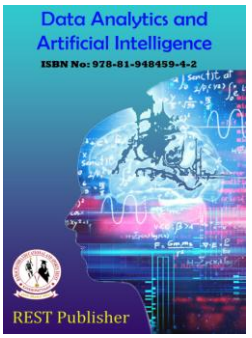
Data Analytics and Artificial Intelligence

Vol: 3(1), 2023

REST Publisher; ISBN: 978-81-948459-4-2

Website: http://restpublisher.com/book-series/daai/

DOI: https://doi.org/10.46632/daai/3/1/8



Strengthen Password Using Image Authentication

***C. Madula, K. Soundharya, N. Sharmila Banu, Subash, Senthil Kumar, Pradap**

veltech hightech dr.rangarajan dr,sakunthala engineering college, Chennai,Tamil Nadu, India.

*Corresponding Author Email: madula.777@gmail.com

Abstract: *Authentication is by password It is alphanumeric in nature. However, the user finds it Difficulty remembering long passwords Remember many times while running. instead of this. They create short, simple and insecure passwords. User data vulnerable to external attacks. Graphically Passwords offer a way out of this dilemma Passwords that are easy for users to remember and use Passwords, more secure. With Graphical password, user clicks on image instead of typing it. A text password containing alphanumeric characters. A New, more secure graphical password system Developed using image segmentation. Picture A segmentation system presents images to the user Here the user selects some grid on that image. If These points, entered in the correct order, user. The result is an alphanumeric password and Both graphical passwords worked around the same time, Graphical passwords were easy to obtain and remember. [1]As such, graphical passwords have been found to be harder to crack They are newly implemented and don't have many algorithms Designed to break them.*

keyword: *authentication, encryption, graphical, passwords, images, logins, segmentation.*

1. INTRODUCTION

Computer, network, data and information security considered a serious technical problem day[1]. However, it is now widely recognized Accept that most security mechanisms cannot do this Succeed without Considering User Opinion [2]. Various graphical password schemes are used An alternative to alphanumeric passwords [3]. Research It is shown to enter an alphanumeric password as Both security and usability issues Not a desirable solution [4]. Critical Areas of Security research Determining if a specific user is required Allows access to specific systems or resources. this Paper is intended to convey an understanding of the new Graphical password authentication system with photo segmentation. The importance of this paper is Understanding Flexible Graphical Passwords An authentication system with extensive insight Support it. graphic password authentication Implemented using two techniques: recall-based and recall-based recognition base. Basic concept of image utilization A segmentation system is one that uses images as security Leads to high memory and reduces it Possibility to choose an insecure password. This in turnOverall password security should be strengthened. our elementary school Here are the questions: is a graphical password Competitive for alphanumeric passwords Security, Performance, Retention.

background and related work: Mention security and usability issues It has to do with alphanumeric passwords like . Password problem. ” The reason for the problem is A password is expected to be exchanged for two conflicting passwords Requirements, namely: (1) Make passwords easy to access Remember. The authentication protocol is Can be done quickly and easily by a human. (2) Passwords must be strong. guess, it should look random. they should be changed Often it should be on different or different Multiple accounts for the same user; they shouldn't Write it down or save it in plaintext. meet such Requirements are almost impossible for users. Or This issue is well known in the security community. Classical research [5], dating back more than 25 years, Thus, it was shown that human users tend to make choices Alphanumeric passwords are not secure. A recent study confirmed these results [6]. Password The problem arises mainly from fundamental limitations of human long-term memory (LTM). 1 password After choosing and learning, users should be able to: it that in mind, sign up. But everyone I usually forget my password. power law Forgetting refers to forgetting rapidly immediately after Learning is followed by a very slow decay after that [7]. Psychological Theory Causes Forgotten Collapsed by time and interference ,New elements in memory interrupt existing elements retroactive). Recent reviews highlight Importance of retrospective intervention in everyday life forgot [8]. Collapse and Interference Help Explain Why People Forget Passwords Users Expected Learn passwords,

