iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 11 **Issue:** V **Month of publication:** May 2023

DOI: https://doi.org/10.22214/ijraset.2023.51883

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue V May 2023- Available at www.ijraset.com

Graphical Password Authentication

Utkarsh Bhardwaj[1], Vishal Krishna[2], Tanya[3], Sudhanshu Verma[4], Dr. (Prof.) Ragini Karwayun[5]
Department of Information Technology, Inderprastha Engineering College, Sahibabad, U.P. India

Abstract: ***A graphical password authentication is a form of authentication where users select a picture, image, or sequence as their password. Graphical passwords are an alternative to alphanumeric passwords in which users click on graphical images rather than typing alphanumeric characters to authenticate their identity. This method has gained popularity due to its ease of use and ability to provide better security than traditional alphanumeric passwords. This research paper provides a comprehensive study of graphical password authentication, including its history, types, advantages and disadvantages, security concerns, and future developments. The paper also includes a review of related research on graphical password authentication and its effectiveness in different settings.***

Keywords: Graphical Password, Information Security, Alphanumeric Passwords, Usability, Security, Shoulder Surfing.

I. INTRODUCTION

Authentication is a crucial part of the security system, as it provides access control to the users. The traditional authentication method involves the use of alphanumeric passwords, but this method has several limitations, such as the difficulty of remembering complex passwords and the potential for password cracking. Graphical password authentication is an alternative method that has emerged in recent years as a more user-friendly and secure approach. This method allows users to select a picture, image, or sequence of pictures as their password. Graphical password authentication has gained significant attention in recent years, and several research works have been conducted to evaluate its effectiveness and security. This research paper aims to provide a comprehensive study of graphical password authentication. Verification is the process of determining if a client should be granted access to a given framework or item. It is a fundamental area of safety investigation and practice. Alphanumeric passwords are widely used for authentication, however other methods, such as biometrics, are also available today. In any event, there are problems with these optional developments. As a result, passwords remain prevalent and are expected to remain so for some time.

II. MOTIVATION

The primary motivation for graphical passwords is to make it easier for people to read or understand graphical content. It has been observed that cracking the graphical security mechanisms is difficult with conventional assaults. Graphical secret phrase plans have been presented as a potential alternative to conventional validation methods, owing to the fact that people can successfully recall images. Pictures, overall, are easier to remember or perceive. This research paper aims to provide a comprehensive study of graphical password authentication. Graphical password authentication is not a new concept, and it has been in use since the 1970s. The first graphical password system was introduced by Blonder in 1970, which used a touch screen to draw a signature for authentication. However, the technology was not advanced enough at that time, and the system was not implemented. In the 1990s, several researchers proposed graphical password authentication methods, including PassPoints, which used a grid of images, and Graphical Passwords, which used a combination of colors, shapes, and images. These systems provided better usability and security than traditional alphanumeric passwords. GPA has several advantages over traditional alphanumeric passwords. It is easier to remember than alphanumeric passwords, as users can select graphical elements based on their memory or personal preferences. Furthermore, GPA is more resistant to dictionary attacks than alphanumeric passwords, as the number of possible graphical combinations is significantly higher than the number of possible alphanumeric combinations.

III. LITERATURE REVIEW

1) "Graphical Password Authentication" by Shraddha M. and her colleagues. They created a graphical approach for passwords in which showed some of the most powerful graphical techniques for passwords, such as multiple-image basis passwords, in which a number of figures are visualized to the user and they must choose some of them. Following the grid base scheme, which is a simple item, no additional displays are necessary. Next, there is the Triangle scheme, which has a protruding surface and a large selection of images to choose from. The most important feature in this study is the calculation of the username base. As a result, there is frequently a new scheme that provides solutions to several faults with the present system, "A New Password Scheme which is Graphical That Is Resistant to Shoulder-Surfing".

