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.2023.52227

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

Authentication Based on Image Password

Sarvesh kumar Jaiswal[1], Tejas Chore[2], Kamalesh Patil[3], Kunal Jagtap[4]
[1, 2, 3, 4]*Students, Department of Computer Engineering, Zeal College of Engineering and Research, Pune*

Abstract: ***In the modern day, graphical password authentication that relies on memory or recognition is a different and still developing sort of authentication. The user copies the picture or is able to identify the image that was used or made during the registration process. Only authorised users are able to access resources and information thanks to passwords. The newest fashion is graphic passwords, which appear to be a highly promising authentication technique. It is available as a substitute for text passwords. The most popular method is using usernames and passwords that are alphanumeric. While this method has certain benefits over plain text passwords, it also has some drawbacks. Users strive to memorise short, strong passwords that can be broken when using alphanumeric passwords, but doing so becomes cumbersome. Users that use graphical passwords save a picture or certain areas of an image as their password. Biometrics is now the most sophisticated and secure form of authentication, yet it is too costly for widespread usage. Graphical passwords are a fantastic alternative authentication mechanism since they are less expensive, more secure, and simpler for everyone to use. [1]***
Keywords: Authentication, graphical password, security, shoulder surfing, data encryption algorithm.

I. INTRODUCTION

Text-based passwords are the foundation of password-based authentication. Text-base password have grown to be significant component of security and continue to do so. Users can choose to authenticate using text or picture passwords. Text passwords are useful for users and simple to remember. Text-based passwords have the drawback of being subject to a variety of assaults. dictionary attack, DOS attack, and eavesdropping attack. To address these issues with text passwords, graphical passwords were devised. Based on the notion that graphical passwords offer several benefits over text-based passwords, this study developed a technique. These authentication methods' effectiveness is predicated on or counsels against susceptible attacks. These areas are pertinent to this project.[1]

II. DISCUSSIONON SHOULDER-SURFING RESISTANT

The Passface system is updated in this research's proposal for directional-based graphical authentication, adding a direction image as an additional security feature to hide the password and also we used Grid shuffling and Minimize brightness level.

III. OVERVIEW OF AUTHENTICATION

Information and communication technology has brought about great changes in the way information is handled. It has a positive impact on most sectors such as the economy, manufacturing, government and even tourism. A platform is being developed to manage most of the world's data. The platform is characterized by speed, reliability, robust and high performance.[1]

Security are a major concern when it is comes to accessing, transferring, and storing data. Security threats come in many forms. Developers, programmers, and even end users need to take good care to preserve information and data [2].

Human factors were identified by Patrick et al. [2] as the computer system's weakest security link. The three main areas where humans should actively interact with computers are in the areas of authentication, security operation, and secure system building. Authentication is the main topic here.

Since we're talking about authentication, it's important to know that this is a process when a user requests services from the system by presenting a form of identification. Only after the system accepts the credentials that have been provided may a user be approved [Michael Burrows, Martin Abadi, and Roger Needham, 1990]. Verifying one's identity is another name for authentication [Kurose and Ross, 2003].

The three main categories of modern authentication methods are:

1) *Biometrics Based Authentication:* This method of identification relies on the user's distinctive behavioural characteristics, or "What You Are." Biometric identification uses behavioural traits including fingerprints, voice recognition, eye scanning, and facial recognition, as the name implies. The system then verifies the data by turning it into digital information. Biometric hardware scanning equipment will collect input like fingers prints, the user's voice, iris scans, or possibly facial scans.

These biometric methods are not used very frequently. Although the biometric-based method offers a high levels of security, it also has the disadvantage of being quite expensive. Widely utilised is knowledge-base authentications. Along with text-based passwords, it also has picture-based password levels. There are further subcategories of this pic-based method, such as recall-based, where the user must recreate a replica of anything they selected or made during registration. Based on recognition, the user must accurately identifies or recognises the photographs or images throughout the registration procedure[1].

