International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

A Secure Authentication- Graphical Password Authentication System

Dr. Uday Chandrakant Patkar[1], Dr. Shikha Bhardwaj[2], Dr. Uday Shankar Patil[3], Prof. Namrata Khope[4], Shubham Nandu Ovhal[5], Pranav Vinod Mahalpure[6] , Shruti Nagar[7]

Submitted: 23/08/2023 **Revised**: 06/10/2023 **Accepted**: 20/10/2023

Abstract: This paper gives brief idea about "Graphical Password Authentication System" . As we know according to human psychology , human mind have great tendency to remember pictures than that of text. By this motivation the graphical password authentication system is created as a replacement for Text-Based Passwords. The main purpose of this paper is to study about graphical password authentication system , it's importance , advantages , drawbacks , future scope ,etc. Graphical Password authentication is grate alternative to the traditional password methods . As we all know the human mind have great capability of remembering what they see rather than alphanumeric characters and the graphical password authentication do same thing .This method allows user to register by selecting a set of pictures as he likes .The user has to select from images in specific order as he or she like as password . images for password can be from any domain like images of face, any grocery etc. so it will helps the user to remember the password. mainly this system has been developed to reduced the limitation of the alphanumerical passwords . also this is one of the solution for remembering the passwords . [1] [2].

Keywords: *Authentication , Password , Usability , Graphical User Interface , Security.*

1. Introduction

A user's access to a certain system is determined through the authentication process. In order to authenticate users and ensure security, systems and websites need passwords, but utilising traditional alphanumeric passwords has significant dis-advantages.For example, strong passwords are difficult to remember, and on the other hand, passwords that are easy to remember are also easy to guess. Most users write down their passwords or use the same password across multiple websites to reduce memory load risking security. It is both required and imminent for ordinary alphanumeric passwords to be replaced with a more secure form of authentication. Alphanumeric authentication problems may be overcome with biometric authentication, although this system is complicated and expensive.[3]

[1] *HOD, Department of Computer Engineering, Bharati Vidyapeeth's College of Engineering, Lavale Pune, India*
patkarudayc@gmail.com
[2]*HOD, Department of Engineering Science, Bharati Vidyapeeth's College of Engineering, Lavale Pune, India*
shikha.shrivas@bharatividyapeeth.edu
[3]*HOD, Department of Civil Engineering, Bharati Vidyapeeth's College of Engineering, Lavale Pune, India*
udayshubu@gmail.com
[4]*Prof., ENTC Department, Bharati Vidyapeeth's College of Engineering, Lavale Pune, India*
namrata.khope@gmail.com
[5]*Student, Department of Computer Science, Bharati Vidyapeeth's College of Engineering, Lavale Pune, India*
1shubhamovhal@gmail.com
[6]*Student, Department of Computer Science, Bharati Vidyapeeth's College of Engineering, Lavale Pune, India*
pranavmahalpure0306@gmail.com
[7]*Student, Department of Computer Science, Bharati Vidyapeeth's College of Engineering, Lavale Pune, India*
shrutinagar32@gmail.com

All these drawbacks can be eliminate with the help of new authentication system known as "Graphical Password authentication system". The one of the promising authentication technology is graphical password authentication. For our computer or digital device to create a safe zone computer security is considered . to provide security to our digital device or any important device the graphical password is used . as earlier mentioned our human brain have great capability to store or recall an image or image-based password .So for that purpose we can use graphical password for registration with high security and we can easily recall the password. The authentication can be define as "It is a data access point that helps the consumer security assurance" . i.e . it is a process of providing grant for particular data to particular user . Authentication techniques can be categorized as validation based on biometrics , token based authentication ,validation-based upon knowledge . In token based authentication alphanumeric symbols are used as passwords and these tokens are used as hidden keys. As name graphical suggest that it uses different images and shapes as password and in addition to this human psychology says human brain can remember pictures easily than any text . For this authentication human brain can easily select image for password and process it in to the brain. The graphical password is mainly used as it overcome the drawbacks of the traditional alphanumeric passwords such as keylogger , dictionary attack and any other guess method.

Graphical Password schemes are broadly classified as recognition-based and recall-based graphical technique . In methods based on recognition. The user must authenticate himself by selecting one or more photographs from the ones

he selected during registration. Recall-based approaches need the user to recall a process that was performed at registration .