©IJRASET: All Rights are Reserved

2) Patrick al. identified the least strong link in computer system security: human mistakes. The major areas in which humans interact with computers intentionally include Security operations, authentication and the development of secure systems are all areas of expertise. This section focuses on authentication. Since we currently are on the subject of authentication, it's very critical to realize that it's a function in which the user gives a proof to the system in order to receive services.
3) The security properties of graphical authentication are discussed in this study. Different graphical password schemes take different ways to preventing cyber-attacks. As you know, graphical passwords are simple to remember and provide strong security. As a result, graphical password schemes provide higher levels of security than text-based passwords. Examples of graphical password authentication attack resistance include shoulder surfing, brute force, dictionary attacks, guessing attacks, malware, and social engineering assaults.
4) Jermyn et al. devised the concept of sketch a secret, which allows users to draw passwords that have nothing familiar. The person is provided a 2d grid-based platform on which to design a uncomplicated artwork, as illustrated in Fig 1. During authentication, the user is eager to repaint the image. Only when the image goes through the identical sequence of grids as during the registration step is the user verified. Grid is a simple object that does not require any further displays. Disadvantages: Sequence during authentication or grid Because it is only a drawing, it may not be the same.
5) Jensen et al. proposed an image password strategy for PDAs in which the person was questioned to choose a theme with dimensions of 40 x 40 were presented in a 5 X 6 matrix on the basis of a preset subject; the operator had to select appearances from the matrix using a stylus. A password is developed by recording a order which is numerical based on selection of photos. During the login period, the person must recognize the same photos in the same sequence. The main flaw was that the password space was limited because the number of photos was limited to 30.
6) Real User Corporation developed passfaces, a product that is supported by the notion that the human brain can instantly recognize familiar faces. The user must select four options during registration. If the user accurately recognizes four passfaces twice in a row, the registration process is complete. A screen questioning for login with a grid of faces is given to the user via the login. The user must choose 4 faces, one from every of 4 grids of nine faces. Passfaces are predictable because they are influenced by competitiveness, gender, and beauty.
7) Patrick al. identified the weakest link in computer system security: human factors. The major areas where humans should interact with computers intentionally include authentication, security operations, and developing secure systems. Authentication is the focus of this section. Since we are on the subject of authentication, it's important to realize that it's a function in which the user gives a proof to the system in order to receive services.
8) Davis al created own Faces version and organized a long-term user research. The results indicated that people will remember their photos properly, but that chosen passwords were easily guessable. Davis al. suggested Story, an alternate approach that used ordinary images rather than faces and asked users to select photos in the appropriate order. As a memory aid, users were urged to compose a story.
9) Sobrado and Birget devised a technique for preventing surfing attacks. During registration, the person was asked to choose things from a list of presented things. At login time, the user must select the items indicated during registration and then strike inside the convex hull formed by the objects. 1000 items were used during the login procedure to expand the password space. The display, on the other hand, became clogged, making it difficult to locate pass-objects. Greg Blonder pioneered a recall-based graphical password technique in 1996. In general, graphical password procedures are divided into two categories: recognition-based graphical techniques and recall-based graphical techniques.
10) Wiedenbeck et al. proposed a system in which the operator must select a background. The user can randomly click on the image to register the order of click points on the image to be used as the password. When login in, the operator must click on points like they did during registration. If the click points are within the predefined level of tolerance, they are tolerated. This strategy provides a lot of password space.
11) Grinal Tuscano et al. proposed a two-step graphical password authentication method based on Pass faces. To create a system that is both user-friendly and tough to crack, we mixed visuals and text. The initial photos chosen by the user are extremely vulnerable to guessing attempts.
12) Man et al. created an algorithm to resist shoulder surfing attacks. In this approach, the user selects a large number of photographs as pass-objects. Every so-called passobject contains multiple variants, and each variety is assigned a code that is unique in nature. The user is given with a variety of objectives and situations during authentication. Each scene contains a big number of pass-objects (each in the form of a randomly selected variant) as well as a huge number of decoy-objects. The user

must specify the unique code that corresponds to the different versions of the pass-objects in the scene, as well as the code that specifies the pass objects' relative location in reference to a pair of eyes.

13) G.E Blonder proposed a technique in which a picture is accessible to the user through tap parts, and the user must authenticate by clicking inside those tap areas in a specific order. The main downside of this design was the lack of memorable password space, as well as the user's inability to click where he desired due to already arranged sections.