remember them, and remember them over time. But other elements in memory conflict with it Passwords are hard to remember. if the password Especially vulnerable if used infrequently forget. In recent studies, User cannot remember password. Get some of it right [9]. however, The password for password authentication is Partly because it is based on a very precise recall A good password is worthless now. Aside from that, Users now have many passwords on their computers, networks, websites, etc. Also, some The system requires frequent password changes. It's probably a misguided attempt to increase security. This usage passwords increase the chances of intrusion, Perhaps you forgot your password or Forget the system to which the password is assigned When. What should the user do? In most cases the user sacrifice to reduce the load on his memory safety. Probably most of the time users write: Write down your password and keep it in a suitable place. This prevents passwords from being compromised. One of his approaches to increasing password security is to use .Formation of [10]. However, given the contradiction Between passwords and human skill Fundamental change is unlikely [11]. A better way to solve the password problem is to use Develop password systems that reduce storage problems while maintaining security. recall base The technique asks the user to recreate something .he/she has previously created during the registration stage .An example of a polling-based system is the Draw-A Secret scheme .An image on a two-dimensional grid during registration and its store the coordinates of the grid in that order Drawn. This technique has drawbacks The image attached to it-redrawing should touch it Same grid in exactly the same order throughout certification. Detection-based techniques are introduced Shows a series of images to the user and prompts the user Recognize and identify selected images registration phase. One such example of lying Between recall and recognition-based technology Pass point technique. the system allows anyone Random image used. Many possible click points. The role of images is only Provide helpful hints for users Remember click points. click to register Points must be selected in the same order as before registration phase within somewhat adjustable tolerances distance. This is very time consuming and Remember these specific points. attached setbacks This technique can be processed using images. segmentation system. image segmentation is a call backBase system for providing points to establish Trigger context and saved memory [13].

***Image Segmentation*:** The Pass Points program is similar in many ways. However, Blunder's scheme uses only one image of him. This Schemes are flexible as they can be of any kind. image. provided by the system, or Selected by the user. The proposed system allows users to Change to set photo as password Users know the images they have inserted. A Upon receiving the image, the system segments the image Convert and save as a series of images in raster format according to them. Next time the user will The system receives segmented images from the system In a jumbled order. the user Image to er the original image If submitted, the user is considered authenticated. otherwise, the user not considered authentic. the only practical A prerequisite for choosing a particular image is The image he must not consist of one large part monochromatic object. for example: wall or The image of the sea, the sea, and the sky without clouds. That's right, it It's not easy for users to guess what's right .A succession of grids to form a big picture. More Images should be content-rich and contain a variety of elements Components and objects that define patterns only displayed to the user. (segmented image).

2. LITERATURE SURVEY

Graphical Password Authentication. They designed a graphical password technique given some of the powerless techniques of graphical passwords. For example, a basic multiple-image password provides a user with many images from which he must choose one. Or more. No other display is needed as the following basic grid scheme is a simple object. Choosing the following triangle scheme is difficult. It has a protruding surface and virtually the same number of images displayed. The most helpless thing in this paper is calculating the cardinalities of usernames. Therefore, it is often a new scheme that solves many problems of existing systems.

Enhancement of Password Authentication System: Using Graphical Images: This post is primarily focused on building graphical password systems using various authentication schemes. Also, the underlying goal of this method is to provide greater security in a simpler technique that is user-friendly and more resistant to guesswork by hackers. That's why they are developing his three types of authentication systems. A. Pass point, B. Cued click point, C. Persuasive click points. Pass points, in this system, the user has to select five points from his one image, and from the time of selection to the time of login, the user has to repeat the same series of points from one image it won't work. Cue Click Point has the same configuration as Pass Point, but the biggest difference between the two is that in 5 completely different frames he passes 5 points and every frame he passes 1 point. PCCP could be an authentication technology. PCCP is the best technology, but it has security issues.

A New Graphical Password Scheme Resistant to Shoulder-Surfing: In this paper they are discuss about security features of graphical authentication. Different graphical password schemes have different techniques to scale back the cyber-attacks. As you recognize that graphical password is simple to remember and high usability with high security. So graphical password schemes are provided higher security than text -based passwords. Some of the resistance of

graphical password authentication attacks are shoulder surfing, brute force, dictionary attacks, guessing attack, spyware and social engineering attacks. During this paper they supply a quick description and classification of various graphical password schemes followed by information about vulnerabilities within various schemes and suggestions for future development.

3. EXISTING SYSTEMS

A graphic password refers to using a picture or different colors as a password. Graphical passwords are easier to remember because people are more likely to remember pictures than words. Graphically his password is more resistant to brute force attacks. Graphic passwords are a more attractive, visual representation used in place of text or alphanumeric characters. The graphical passwords consist of six sections namely:

A. Image-based scheme: This scheme provides a number of images and requires the user to select an image as a password. From the grid, the user has to select the actual images in the correct order for authentication. As you can see in the picture, users can easily remember the password. Image-based passwords are more attractive and the image position changes with each login attempt. This scheme therefore largely avoids shoulder surf attacks. These classes define good weak password sub ranges in the attack dictionary.