2. Classification of Authentication System:

Recent incidents of fraud and terrorism have made it more crucial than ever for an organisation to offer a precise and trustworthy method of verification. knowledge based(single factor), Token based (two factor) and Biometric based (tree factor) three broad areas of authentication [4].

To access the computer is allow to user by authentication . Additionally, it will be withheld from the unauthorised individual if the authentication does not match. Any digital system or website that needs to know who the actual authorised user is will utilise authentication techniques. Even authentication is used to control what resources a user can access, when they may access those resources, and how much of the source they can consume. The server primarily uses login and password for authentication purposes.. Even authentication is used to restrict a user's access to certain resources, as well as the times and amounts of those resources. When a client authenticates, the server often gives the client a certificate, which a belived third party, like a bank, expects from the client to do. What actions or files a person is permitted to view is not determined by authentication. Simply said, authentication establishes the identity of the user or system.

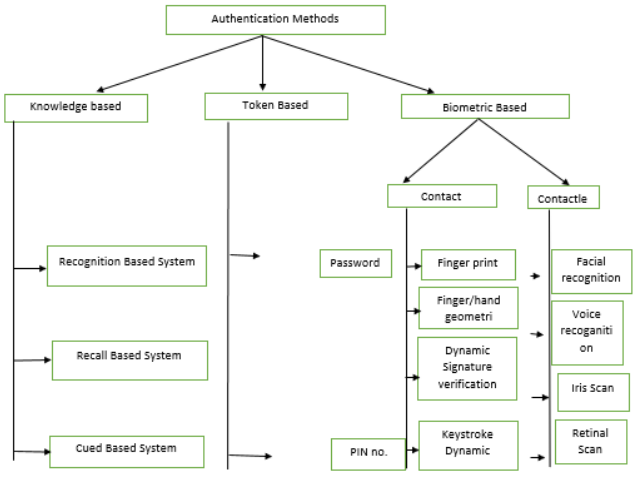


Fig. 1 Classification Of authentication methods

2.1. Token Based Authentication :

This is the authentication which is based on “something that you passes”. As an illustration, consider smart cards, a student ID card, a driver's licence, a credit card, etc. Instead than using their login and password, users can submit their login details to get a token that enables them to extract a specified resource. Once they have their token, which grants temporary access to a particular resource, the user can show it to the access point[5].

2.2. Biometric Based Authentication :

As in word suggest combination of bio and metric means combination of human and measurement. Biometrics, to put it simply, is any measurement relating to human properties that distinguishes one individual from others. The term "biometric authentication" describes a special security method that uses biological traits like our voice, eye retinas, fingerprints, eye retinas, etc[6].

Although this method of authentication offers great security, it is rarely employed due to its drawbacks. The main drawback is the high price. Different biometric systems make use of various expensive devices. Utilizing biometric technology is difficult and time-consuming. A denial of service problem in a biometric system happens when a system fails to identify a genuine user or mistakes an unauthorised user for one who is authorised[3].

2.3. Knowledge Based Authentication :

The authentication techniques which involves both picture and text based password are called knowledge based authentication and these authentication methods are widely used[7]. This technique is based on the something that you know e.g password. In this method user set a secret question to login and every time during the login user is asked to answer that particular question[8].

3. Graphical Password Authentication :

As stated in the name itself it is combination of images and shapes for authentication purpose .In graphical password different pictures or drawings are used as a password. As compared to theory or text humans can easily remember the pictures which are set as password. Also this is more resistance to the hacker attack techniques such as brute force attacks, cause the search space and time is practically infinite. Recall based graphical techniques and recall based graphical schemes are two main categories of graphical password techniques. In recognition-based scheme, a user is made to prove their identity by asking them to identify one or more photos they chose during the registration process. When using recall-based method user has to redraw same password as he selected during the signup stage. a recognition-based authentication method that tests a user's ability to recognise human faces is Pass-faces . In 1996 the Greg Blonder introduced the recallbased graphical password technique. During this by clicking several locations on the image a password is created and the re-entering the password user has to select same location point as earlier and in same sequence . the greatest alternative to a text password is a graphical password, which uses two methods of authentication: color-based and image-based. Both are simple to remember and hard to guess. Graphical passwords take advantage of the fact that humans are visual beings who process and retain visual cues better than most

other types of data.[9].