IV. PROBLEM STATEMENT

An alphanumeric password is an old and widely used authentication technique. In practice, this old method is an insecure system. For example, if the user does not choose a strong password, the attacker may use an easily guessed password. The user may use the same password for multiple devices or websites. All of these are unsafe characteristics for normal users. And authentication is one of the critical security points where the user bears active responsibility for the security of their personal information. If we employ an old traditional password system, we may be vulnerable to dictionary attacks and brute force attacks.

V. COMPUTER AUTHENTICATION

Authentication [1] is the procedure by which a user proves their identity to a system or server. Entering a username and password when logging into a website is a common example. There are numerous forms of authentication.

1) SFA (single-factor authentication).
2) Two-factor authentication (also known as 2FA).
3) MFA (multifactor authentication).

Authentication permits legitimate users to gain access to the computer. If the authentication does not match, the unauthorized user will be refused access. Any digital system or site that needs to know who the actual authorized user is will employ this authentication mechanism. Even authentication is used to determine which resources the user has access to and which are denied access to, when the user has access to the resource, and how much of the source the user can consume.

Typically, server authentication requires the usage of a login and password. Other methods of authentication include cards, retina scans, voice recognition, and fingerprints, for instance. Client authentication often entails the server supplying the client with a certificate that a trusted third party, such as a bank, expects from the client. Authentication does not define which activities or files a user may conduct or view. Authentication merely identifies and verifies the identity of the user or system.

The primary goal of authentication is to grant authorized users access to the computer while denying unauthorized user access. Passwords, physical identification, and biometrics are three methods used by operating systems to identify and authenticate users.

VI. METHODOLOGY

A. Flowchart

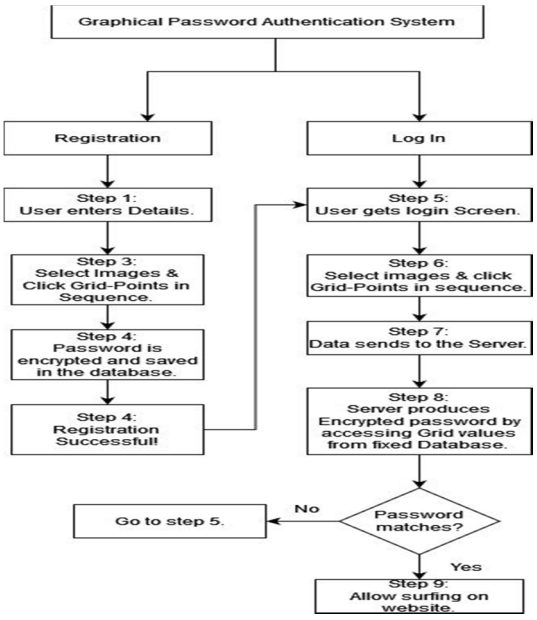


Figure 1 Flowchart for proposed system

B. Sequence Diagram

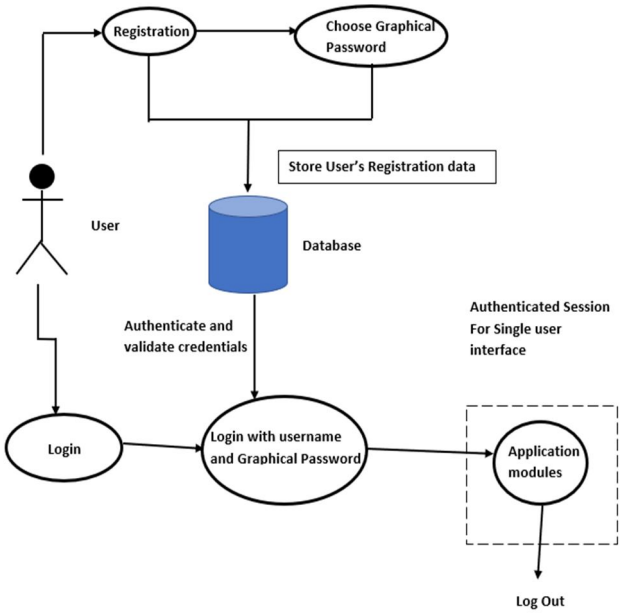


Figure 2 Sequence diagram for proposed system

C. Modules

The major modules and their respective functionalities are as follows:

1) Login page: contains username, graphical password, and captcha.