B. Color base scheme: This scheme provides a number of colors and requires the user to select a color as a password. The system uses a variety of colors to confuse scammers, but is easy to use for authorized users. The password is displayed in color, making it easy to remember. Resistant to shoulder surf attacks. The user must select the spot colors in the correct order for authentication. The password is then saved in the database.

C. Recognition Based: With this technique users set an image as a password during registration. User must reproduce or remember their own passwords, and thus no hints are given to remember the passwords. The user must select the specific number of images in this set as a password.During authentication, the user must correctly recognize these preselected images.

D. *Signature Based Scheme:* In this scheme, the user's signature is used for the password mentioned in the system. Anyone's signature cannot be copied as it is. A small error in the signature can prohibit the access.

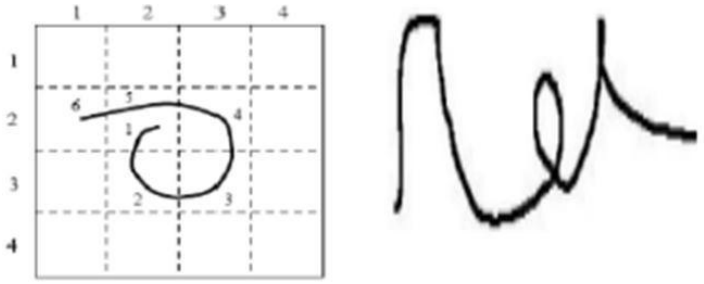


FIGURE 1. Signature Based Scheme

E. *Based on pure memory:* Callback-only authentication systems are difficult for users to remember. Some published results of recall-only authentication schemes offer higher levels of entropy than text-based passwords. This scheme requires the user to draw a password on a grid or blank canvas. The user must redraw the drawing so that it touches the set of coordinates listed. Although more secure than detection-based techniques, it is very difficult for users to remember passwords.

F. Cued Recall Based: This scheme requires the user to select multiple click points on the image in a specific order during the registration phase. The user must then select the same click points in the same order when selecting the click points in the same order as they selected during the registration phase.These techniques are simpler than pure polling-based techniques because they provide the user with a clue to remember their password.

4. METHDOLOGY

In this project, when a user tries to access the home page, they are presented with three options: Register, Login, and Developer. If you have not registered yet, you will need to click the register option. 1) A registration page will appear. You will need to enter an initial text-based password and required information such as first name, last name, email, password, and security question. 2) Click on the image-based password page below and you will be prompted to select multiple images to save as your password. 3) Now you need to go back to the home page and click login. You will then have to provide your username and correct password. If your Text basis username and password are correct, you have successfully logged in with your Text basis password. 4) Next, you will be presented with the

image-based password page. Then you have to select the image base with a password. If correct, you have successfully logged into the image's base password.
5) Next, you will see the main page.

5. SYSTEM MODULES

Module-1: Registeration Form
Module-2: Login Form
Module-3: Image Segmentation
Module-4: Image Retriving