4. Classification of Graphical Password Authentication :

As we have mentioned above knowledge based technique involves both picture based technique and text based technique.

These picture based techniques are broadly classified into two main classes as mention bellow:

1) Recall Based Technique .

2) Recognition Based Technique.[10]

4.1. Recall Based technique :

Picture password can be of two categories first one is Repeating a selection and second is Reproducing a drawing.

4.1.1. Reproducing Drawing:

Jermyn suggested a method called "Draw-A-Secret (DAS)" that enables the user to sketch their particular password [11]. From the below fig[,2,3,4] the fundamental idea underlying Draw a Secret (DAS): Humans are excellent at creating images. "Passwords" should be created to help in identification and remembering. to make use of that capacity. Initial implementations merely observed how well users could create a free-form shape on the touch-sensitive display using a stylus. However, the creators of the current work have improved the method by parsing the patterns with a flexible grid, that enabled them to more precisely identify important elements such variations in the direction of the stroke. This DAS system's main drawback is the user's potential to precisely recreate a complex structure from memorization.

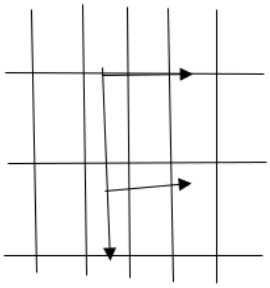


Fig 2: 4X6DAS Password

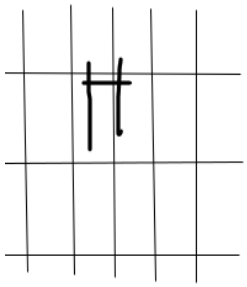


Fig 3: Central Password

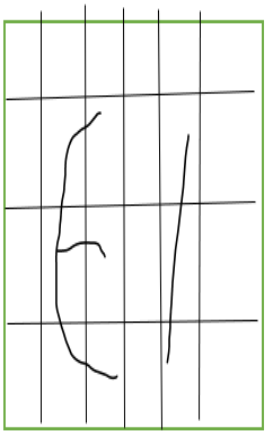


Fig 4.1: User Print

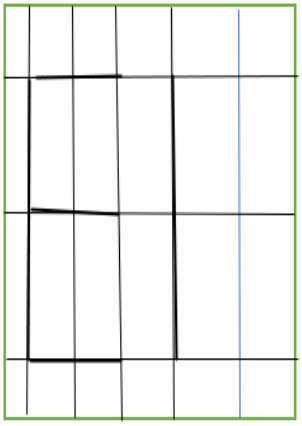


Fig 4.2: Internal **Expression**

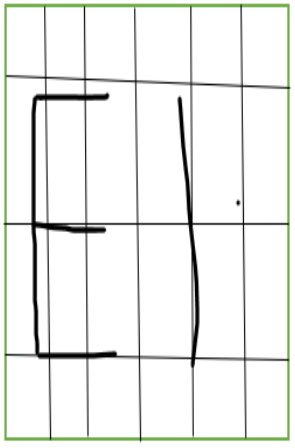


Fig 4.3 : Logout Input

Fig 4: Checking scheme

4.1.2. Repeating The Selection :

Blonder developed a graphical password system in which the user creates a password by clicking on various points on a picture[12]. The user has to click on the specific places of those regions during authentication. Based on this concept, Passlogix created a graphical password system[13]. In this approach, users are authenticated by pointing on specific parts of the image in the right order. Blonder's concept was developed upon by Wiendenback's "PassPoint" technology,[14][15] which did away with specified bounds and permitted the usage of any image. As a consequence, a

user can generate a password by clicking anywhere on an image (as contrast to a few pre-defined regions). This method uses Birget proposed method i.e. decentralization.[16].