2) Token-based authentication is based on what you own or possess and is defined or decided accordingly. Taking into account the likes of a driver's licence, identification card likes a college ID, etc. allowing the user to enter their usernames or user ID and password in order to receive a token that allows them to utilise or request system resources This approach also incorporates the usage of knowledge based to increase security. examples are PIN-based ATM cards. [1]

IV. OVERVIEW OF GRAPHICAL PASSWORD

The conventional authentication method, which relied on the username and password, has several flaws and has been used by users up to this point. The primary challenge is keeping track of numerous text passwords. Studies have shown that people prefer passwords that are short and simple to remember. These passwords, along with the accounts they are associated with, are easily hackable. Biometrics is an alternatives to this text-based username and password. But we will only pay attention to the graphical passwords today.[1]

According to psychological research, people prefer to remember visuals better than text, which is the inspiration for the invention of graphical passwords. A graphical password requires more password space than a text password but offers better defence against dictionary attacks. Therefore, graphic passwords are utilised on many mobile devices as well as for workstation and website log-in.Graphic Password, mainly into two types:

1) *Recall-based techniques:* As part of the registration process, a user is required to produce a duplicate of everything already completed or chosen. Because users are capable of recalling and recreating a hidden picture, recall-based graphical password systems are frequently referred to as draw metric systems. This technique, which enables users to recall and replicate drawings that have a concealed nature, is also known as the "system of draw metrics." It's harder than it looks to recall things. [1]

2) *Recognition-based techniques:* In this case, authentication is finished by locating the images that were chosen during the registration process. The user is given access to a gallery of images in this scenario. Users of recognition-based systems need only memorise cases of photos in order to create a password; in order to log in, they must then distinguish between the same set of photos and fake ones. [1]

The remainder of the material is divided into the following sections: A review of the literature is given in Section II, an example of the approach is given in Section III, and the results are given (or a request for system resources is made) in Section IV.[1]

This strategy combine the use of knowledge-base methods with security. examples are PIN-based ATM cards.

V. LITERATURE SURVEY

Draw a Secret, an invention of Jemyn et al. [4], allows users to generate passwords that are completely unique. A platform with a 2D grid basis is provided for the user to design the straightforward image in Figure 1. The user is eager to redo the image during authentication. Only when the photo goes through the same grids in the registration step can the user be verified. Benefits: Grid is a simple object; no additional displays are necessary. Cons: Since it's only a drawing, there's a chance that the grid or sequence at authentication won't match..[1] The password is highly challenging to crack because to Wiedenbeck et al[5] .'s strategy of choosing a triangle to cover a particular area of the image password space, as illustrated in Fig. 2. The password surface is crowded and challenging to locate, which is an advantage. Cons: Convex surfaces require a lengthier assignment procedure..[1]

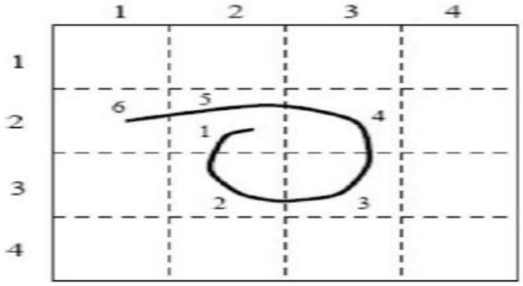


Figure 1.Drawing Grid used in literature[1]

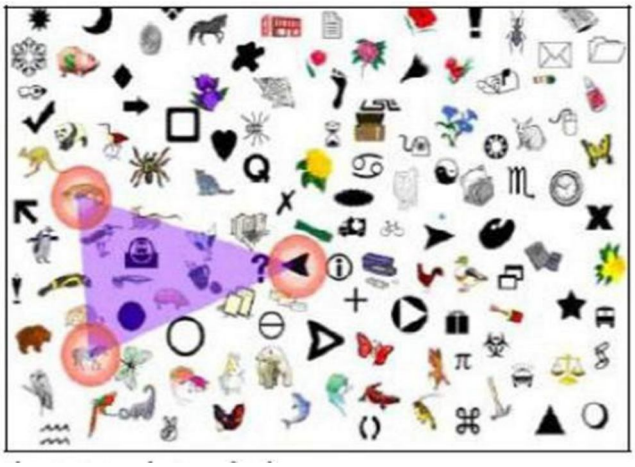


Figure 2. Triangle formation in literature [1].