2) Password: contains image in matrix format.

VII. RESULTS

Techniques	Text Based	Color Based	Image Based
Security	Less	Highest	Highest
Usability	Easy	Easy	Easiest
Recollection Factor	Decline with time	Moderate	High
User Interface	GUI Based / Less interactive	GUI Based / More interactive	GUI Based / Most interactive
Prone to Shoulder Surf	High	Low	Low

Figure 3 Comparison of existing authentication techniques

VIII. IMPACT ON SOCIETY

Graphical password authentication has a significant impact on society, as it provides a more user-friendly and secure method of authentication compared to traditional alphanumeric passwords. Some of the impacts of graphical password authentication on society are as follows:

A. Improved Security

Graphical password authentication provides a higher level of security than traditional alphanumeric passwords. It is difficult for attackers to guess or crack graphical passwords, as the combination of images and sequence is unique to each user.

B. Ease of Use:

Graphical password authentication is more user-friendly than traditional alphanumeric passwords. Users can easily remember their selected images and sequence of images, and the authentication process is less cumbersome.

C. Accessibility

Graphical password authentication is accessible to a wide range of users, including those with disabilities such as dyslexia, as it does not rely on text-based input.

D. Reduced Risk of Identity Theft

Graphical password authentication reduces the risk of identity theft, as it is more challenging for attackers to gain unauthorized access to a user's account.

E. Improved User Experience

Graphical password authentication provides an improved user experience, as it offers a more engaging and interactive way of authenticating. Users can select images that are meaningful to them, making the authentication process more enjoyable.

F. Potential for Innovation

Graphical password authentication has the potential for innovation, as researchers and developers can continue to explore new ways to enhance its security and usability. This could lead to the development of new authentication methods that are even more secure and user-friendly.

IX. CONCLUSION

In conclusion, graphical password authentication is an alternative method that has gained popularity due to its ease of use and ability to provide better security than traditional alphanumeric passwords. Future developments in graphical password authentication should focus on enhancing its security and usability. The development of biometric graphical password authentication, contextual graphical password authentication, multi-factor graphical password authentication, machine learning-based graphical password authentication, and usability improvements are some of the potential future developments in graphical password authentication. These developments can address the security concerns of graphical password authentication and provide a more secure and user-friendly authentication method.