4.2. Recognition Based Technique:

A graphical authentication system based on the Hash Visualization Technique was presented by Dhamija and Perrig. [17][18] In recognition-based procedures, a client is verified by asking them to identify one or more images they chose while registering. Systems based on recognition, also referred to as searchmetric or cognometric systems . Users are typically required to memorise a portfolio of images when creating passwords, and they must then distinguish their photographs from decoys in order to log in. The ability of humans to recall previously seen images, especially ones that were only briefly seen, is outstanding. Such systems are not good alternatives for text password schemes from a security standpoint because their password spaces only support 4 or 5 digit PINs. Numerous sorts of images have been used in the development of acknowledgment systems, most focused faces, random works of art, commonplace objects, and icons. Renaud examines particular authentication and usability issues, and provides usability design recommendations with an emphasis on recognitionbased systems. The system must maintain knowledge of some specifics of the shared secret for some graphical password techniques, This information needs to be saved in a way that the system can access it and everyone with rights to the stored data can see it in its original form.

Fig 5: Human Face recognition

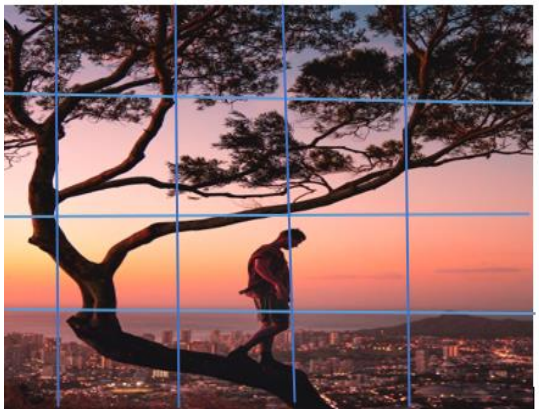


Fig 6: Selecting Sequence of image password

5. Implementation Of Graphical Password Authentication system :

In our proposed system, there are three alternatives presented to users who attempt to reach the Homepage: register, login, and about developer. You must select the register option if you haven't registered already[19].

1) Starting is with the user name and a text password that are stored in the database must be typed in order to proceed. In order to sign in, the user must authenticate with that exact registered user and text password.

2) In the second stage, the user is presented with a list of objects, from which he or she must choose at least three; there is no max limit on the number of things that may be chosen. One of the recognition-based techniques is used for this. The user then draws the chosen items, which are then saved in the database with the given username. Objects can be simple, often encountered objects, characters, symbols, auto forms, etc.

3) while authentication, the user uses a mouse or a stylus to sketch pre-selected symbols on a touch-sensitive display (or elsewhere as appropriate) as his password. In order to accomplish this , the solely recall-based techniques.

4) During this step pre-processing is done by the system.

5) The user's input is used by the algorithm to blend the user-drawn sketch's lines in the fifth stage.

6) Hierarchy is constructed by the system after merging the lines.

7) This step involves simplification of sketch.

8) During step eight , The user's sketch is used to extract three different types of characteristics.

9) This is the last step which involves the hierarchical matching.