Zheng et al. [6] described a method in which the user is instructed to choose a form that is simple for him or her to recall. Any shape, such as a numerical shape, a geometric shape, or any other random shape, can be used for this form, as seen in Fig 3. If there is a standard for choosing a form, it should be that the user can easily remember the shape. The user should click the grid interface once they are done and happy with the selected form in order to follow the proper stroke order. The system will then record the user's password as the order of the shape and stroke sequences. However, there are still some issues with the system. The user will first select the simplest sequence because this technique for generating passwords based on the sequence of keyboard strokes is extremely challenging and would look challenging to the general public. Second, the initial password generation process is more likely to include human mistake than the login process does. Finally, it takes a while to complete a login. [1]

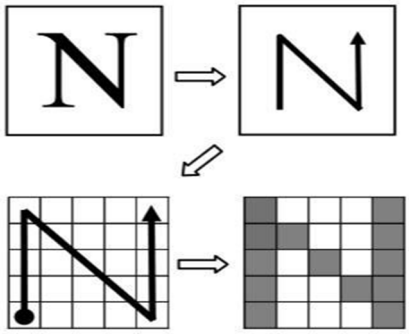


Figure 3. Stroke based Textual Password.[1].

Syukri et al. [7] created a system in which the final stage of authentication is the user's mouse-drawn signature. This approach comprises two separate phases: registration and verification. During the registration procedure, the user will use the mouse to create their signature, which the system will later record. During the verification stage, the system receives this signature as input, does normalisation, and extracts all the parameters. The emergence of duplicate signatures is a problem. When doing so for verification, it is very challenging and frequently impossible to precisely recreate a mouse-drawn signature. [1]

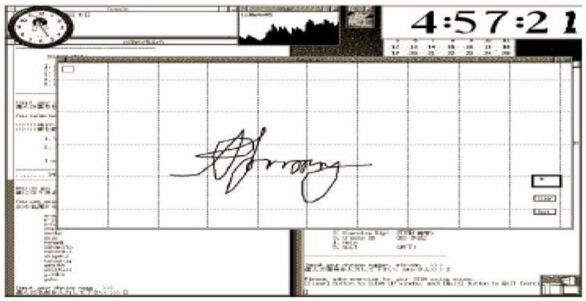


Figure 4. signature based technique [1].

A two-step graphical password authentication system based on Pass faces was proposed by Grinal Tuscano et al. in [8]. Text and images have been blended to create a system that is simple to use and hard to hack. Text and graphics are combined in a secure system that is simple to use and hard to crack. Users' initial photo selections are especially vulnerable to guessing attacks. There is a slim chance that the attacker will guess the photographs even if they have no prior knowledge about the user. The distortion method depicted in Fig. 5 can reduce the danger of attacks using group guesses that profit from biases in users' selections of authentication photographs. [1]displayed in Fig. 5 can mitigate the danger of group educated guess attacks that take use of biases in users' selections of authentication photos. [1]

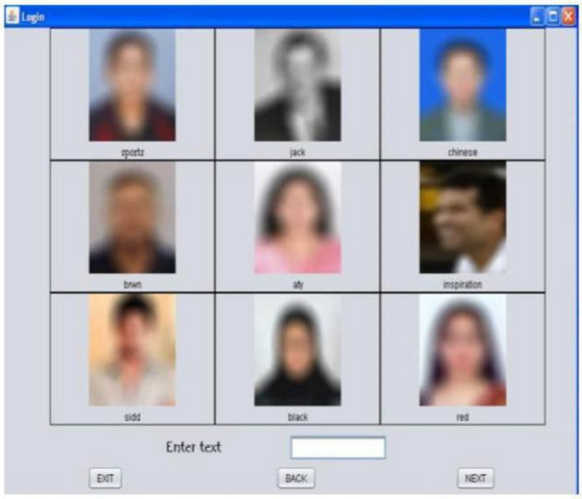


Figure 5. Interface designed for password login[1].

As seen in Fig. 6, Man, et al. [9] created an algorithm to fend off shoulder surfing assaults. A substantial number of images are chosen by the user to serve as pass-objects in this algorithm. There are several variations of each so-called pass-object, and each variation has a unique special code. Upon logging in, the user is given access to a number of options and tasks.Every single scene is made up of a sizable number of pass items (each taking the shape of a randomly selected version) and several fake objects. Here, the user must provide both a specific code designating each of the several pass-object variations that are present in the scene and a code designating the pass objects' placement in respect to a pair of eyes. A password like this is very difficult to guess, even with a video recorder, as there is no mouse click to expose the password's specifics. The alphanumeric code for each pass-object must still be kept in mind by the method's user. [1]

