet series. I understand that a two-digit range can start with the range 1-9 itself. the server is already A series of pictures made. The image sets are assigned according to the final result of the calculations that the server has. Get it in the second step. Meaning: If the first digit is 1, assign A1 and bet. If the first digit is 2, Then specify it to be B1. This full password is divided into two sections and is based entirely on the first Second, user selection is primarily based on the set of images provided by the server. For user selection, it is specified as follows: In the image set, the user must select two images as his password. Two images served by the server

User creates a complete password.

2.15.A Modern Image Authentication Algorithm Using Image Click Points To Resist Shoulder Surfing Attack

A user first logs in or registers with the application. The pixels selected by the user are Pixels stored in the database. If they are correct, the user is allowed to login. When logging in for the first time, the user must do this Then select the images and pixels you want to store in the database. User can save used image Create a system and select the pixels that will eventually be stored in the database. Selected pixels are It is stored in the database in the form of

key-value pairs required for authentication. the user is Login is only possible when the correct pixel is selected. Each time a random pair of images is retrieved from the database. It will be displayed. The user has to select the correct pixels in both images in a defined order. user Also, there is one modification that changes the image if you forget the pixels of the image. if the user does not If he selects the correct pixel 5 times in a row, the user will not be able to log in and will see a message like this: certification failed. The application algorithm is a cue recall based algorithm. Chosen person Pixels are stored in the form of key-value pairs, and clues consist of images that aid in authentication fast and accurate. The algorithm compares pixels on the backend and returns the result to system. This saves time and provides the highest security.

2.16.Combating Shoulder surfing Attacks in Computer Security with a New Graphical Password Technique

With graphical password authentication, the user selects one or a series of images. Create a unique password. Passwords are stored in a database on the server and encrypted for security reasons. When a user logs in, the authenticator validates the password against stored passwords. password. If the password is correct, access is granted. Graphical password authentication process The user creates a unique password by selecting one or a series of images. password is saved It is stored in a database on our server and encrypted for security reasons. When a user logs in, the authentication system is activated Validates a password by comparing it to stored passwords. If the password is correct, access is granted. Module 1 requires the user to select at least 3 image categories and select at least 1 image from each. Category if registration is successful. In module 2, when logging in, the user will be assigned a category and Images in correct order selected at registration

2.17.Password Protection for Online and Offline Data

Password protection for online and offline data is a multi-level password authentication system. In this The project proposed different password authentication schemes at each level. can be used as Passwords for folder locks, web control applications, desktop locks, etc. The first level is alphanumeric passwords. The user's password is encrypted by her MD5 algorithm. The next level is implemented by: Use the RGB color pattern. To log in, users must submit their username and corresponding password. system. The first level requires the user to enter a username and an alphanumeric password. of The system authenticates users and only authorized users can access the system. The user Correct password combination. The user is redirected to her second level only if possible. Enter the correct password at the first level. At the second level, the user has to specify her correct RGB color. sample code. The system checks if the password matches the registered password previously stored in the database. If the pattern matches, only the user can continue. at the last login level

2.18.Pixel Based User Authentication System

The efficiency is most important in password systems user want to have a quick access the time to input a graphical password by highly skilled ,automated user can be predicted by the Fit's law .the Fit's law state that “the two point towards a target depend on the distance and the sized of the target”. Greater distance has smaller target lead result in slower performance. In the text based password authentication flaws in aspect of usability and security that bring problems to the user and difficulty in remembering text passwords The system can be problematic if user forgot the point of click The system can be become complex with the increased number of images. to overcome these problems we have to use alternate mechanism like pixel based password. examine the username of cued Click Point (CCP) it is one type of Cued-recall graphical password technique in which users click on one point per image per sequence of images and the next image is based on previous click point. Here are the results of our first user survey. It was positive. Result: CCP's performance is very good in terms of speed accuracy. of a mistake. User connects to her CCP Control points were easy to display by just selecting and saving one point per image and each was displayed The image triggered a memory in them of where the corresponding dot was. I also suggested that it be larger Security is not provided by her CCP as a transit point. Large numbers of images can increase an attacker's workload. A series of images will be displayed, followed by the next image based on the previous click point. So the user Receive instant implicit feedback on whether you logged into your account correctly. safety Ease of use is improved by adopting CCP

2.19.Graphical Password Authentication System For Improving Security In Online Examination

In recent years, various authentication technologies have been used. Here, we propose a system that combines the following. Token-based and knowledge-based methods. The proposed system consists of a registration module, a registration module, Login/authentication module and exam portal. In the registration module, users enter their name, role number, and email ID. and password. The user will see a folder containing images from the database.Users can select any folder. Then the user has to select exactly 3 photos of her from this folder. Then select a click point from the selected click points Use your photo as your password. From each image he selects exactly two points. The point of selection depends on the selection user's. In the login module, the user enters the role number and password and the system displays the image from the database. The user selects a previously selected image and clicks the dot. Token will be sent after successful authentication to user email. Users can use tokens to register for exams. Exam Portal MCQ Types A question is asked (MSQ mixed). The exam has a deadline. When time passes or user clicks submit The 'Exam' button is successfully submitted, the results are generated, and the results are successfully sent to the student's email.