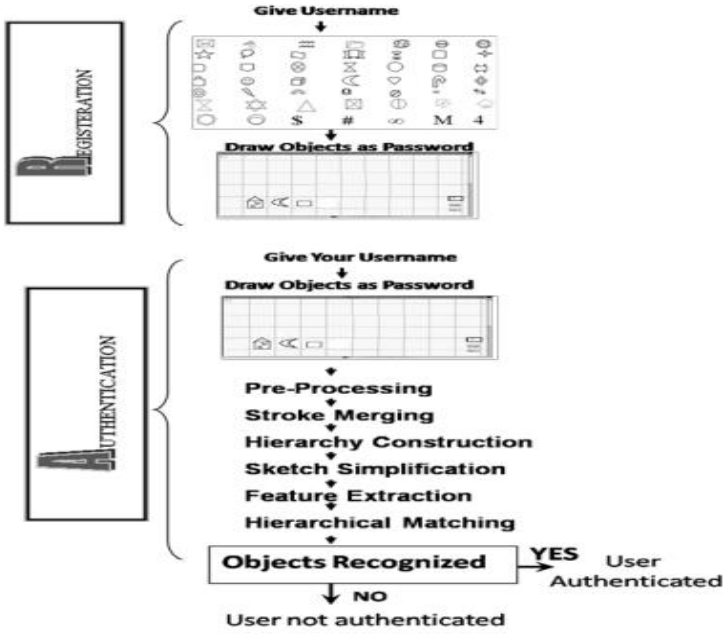
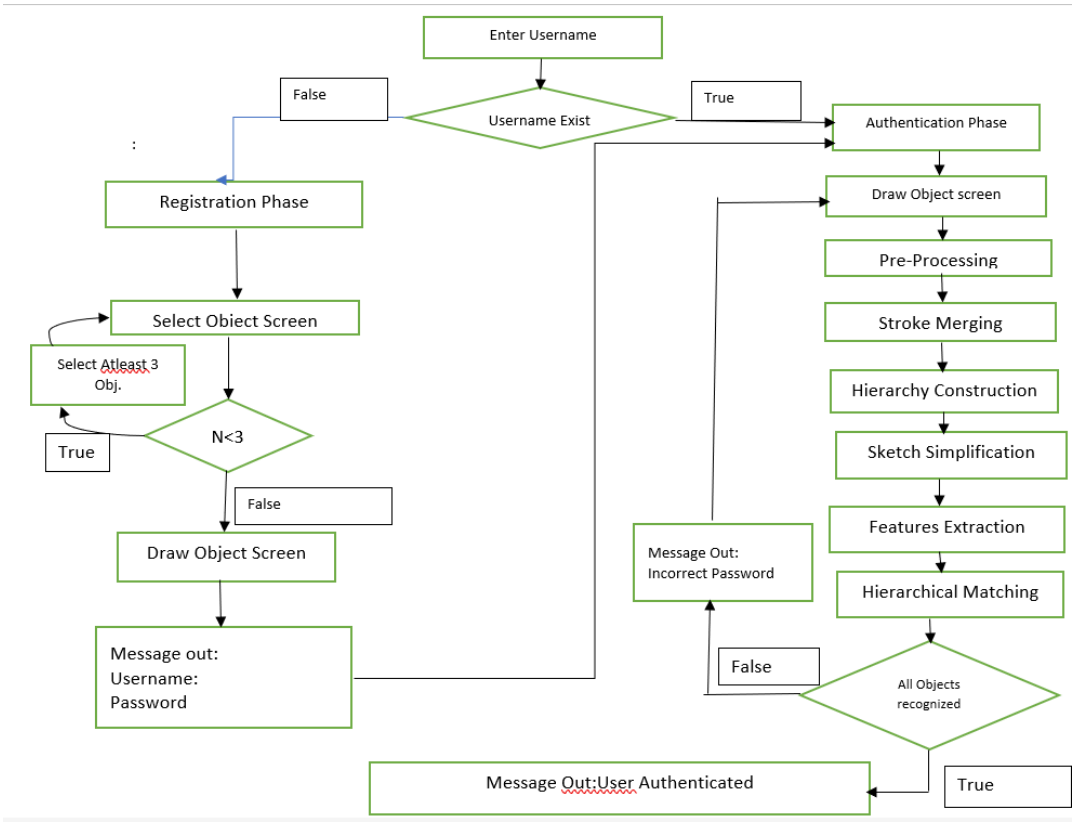


Fig 5: Graphical Represntation of Proposed System

5.1. Graphical Authentication System Flowchart:[19]



5.2. Result and analysis of the implemented of the implemented system :

5.2.1. User friendly of Graphical Password:

An easy-to-use authentication scheme is the graphic password. We can utilise this system on any device or website thanks to user-friendly authentication. Because of how simple it is to use, anyone can quickly remember their password. A graphical password system like this one offers an alternative to text-based passwords. graphic authentication method, which allows users to create passwords at random and is more secure than others. The registered password is not tough to remember in this system's primary feature. The main objective of this system is to increase security using methods that are simple for users to use and challenging for hackers to guess[1].

5.2.2. Security Analysis:

Since graphical password systems have two levels, they provide strong protection against guessing and brute force attacks. The password system is a shoulder-surfing resistance scheme that is difficult for a person to guess. Its password selection is fairly broad.

A) Brute force attack:- In a digital attack known as brute force, the hacker tries to figure out the right password. Therefore, to protect against brute force assaults, the system should use a vast number of password combinations that are highly challenging for humans to remember. We develop a graphical password system in place of huge text passwords. The right password is quite difficult to figure out.