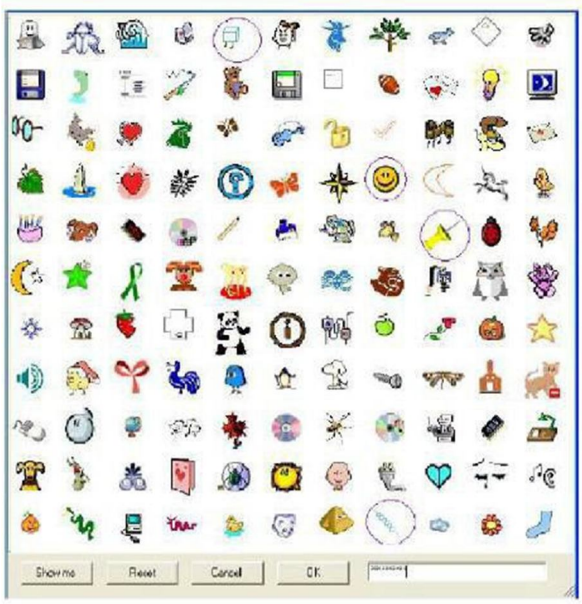


Figure 6. Shoulder surfing resistant scheme.[1].

Danish et al. [10] developed a recognition-based technique of graphic password authentications. As illustrated in Fig. 7, the user must place the registered picture in each of the three concentric rings. When all of the photos are correctly aligned, the login will be successful. [1]

Figure 7. Three chosen photographs are lined together in a certain way.
The user will click the submit button after aligning [1].

VI. METHODOLOGY

The proposed technique is depicted in Fig. 8's flowchart. The flowchart has a home page that shows two more alternatives, such as the sign-up and login pages. Customers who are new to the system utilise the sign- up page. The pre-existing users choose and use the login page.

Customers that are new to the system can sign up using this option. Users must sign up by using the sign up option in order to utilise any system and its services. Our system's sign-up option has a two-step verification process. The user must enter information, much of it of a personal nature. [1]

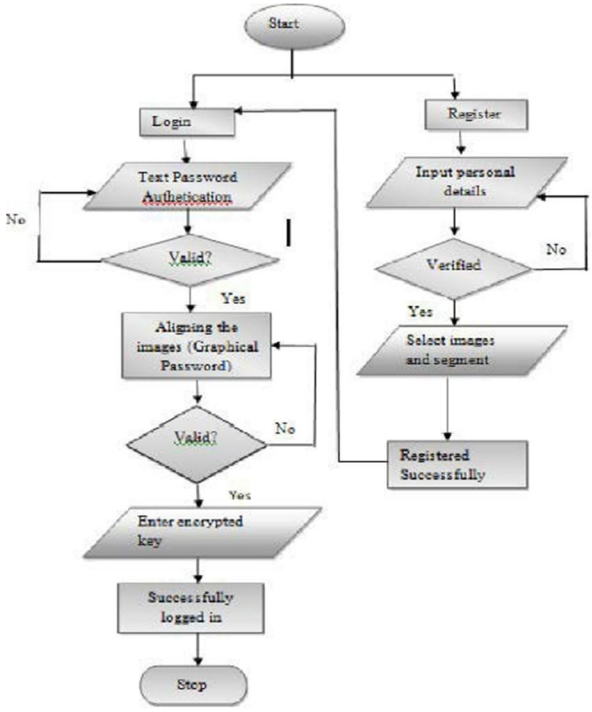


Figure 8. Overall Flowchart of the proposed method

VII. ALGORITHM FOR HASHING

we are created own algorithm for hashing a image password, which is most secure because not any attack available for this algorithm.