X. ACKNOWLEDGEMENT

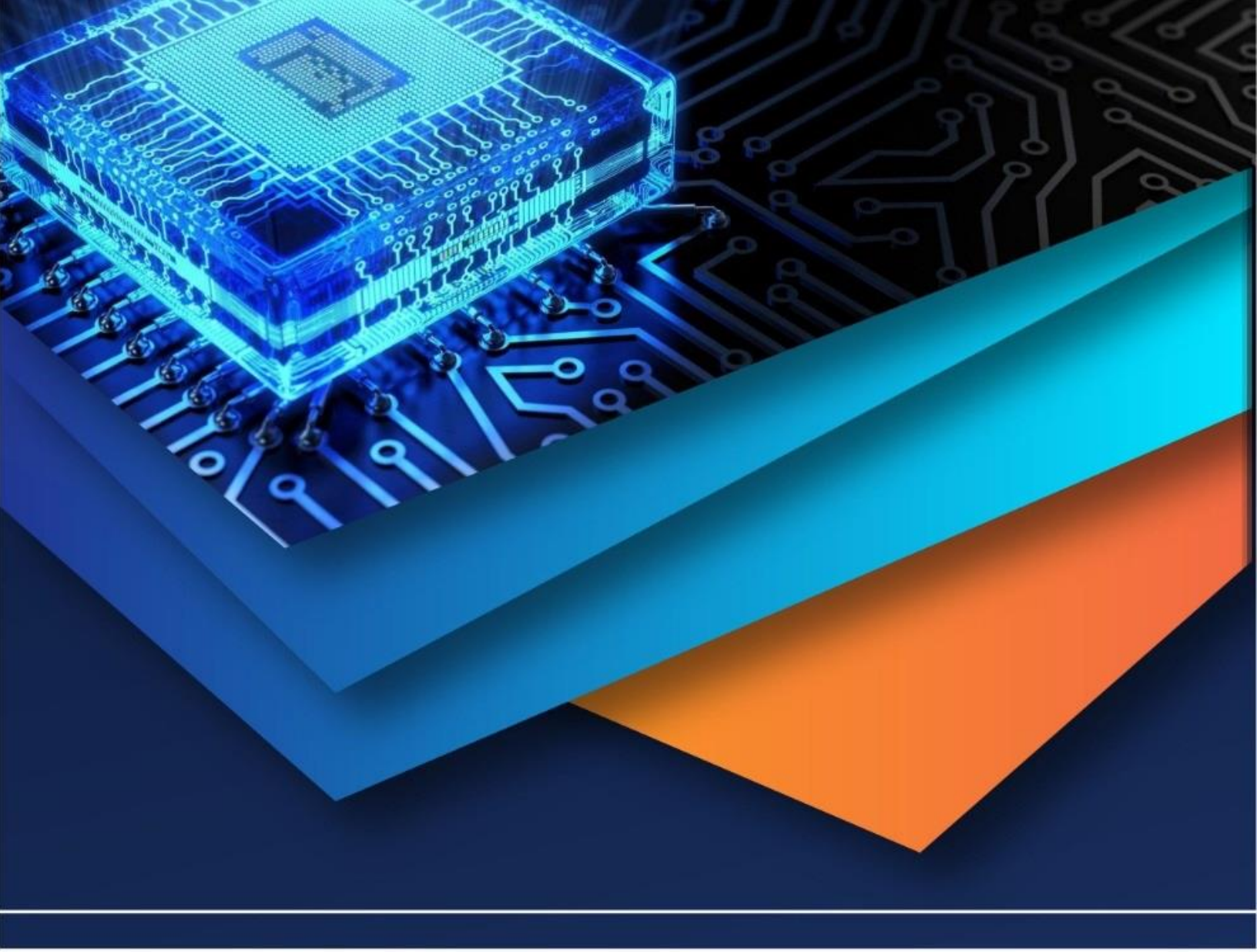
We take this opportunity to express our profound gratitude and deep regards to Dr. (Prof.) Ragini Karwayun for her exemplary guidance, monitoring and constant encouragement throughout the course of this project. The help and guidance given by her from time to time shall carry us a long way in the journey of life on which we are about to embark.

REFERENCES

[1] Graphical Password Authentication. Shraddha M. Gurav Computer Department Mumbai University RMCET Ratnagiri, India. Leena S. Gawade Computer Department Mumbai University RMCET Ratnagiri, India, 2014 IEEE.
[2] A. S. Patrick, A. C. Long, and S. Flinn, “Hci and security systems,” in CHI’03 Extended Abstracts on Human Factors in Computing Systems, pp 1056-1057,ACM 2003.
[3] A New Graphical Password Scheme Resistant to Shoulder-Surfing. Uwe Aickelin School of Computer Science the University of Nottingham Nottingham, NG8 1BB, U.K.
[4] I. Jermyn, A. Mayer, F. Monrose, M. K. Reiter, and A. D. Rubin, “The design and analysis of graphical passwords.,” USENIX Association, 1999.
[5] W. Jansen, S. Gavrila, V. Korolev, R. Ayers, and R. Swanstrom, "Picture Password: A Visual Login Technique for Mobile Devices," National Institute of Standards and Technology Interagency Report NISTIR 7030, 2003.
[6] A. Jain, L. Hong, and S. Pankanti, "Biometric identification," Communications of the ACM, vol. 33,pp. 168-176, 2000.
[7] D. Weinshall and S. Kirkpatrick, "Passwords You’ll Never Forget, but Can’t Recall," in Proceedings of Conference on Human Factors in Computing Systems (CHI). Vienna, Austria: ACM, 2004.
[8] Real User Corporation, Passfaces TM http://www.realuser.com, January 2007.
[9] S. S. Ganorkar ,Prof. H. V. Vyawahare, “Review Paper On Graphical Password Authentication Techniques “ Volume 5, Issue 03, March -2018.
[10] D. Davis, F. Monrose, and M. K. Reiter, "On user choice in graphical password schemes," in Proceedings of the 13thUsenix Security Symposium. San Diego, CA, 2004.
[11] G. E. Blonder. Graphical password. U.S. Patent 5559961, Lucent Technologies, Inc. (Murray Hill, NJ), August 1995.
[12] D. Hong, S. M an, B. Hawes, and M. Mathews, “A password scheme strongly resistant to spyware”, In Proceedings of International conference.
[13] Xiaoyuan Suo, Ying Zhu, and G. Scott Owen. Graphical passwords: A survey. In Proceedings of Annual Computer Security Applications Conference, pages 463–472, 2005.
[14] R. Dhamija and A. Perrig. “Déjà vu: A User Study Using Images for Authentication”, In Proceedings of the USENIX Security Symposium, 2000.