B) Spyware : Another potential attack method for graphical passwords is spyware. Spyware comes in a variety of forms, including as keyloggers, hijackers, and spybots. User-provided data is gathered via spyware. Because it is more challenging to precisely duplicate mouse movements when using graphical passwords, spyware-based assaults are more challenging to carry out. Pass picture and CAPTCHA combinations may be particularly spywareresistant.

C) Shoulder Surfing: Shoulder surfing is the practice of peering over someone else's shoulder in attempt to collect confidential material such as a password or PIN. This kind of assault happens more frequently in crowded places where it's normal for individuals to stand in line behind one another for ATMs. Shoulder surfing is a major security issue in computer networks. In shoulder surfing, an attacker listens to data sent over a communications link without being detected. When the attacker uses the information gathered, he may be able to access confidential information, compromise a system, or otherwise cause damage [1].

6. Advantages of Graphical Password Authentication :-

1. Graphical passwords are highly secured than text-based passwords.
2. Graphical passwords are easier to remember than text-based passwords.
3. Graphical passwords are more difficult to guess than text-based passwords.
4. Graphical password authentication is available on a variety of devices.
5. Increased Security

With graphical password authentication, it's much harder for someone to guess your password simply by looking over your shoulder. That's because a picture is worth a thousand words – and it would take a lot longer for someone to crack your code if they had to guess not just one word, but an entire image.

6. Greater Usability

Graphical password authentication is also more user-friendly than traditional text-based passwords. With a graphical password, you can easily create a unique image that you'll remember – but that would be nearly impossible to guess.

7. More Memorable

Let's face it, traditional text-based passwords are often hard to remember – which can lead to frustration when you can't login to your account. With a graphical password, you can create an image that is meaningful to you – and that will be much easier to recall when you need it.

8. Increased Flexibility

Finally, graphical password authentication is more flexible than text-based passwords. With a text-based password, you're typically limited to using letters and numbers – but with a graphical password, you can use any image you want. This means you can easily tailor your password to fit your own personal style.

7. Disadvantages Of Graphical Password Authentication :

There are a few potential disadvantages of graphical password authentication (GPA) that

should be considered before implementing it as a security measure.

1. GPA can be more difficult to remember than a traditional text-based password. This is because users have to remember the specific details of an image, rather than just a wordor phrase. If users forget their graphical passwords, they may have difficulty resetting them.

2. Second, GPA can be more time-consuming to input than a traditional text-based password. This is because users have to take the time to click on the correct images in the correct order. This can be especially frustrating if the images are small or hard to distinguish from one another.

3. Third, GPA may not be compatible with all devices and software. For example, some devices may not have the ability to display images, making it impossible to use GPA on those devices. Additionally, some software applications may not be designed to work with GPA, making it difficult or impossible to use GPA on those applications.

4. Fourth, GPA can be susceptible to shoulder surfing attacks. This is where someone looks over a user's shoulder while they are entering their password in order to see what images they are selecting. While this type of attack can also

be used against text-based passwords, it is often easier to carry out against graphical passwords since the attacker does not have to memorize a long string of characters.

5. Overall, there are some potential disadvantages of using graphical password authentication that should be considered before implementing it as a security measure. However, these disadvantages should not outweigh the advantages of using GPA, which include increased security and usability.

6. One of the main disadvantages of graphical password authentication is that it can be quite easy to forget your password. If you are someone who tends to forget things easily, then this type of authentication may not be right for you.

7. Additionally, if you lose or misplace your phone or tablet, anyone who has access to it will be able to unlock your device and potentially gain access to all of your personal information.

8. Conclusion and Future Work :

Digital devices are meet a larger portion of our daily life. Using digital tools, we were able to learn well the procedure of authenticating. Validation is a vital part of safety. Authentication will make the customer feel more secure. Specific research reports in the same topic have focused on the particular attacks discovered during validation. Printed hidden term authentication is a useful testing technique. It is more useful and safe as compared to prior, simpler graphical password authentication techniques. As a result of the scope of the password space, it offers defence against brute force attacks. Utilizing it is easy. It's easy to create and remember passwords.. In both authentication systems, randomization offers good security against shoulder surfing. High security and decent usability are essential components of every successful system and cannot be separated. Attacks on the shoulder while navigating are subject to safety measures. However, there is still room for improvement in the shoulder surfing problem's suggested solutions. The textbased password system can also be strengthened with the help of this approach. When comparing with a biometrics system, this technology is incredibly affordable. There is always room for improvement, so we need to make our authentication methods more safe, dependable, and durable. We are collaborating on the System,Research and implementation. Future research will focus on user adoption, usability, and system security, among some other key aspects of our system's performance.