2.20 A Bankable Pictorial Password Authentication Approach

The most commonly used text passwords pose a security problem in large systems. a An alternative approach to authentication is graphical passwords. These passwords are used to constrain known passwords. Problems with traditional authentication methods. This article describes knowledge-based authentication technology were investigated and the need for graphical passwords was discussed. This article analyzes Pure. Remember the "Draw A Secret" graphic password technique and suggest the Advance DAS technique. This overcomes all DAS security and usability issues. Introduce the proposed method It delivers promising results in terms of security, usability, and memorability. Then the registration page will be displayed. You must enter an initial text-based password and required information such as first name, last name, and email address. passwords, security questions, etc. After clicking the password security page for the second color-based graphic you must choose a password immediately. And don't forget to pay attention to color. Click Next to display the Image Based Password page. You must select multiple images as your password and save it. Then you need to go back to the home page and click "Login". then you can Enter your username and correct password. If your Text basis username and password are correct, You have successfully logged in with your text-based password. Then you will see a page with colored basic passwords You must specify a color-based password. If correct, you have successfully logged in with your color- based password. Next, the Image Based Password page is displayed. Then you need to select "Image base as password". in that case Yes, I have successfully logged in with the image's basic password. Then you will see the main page

3. Comparative Analysis

Title	Techniques & Mechanisms	Parameter Analysis	Future Work
Cued Click Points Password Authentication using Picture Grids	Cued Click Points Technique, Encryption algorithm , Hash function	Solution for Shoulder surfing	Security in Picture password is still immature, more research is required in this field
User Authentication Through Cued Click Points Based Graphical Password	Cued-recall graphical password	examine the usability and security	To reduce the problems with existing graphical based password schemes
Three Factor Graphical Authentication Mechanism	combination of recognition and recall based approach.	Resistant to shoulder surfing	System might help the normal human being to convert their text into sign language which will build two-way communication
Graphical Based Authentication Using Cued Click and Binary OTP	Multi factor authentication	multi-layer security	require limitations for the image click
Preventing Shoulder Surfing Attack in graphical password authentication scheme	Cued Clicked points technique	reduce shoulder surfing attack	To increase the processing speed and make it more UI friendly
Graphical based Authentication System using Keystroke Parameters and Cued Click- Points	Graphical-Based Password ,Cued Click Point	Improve protection and confidentiality	to develop a system that can give the high security to other application including banking application
Web Application Authentication Using Visual Cryptography and Cued Clicked Point	secret sharing technique.Cued Click Points	overcome the shoulder-surfing and key-logging attacks	Recognition based authentication can be used in combination with the visual cryptography
Recall-based Graphical Password			
Cued Click Point Based Authentication	Cued Click Point	Essential, usable, and secure	exceptionally secure in contrast to existing frameworks.
Graphical Password System Using Cued	Cued Click Point algorithm	quantity of pictures	To Lesser the problems with graphical based password

Points			
Graphical Password Authentication System	three-factor authentication	combat shoulder surfing attacks	shoulder surfing problem still need to be improved
Graphical Password Authentication Using Block-chain Technology	click-point method	security of graphical passwords	minimize the risk of attacks
Puzzle Based Password Authentication by using Grid Selection	Pattern Matching and Converting the matched pattern image into a grid of passcodes**.**	high-level security	overcome the loopholes present in the traditional authentication methods.
Cued Click Point Graphical Authentication	Cued Click Point	Resist the user from shoulder surfing attack, observation attack and guessing attack.	user can upload their own images to make it more difficult for attacker to guess it.
Accessing and Study of Cloud Services using Graphical Password Authentication	Cued Click Points	Computer security, Security attack	presenting extra memorable password
A Modern Image Authentication Algorithm Using Image Click Points To Resist Shoulder Surfing Attack	Pass image algorithm	provide a better security	Active learning techniques to optimize
Combating Shoulder surfing Attacks in Computer Security with a New Graphical Password Technique	image-based authentication,	resistant to shoulder surfing	secure access to information and devices
Password Protection for Online and Offline Data	Cued Click Point	effective password space	Provide more usable and memorable authentication mechanism
Pixel Based User Authentication System	Cued click point	speed accuracy	security features must be balanced
Graphical Password Authentication System For Improving Security In Online Examination	Recall based Authentication	overcome drawbacks of textual password.	More memorable authentication mechanism
A Bankable Pictorial Password Authentication Approach	Draw A Secret ,Cued Click Point	Maintain Security	high on memorability of password

4. Conclusion

Cued click points play an important role in password protection, and graphic passwords are better protected. Better than alphanumeric passwords. An important element of graphical passwords is It's much easier for users to remember and more secure. Online password guessing attacks It's becoming more common these days, necessitating the use of more secure password systems. So we know: graphic password. Image passwords are an alternative to text alphanumeric passwords. will satisfy both Conflicting requirements, Easy to remember, hard to guess. by relaxing your shoulders Password schemes are more secure and easier for browsing and other issues. digital equipment Be a part of our daily life. Learn about authentication through the use of digital devices procedure. Validation is an integral part of security. Authentication enhances customer security user friendly. Passwords are easy to create and retrieve. Randomization in authentication systems Provides strong security against shoulder surfing. Building a good system requires high security and high quality , Ease of use is inseparable.