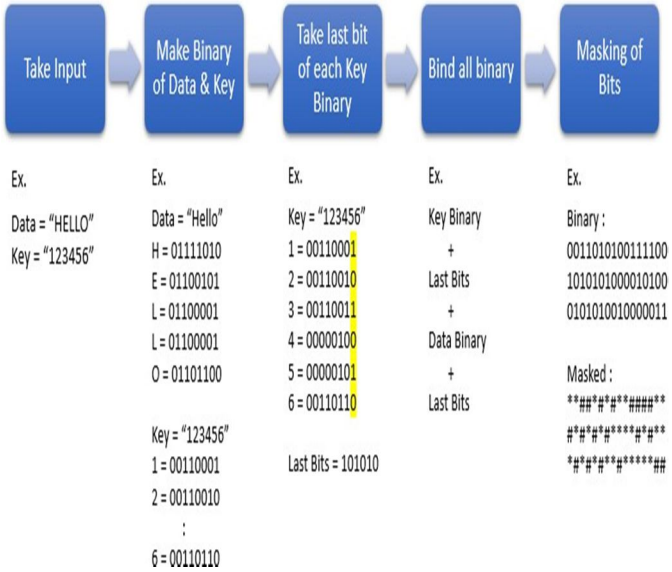


Figure 9. Encryption Method

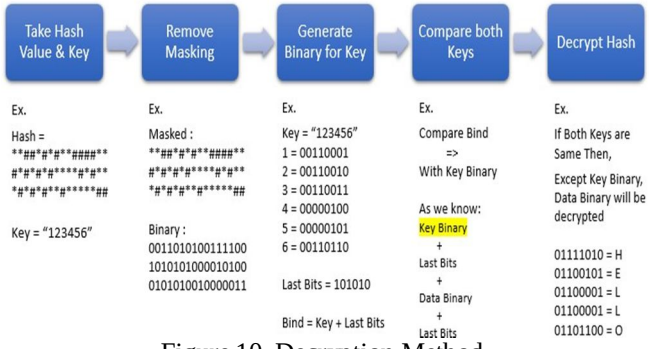


Figure 10. Decryption Method

VIII. DISCUSSION ON SHOULDER-SURFING RESISTANT

The Passface system is updated in this research's proposal for directional-based graphical authentication, adding a direction picture as an additional security feature to hide the password. Figure 1 depicts the proposed authentication's flow. [11]

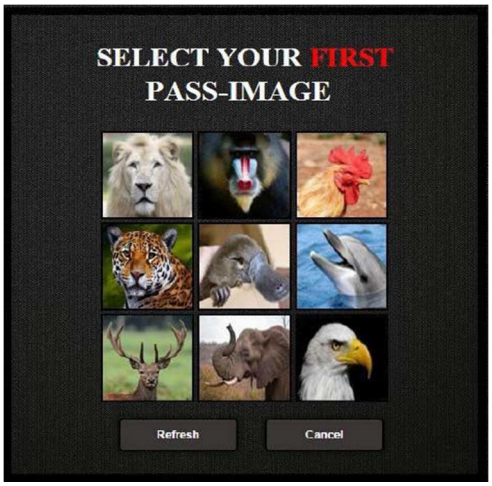


Figure 11. Pass-image Selection screen[11]

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue V May 2023- Available at www.ijraset.com

Each selection page will display nine photographs drawn at random from the first folder, as seen in Figure 2. (Note that each selection screen will show photographs from several directories, therefore each selection's pass-image will be distinct from the others.). By pressing the refresh button, the user can modify the display pictures. The user will be taken to the next selection screen after selecting an image until all four have been chosen. The user must choose a direction for their image on the final selection screen, as seen in [11]

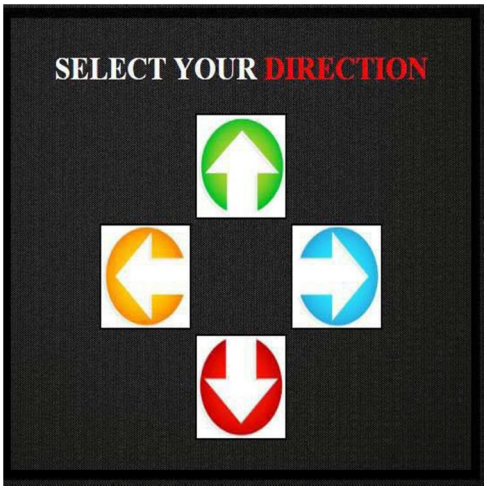


Figure 12. Direction of pass-image[11]

Each selection page will display nine photographs drawn at random from the first folder, as seen in Figure 2. (Note that each selection screen will show photographs from several directories, therefore each selection's pass-image will be distinct from the others.). By pressing the refresh button, the user can modify the display pictures. The user will be taken to the next selection screen after selecting an image until all four have been chosen. The user must choose a direction for their image on the final selection screen, as seen in [11]

Following confirmation of the chosen images, the user's email address and the five selected images will be hashed and stored in a database. The password will also be more secure during transmission because it will have been hashed before being sent to the database. [11]

Extra security for shoulder surfing :

1) *Grid Shuffled:* To provide extra security we can shuffled the grids of image, so no any can see what we are choosing.
2) *Minimize Brightness Level:* We can make screen darker, so no any one to see whole screen, what we are doing.