Table1 : Different Graphical Password Authentication system with their potential to oppose the hacker attacks.

Graphical Password System	Type of the system	Resistance to the possible attack (in terms of Yes or No)					
		Brute Force Attack	Dictionary Attack	Guessing Attack	Spyware	Shoulder Surfing Attack	Phishing Attack
DAS[20]	Pure recall based	NO	YES	YES	NO	YES	NO
Qualitative DAS[21]	Pure recall based	NO	-	-	-	-	-
BDAS [22]	Pure recall based	NO	-	-	-	-	-
Syukri Algorithm [23]	Pure recall based	NO	YES	YES	NO	YES	NO
Pass-Go [24]	Pure recall based	YES	-	-	-	-	-
Pass-Map[5]	Pure recall based	YES	NO	-	NO	YES	NO
Viskey SFR	Pure recall based	YES	NO	YES	NO	YES	NO
Passdoodle [25][26]	Pure recall based	NO	-	-	-	-	-
YAGP[27]	Pure recall based	YES	-	YES	-	YES	-
Haptic password system[28]	Pure recall based	-	-	-	-	YES	-
Blonder's Scheme	Recognition based	YES	NO	YES	NO	YES	NO
Pass-Face[2][4]	Recognition based	YES	YES	YES	NO	YES	NO
Perring and song[3]	Recognition based	YES	NO	YES	NO	YES	NO

Man et al Scheme	Recognition based	YES	NO	NO	YES	YES	NO
Sobrado and Birget[3]	Recognition based	YES	NO	YES	NO	NO	NO
Picture password system	Recognition based	YES	NO	YES	NO	YES	NO
WIW	Recognition based	-	-	-	-	YES	-
Photographic authentication[16]	Recognition based	-	YES	-	-	-	-
Association based system	Recognition based	-	-	-	-	YES	-
Two step authentication[	Hybrid	-	-	-	YES	NO	YES
CDS	Hybrid	-	-	-	-	YES	-
Our Implemented System	Hybrid	YES	YES	YES	YES	YES	YES

References

[1] Graphical Password Authentication System. Pathik Nandi, Dr. Preeti Savant. Ijraset Journal For Research in Applied Science and Engineering Technology. 2022-04-19.

[2] Graphical Password Authentication System .Akshay Karode, Sanket Mistry and Saurabh Chavan. International Journal of Engineering Research & Technology (IJERT). 9, September – 2013.

[3] Graphical Password Authentication for Secure Online Services , Prashanthi Muddam, D.Raman, International Research Journal of Engineering and Technology (IRJET) 08,Aug-2016.

[4] Hafiz Zahid Ullah Khan, "Comparative Study of Authentication Techniques", International Journal of Video & Image Processing and Network Security IJVIPNS Vol: 10 No: 04.

[5] Token Based Authentication: http://www.w3.org/2001/sw /Europe/events/foaf galway/papers/fp/token_based_authentication.

[6] Graphical Password Authentication . K Himaja Sri , M Vishnu Vardhan, K Nikitha , K M Kiran , Mrs Saritha A K . Journal of Xi'an University of Architecture & Technology,2020.

[7] Approaches to Authentication: http://www.e.govt.nz/plone/archive/services/see/see-pki-paper-3/chapter6.html?q=archive/services/see/see-pki-paper-3/chapter6.html .

[8] Knowledge based Authentication: http://searchsecurity.techtarget.com/definition/knowledge-based-authentication .

[9] A Novel Graphical Password Authentication Scheme with Improved Usability. Touraj Khodadadi; Yashar Javadianasl; Faranak Rabiei; Mojtab. IEEE 2021.

[10] User Authentication by Secured Graphical Password Implementation, Ankesh Khandelwal, Shashank Singh, Niraj Satnalika , International Journal of Computer Applications (0975 – 8887)

[11] I. Jermyn, A. Mayer, F. Monrose, M. K. Reiter, and A. D. Rubin, "The Design and Analysis of Graphical Passwords," in Proceedings of the 8th USENIX Security Symposium, 1999.