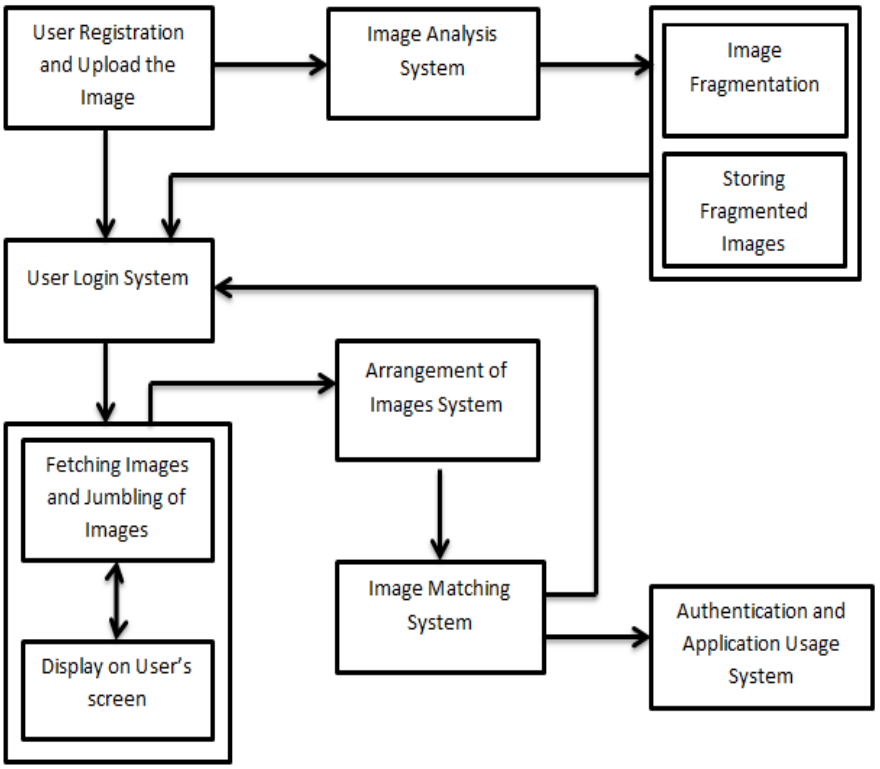


FIGURE 2. Architecture Diagram

7. ANALYSIS

Image segmentation has security benefits. Large password spaces compared to alphanumeric passwords. This It also has advantages in the password space over blunder style graphic passwords and recognition-based. Graphical passwords like Pass faces. regardless of Initial difficulties Graphical password authentication system, after a while User feels comfortable with practice Alphanumeric or graphic-based implementation Password as input. people using graphical Password authentication is then enter the password correctly at a much faster pace I got better with practice. this is, A minority of the graphics participants have serious problems Learning difficulties [15]. but no authentication Schemes must be evaluated in terms of feasibility threat. Image implementation is recommended Used in systems where no online attacks are made possible and where each attack is made against online The system may limit the number of guesses made at one time. Account for a period of time. All Communication between server and client protected via SSL while maintaining the security of the selected click point and the corresponding image, Therefore, simple network-based attacks are avoided sniff. Image association is recommended Per user as a function of username, i.e. H .give different images to different groups of people Based on username. again, The image set for all users is a multi set containing: There are so many images and users area I assigned a subset of these images to an image map. Attacks against the system that attackers attempt Breaking into accounts [16] slowing down Note above. hotspot analysis Used to increase the efficiency of attacks A dictionary, but you need to collect pictures, etc. Dictionaries must be generated per user base. Increase in online attacks against specific users. It is troublesome and

needs further consideration. Acquisition of information from shoulder surfing, etc. Most graphical password schemes are vulnerable to shoulder surfing attacks [17]. When With today's small cameras and camera phones, it's easy to Record video of the user's screen or keyboard. Log in Image segmentation is also vulnerable With respect to such attacks and their current forms, Images are easier to see than from a distance Mouse pointer movement during image segmentation. Know what images to look for in your system Given enough guesses, an attacker can do this Click on a random grid to attempt a brute force attack until you reach the correct order. for username All information is available to the attacker if the grid rows can be observed by shoulder surfing. As with most, you need access to your account other password systems. in compromise Computers are also a threat because some computers can have malware Credential collection and sharing information elsewhere. Key logger success For text passwords, software for graphical passwords. Required to capture images and mouse pointers position. If only limited information is known, Can be used to narrow the search for correct guesses. Knowledge of usernames in correct grid order Enough to get the user's only photo. Hotspot Analysis [18] can only be performed at this point. So the image is the one served by the server Safe from Hotspot Analyzer. Image segmentation Not suitable for environments where shoulder surfing occurs User is a real threat or environment Images may be recorded (e.g. insider, malicious software on client computers). Hotspots and dictionary attacks in some cases Where Attackers Can't Conquer Information from users, they are limited to what they can be inferred by image analysis is a hot spot Specific area in higher image Likelihood of being chosen as part of a password by user. If an attacker can accurately predict that. Hotspots in images make building hotspots easier dictionary of passwords by combining these hotspots. Hotspots are known to be problematic on image segmentation [19] further analysis is needed Decide whether to carefully consider considerations .You can minimize this threat by choosing a grid. Key Advantages of image segmentation what it can do For brute force attacks and dictionary attacks. again, How to be more charitable, yet powerful password. For example, when the user selects an image, A building he knows. in this way, User can easily place the grid correctly You can also protect data, not just sequences Invader. This increases the security of your system very high. However, a major drawback is Registration and login to the system takes a lot of time.