[15] Sobrado, L and Birget, J. “Graphical Passwords”, The Rutgers Scholar, An Electronic Bulletin of Undergraduate Research, Ruthgers University, New Jersey, Vol.4, 2004.
[16] S. Wiedenbeck, J. Waters, J. C. Birget, A. Brodskiy, and N. Memon, “Authentication Using Graphical Passwords: Basic Results”, In Human-Computer Interaction International (HCII 2005), Las Vegas, NV, 2005.
[17] M. G. Tuscano and A. Tulasyan, “Graphical password authentication using pass faces,” International Journal of Engineering Research and Applications, vol. 5, no. 3, pp. 60–64, 2015.
[18] S. Man, D. Hong, and M. M. Matthews, “A shoulder-surfing resis-tant graphical password scheme-wiw.,” in Security and Management, pp. 105–111, Citeseer, 2003.
[19] G. Blonder, “Graphical Password”, In Lucent Technologies, Inc., M urray Hill, NJ, United States Patent 5559961, 1996.
[20] P. R. D. Shrikala, M. Deshukh and A. B. Pawar, “Persuasive Cued Click Points with Click Draw Based Graphical Password Scheme”, International Journal of Soft Computing and Engineering, Vol.3, Issue-2 May 2013.
[21] R. Dhamija and A. Perrig, "Deja Vu: A User Study Using Images for Authentication" in Proceedings of 9 USENIX Security Symposiums, 2000.
[22] S. Chiasson, P. van Oorschot, and R. Biddle, “Graphical Password Authentication Using Cued Click Points,” Proc. European Symp. Research in Computer Security (ESORICS), pp. 359-374, Sept. 2007.
[23] J. Yan, A. Blackwell, R. Anderson, and A. Grant, “The Memorability and Security of Passwords,” Security and Usability: Designing Secure Systems That People Can Use, L. Cranor and S. Garfinkel, eds., ch. 7, pp. 129-142, O’Reilly Media, 2005.
[24] L.O’Gorman, “Comparing Passwords, Tokens, and Biometrics for User Authentication,” Proc. IEEE, vol. 91, no. 12, pp. 2019 2020, Dec. 2003.
[25] A. Jain, A. Ross, and S. Pankanti, “Biometrics: A Tool for Information Security,” IEEE Trans. Information Forensics and Security (TIFS), vol. 1, no. 2, pp. 125-143, June 2006.
[26] S. Wiedenbeck, J. Waters, J. C. Birget, A. Brodskiy, and N. Memon. "PassPoints: Design and evaluation of a graphical password system", International Journal of Human-Computer Studies, 2011.
[27] P. Golle and D. Wagner. “Cryptanalysis of a cognitive authentication scheme”, IEEE Symposium on Security and Privacy, May 2007.
[28] L. Sobrado and J.-C. Birgit. "Graphical passwords," The Rutgers Scholar, An Electronic Bulletin for Undergraduate Research, vol. 4, 2002.
[29] I. Jermyn, A. Mayer, F. Monrose, M. K. Reiter, and A. D. Rubin. "The Design and Analysis of Graphical Passwords," Proceedings of the 8th USENIX Security Symposium, 1999.
[30] R. Dhamija and A. Perrig. "Deja Vu: A User Study Using Images for Authentication," Proceedings of 9th USENIX Security Symposium, 2000.

©IJRASET: All Rights are Reserved



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)