References

R. Shantha Selva Kumari, S.Viji,"Cued Click Points Password Authentication using Picture Grids", International Journal of Computer Science and Network, Volume 4, Issue 6, December 2019.

Hasi Saha, g c Saha,Roshidul.h, Zakirul Islam,"User Authentication Through Cued Click Points Based Graphical Password ",American Journal of

Agricultural Science, Engineering and Technology,2019.

Vivek Solvande, Jay Chokshi, Mandar Gharat, Aparna Patel, Namit Kadget,"Three Factor Graphical Authentication Mechanism",International Journal of Research in Engineering, Science and Management Volume-2, Issue-4, April-2019

Umesh Popat Salunkhe,"Graphical Based Authentication Using Cued Click and Binary OTP",National College of Ireland,2021

Hammed.M,Adebedo.N.O,"Preventing Shoulder Surfing Attack in graphical password authentication scheme",Annals. Computer Science Series. 18th Tome 1st Fasc. – 2020

Ruta Gore, Chaitrali Bokil, Chinmay Deshpande, Mrunalinee Patole, "Graphical based Authentication System using Keystroke Parameters and Cued Click- Points",International Journal of Research in Engineering, Science and Management Volume-2, Issue-3, March-2019

Mary Ogbuka Kenneth ,Stephen Michael Olujuwon, "Web Application Authentication Using Visual Cryptography and Cued Clicked Point Recall-based Graphical Password",Journal of Computer Science Research | Volume 03 | Issue 03 | July 2021

Suvarna Pansambal, Apeksha Waghmare, Aruna Pavate, Divya Kumawat4, Swati Shirke5,"Cued Click Point Based Authentication,Journal of Engineering (IOSR JEN) www.iosrjen.org,2019

Prasanna Lad, Shubham Thasal, Abhishek Shetty, Prof. Sanket Patil, "Graphical Password System Using Cued Points",International Journal of Advanced Research in Computer and Communication Engineering Vol. 10, Issue 5, May 2021

Pathik Nandi, Dr. Preeti Savant, "Graphical Password Authentication System",International Journal for Research in Applied Science & Engineering Technology (IJRASET),Volume 10 Issue IV Apr 2022.

Vishal Saibanna Mali, Pravin Santosh Mishra, Yashraj Mahesh Patil, Siddhesh Khanvilkar,"Graphical Password Authentication Using Blockchain Technology,",International Research Journal Of Modernization In Engineering Technology And Science (Peer-Reviewed, Open Access, Fully Refereed International Journal) Volume:05/Issue:04/April-2023

J Lin Eby Chandra, M Kumaran, R Chandrakala, V Seedha Devi, S Rajendran"Puzzle Based Password Authentication by using Grid Selection" Vol. 71 No. 4 (2022)

Yogesh V Mahajan, SVIT Chincholi, Ganesh R Tile, Devidas S Thosar, Paresh S Patil,"Cued Click Point Graphical Authentication" Vidyawarta®, 2019

Jasmin P Bhootwala, Pravin H Bhathawala, Ahmadabad Navrangpura,"Accessing and Study of Cloud Services using Graphical Password Authentication", International Journal of Engineering And Technology, ISSN, 2278-0181,2019.

Devidas S. Thosar* and Dr. Dhanraj Verma ,"A Modern Image Authentication Algorithm Using Image Click Points To Resist Shoulder Surfing Attack",Webology (ISSN: 1735-188X) Volume 18, Number 4, 2021

N Moratanch, P Ajithkumar, T Bhuanesh Kumar,"Combating Shoulder-Surfing Attacks in Computer Security with a New Graphical Password Technique", Data Analytics and Artificial Intelligence Vol: 3(3), 2023

Kirti Rajadnya, Prathamesh Pasalkar, Vaishnavi Birhade, Prashant Sargar,"Password Protection for Online and Offline Data", International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056 Volume: 07 Issue: 05 | May 2020

Mr. A.K.Zambre1, Ms. Vaishnavi D. Chaoudhari 2 ,Ms. Mayuri P. Kolte3, Ms. Aarti G. Khodke 4, Ms. Nikita A. Shelke5 ,"Pixel Based User Authentication System",International Journal of Interdisciplinary Innovative Research &Development (IJIIRD) ISSN: 2456-236X Vol. 04 Issue 02 | 2020

Ashwini U Chavan, Ankita A Rajeshirke, Jayashree R Kudale, As Sondkar,"Graphical Password Authentication System For Improving Security In Online Examination", Journal Of Analysis And Computation (Jac) (An International Peer Reviewed Journal), Www.Ijaconline.Com, Issn 0973-2861 Icasetmp- 2019

Aakanksha Chopra, Megha Gupta,"A bankable pictorial password authentication approach",Proceedings of the International Conference on Innovative Computing & Communications (ICICC), 2020