8. CONCLUSION AND FUTURE WORK

Finally, consideration of image segmentation It shows its strengths and weaknesses. Graphically Password Users can easily create valid password forgot, they'll have to fire more More disk space than alphanumeric users method and time. Region of interest when using images Segmentation is to satisfy both it contradicts requirements, i.e. easy to remember and hard Guess. In principle this could be the ideal solution All kinds of equipment as opposed to difficulty a long, secure alphanumeric password keyboard all the way. The challenge is Enough space for a password on a small photo. However, this can be accommodated by increasing the area. of the image when the user moves their finger over a particular image area of the screen. Finally image segmentation It seems to promise something safer Because it's easy to get big passwords, Based on complex and natural images. The probability that an attacker can guess your password. His second most important goal for this paper was to Image segmentation usability, image Segmentation does not serve user needs Remember different passwords. Mentally According to research, it can be caused by interference. Noticeable memory problems [8]. Security research [10] Confirm that users have memory problems Create multiple passwords and create insecure practices Solve the problem (write down passwords, etc.)

9. REFERENCES

[1]. Birget, J.C., Hong, d., Memon, N.Robust discretization, with application to graphical passwords. Cryptology ePrint Archive, http://eprint.iacr.org/2003/168, accessed Jan 17,2005 M. Young, The Technical Writer’s Handbook. Mill Valley, CA: University Science, 1989.

[2]. Brown, A.S., Bracken, E., Zoccoli, S. and Douglas, K.Generating and remembering passwords. Applied Cognitive Psychology 18 (2004), 641-651.

[3]. Boroditsky, M.Passlogix Password Schemes. http://www.passlogix.com. Accessed Dec. 2, 2002.

[4]. Brostoff, S. and Sasse, M.A. Are Passfaces more usable than passwords: A field trial investigation. In People and Computers XIV - Usability or Else: Proceedings of HCI 2000 (Bath, U.K., Sept. 8-12, 2000).

[5]. Adams, A. and Sasse, M.A. Users are not the enemy. CACM 42, 12 (1999), 41-46.

[6]. Blonder, G.E. Graphical passwords. United States Patent 5559961, (1996).

[7]. Bradley, M.M., Grenwald, M.K., Petry, M.C. and Lang, P.J. Remembering pictures: Pleasure and arousal in memory. Journal of Experimental Psychology 81, 2 (1992), 379-390.

[8]. Bahrick, H.P. semantic memory content in permastore: Fifty years of memory for Spanish learned in school. Journal of Verbal Learning and Verbal Behavior 14 (1984), 1-24.

[9]. Borges, M.A., Stepnowsky, M.A., and Holt, L.H. Recall and recognition of words and pictures by adults and children. Bulletin of the Psychonomic Society 9, 2 (1977), 113-114.
[10]. Biederman, I., Glass, A.L. and Stacy, E.W. Searching for objects in real world scenes. Journal of Experimental Psychology 97 (1973), 22-27.
[11]. S. Wiedenbeck, J. Waters, J. C. Birget, A. Brodskiy, and N.Memon, "PassPoints: design and longitudinal evaluation of agraphical password system," Int. Journal of HCI, vol. 63,2005, pp. 102–127.
[12]. RealUserCorporation.ThesciencebehindPassfaces.Whitepaper,http://www.realuser.com/published/ScienceBehindPas sfaces.pdf, accessed Feb. 2012.
[13]. I. Jermyn, A. Mayer, F. Monrose, M. Reiter, and A. Rubin, "The design and analysis of graphical passwords," in 8th USENIX Security Symposium, 1999.
[14]. H. Tao and C. Adams, "Pass-Go: A proposal to improve theusability of graphical passwords," Int. Journal of NetworkSecurity, vol. 7, no.
[15]. P. C. van Oorschot and S. Stubblebine, "On countering online dictionary attacks with login histories and humans-in the- loop," ACM Trans. Info. System Security, vol. 9, no. 3,2006, pp. 235-258.
[16]. L. von Ahn, M. Blum, N. J. Hopper, and J. Langford, "Captcha: Using hard AI problems for security," in Eurocrypt, 2003, pp. 294-311.
[17]. S. Chiasson, P. C. van Oorschot, and R. Biddle, "Graphical password authentication using cued click points," in European Symposium on Research in Computer Security (ESORICS), 2007, pp. 359-374.
[18]. E. Stobert, A. Forget, S. Chiasson, et al. Exploring usability effects of increasing security in click-based graphical passwords. In Annual Computer Security Applications Conference (ACSAC), 2010.
[19]. Harsh Kumar Sarohi,Graphical Password Authentication Schemes: Current Status and Key Issues, International Journal of Computer Science Issues,2013, 437-443.
[20]. S.Singh, G.Agrawal "Integration of sound signature in graphical password authentication system" Invertis University Bareilly,India, January ,2011.