[12] G. E. Blonder, "Graphical Passwords," in Lucent Technologies, Inc., Murray Hill, NJ, U. S. Patent, Ed. United States, 1996.

[13] Passlogix, "www.passlogix.com," last accessed in June 2005.

[14] Susan Wiedenbeck, Jim Waters, Jean-Camille Birget, Alex Brodskiy and Nasir Memon, "Authentication Using Graphical Passwords: Effects of Tolerance and Image Choice", SOUPS'05 Conference, July 6-8, 2005, Pittsburgh, PA, USA.

[15] Susan Wiedenbeck, Jim Waters, Jean-Camille Birget, Alex Brodskiy and Nasir Memon, "PassPoints: Design and longitudinal evaluation of a graphical password system", International Journal of Human-Computer Studies (Special Issue on HCI Research in Privacy and Security) 63, 102-127, 2005. - Elsevier Ltd, http://www.science

[16] Jean-Camille Birget, Dawei Hong and Nasir Memon, uGraphical Passwords Based on Robust Discretization", IEEE Transactions on Information Forensics and Security, Vol. 1, No.3, September 2006.

[17] A. Adams and M. A. Sasse, "Users are not the enemy:

why users compromise computer security mechanisms and how to take remedial measures," Communications of th ACM, vol. 42 pp. 41-46, 1999.

[18] R. Dhamija and A Perrig, "Deja Vu: A User Study Using Images For Authentication", 9th USENIX Security Symposium, 2000.

[19] A Graphical Password Based System for Small Mobile Devices, Wazir Zada Khan1 , Mohammed Y Aalsalem2 and Yang Xiang, IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 5, No 2, September 2011.

[20] I. Jermyn, A. Mayer, F. Monrose, M. Reiter, and A. Rubin, "The design and analysis of graphical passwords", In 8th USENIX Security Symposium, August 1999.

[21] D. Lin, P. Dunphy, P. Olivier, J. Yan, "Graphical Passwords & Qualitative Spatial Relations", Proceedings of the 3rd Symposium, On Usable Privacy and Security, Pittsburgh, USA, 2007, pp. 161-162.

[22] P. Dunphy and J. Yan, "Do background images improve \Draw a Secret" graphical passwords?", In 14th ACM Conference on Computer and Communications Security (CCS), October 2007.

[23] A. F. Syukri, E. Okamoto, and M. Mambo, "A User Identification System Using Signature Written with Mouse", In Third Australasian Conference on Information Security and Privacy (ACISP): Springer Verlag Lecture Notes in Computer Science (1438), 1998, pp. 403-441.

[24] Hai tao, "Pass-Go, a New Graphical Password Scheme", Master Thesis, University of Ottawa Canada, June 2006.

[25] J. Goldberg, J. Hagman, and V. Sazawal, "Doodling our way to better authentication", (student poster), In ACM Conference on Human Factors in Computing Systems (CHI), April 2002.

[26] C. Varenhorst, "Passdoodles: A lightweight authentication method', MIT Research Science Institute, July 2004.

[27] H. Gao, X. Guo, X. Chen, L. Wang, and X. Liu, "YAGP: Yet another graphical password strategy", In Annual Computer Security Applications Conference, 2008.

[28] M. Orozco, B. Malek, M. Eid, and A. El Saddik, "Haptic-based sensible graphical password", In Proceedings of Virtual Concept, 2006.

[29] Barwal, R. K. ., Raheja, N. ., Mohan, B. R. ., U, Y. ., Gadde, S. S. ., & Patil, M. . (2023). Analysis and Classification of Breast Cancer Disease Via Different Datasets and Classifier Models. International Journal on Recent and Innovation Trends in Computing and Communication, 11(3s), 135–143. https://doi.org/10.17762/ijritcc.v11i3s.6174

[30] Yathiraju, D. . (2022). Blockchain Based 5g Heterogeneous Networks Using Privacy Federated Learning with Internet of Things. Research Journal of Computer Systems and Engineering, 3(1), 21–28. Retrieved from https://technicaljournals.org/RJCSE/index.php/journal/article/view/37