IX. CONCLUSION

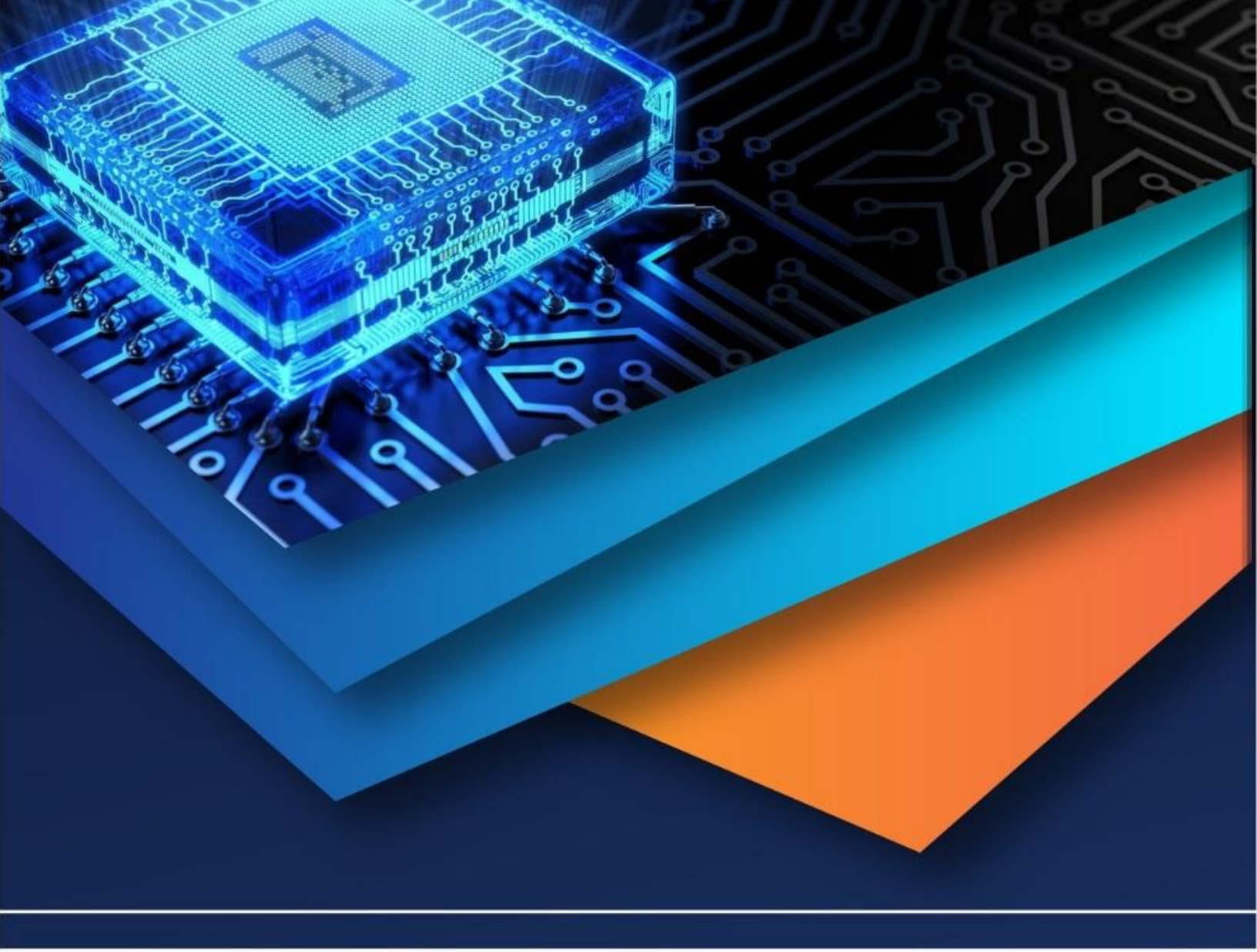
We created a graphical password in this post that is a lot more safe than plain text or alphanumeric passwords. Alphanumeric passwords were challenging to remember, but plaintext passwords were weak and could not survive assaults. A graphical password that we created increases authentication security. B. Strictly maintain the section that contains all of the circle photos. Images can be chosen in any convenient order for the user. This demonstrates that graphical passwords may be susceptible to dictionary attacks, such as, If a hacker notices the area where the alignment is done, they will be able to view the image for the password cracking. 3 * 3 * 3 different combinations are conceivable. However, we also increased email security. An encrypted key will be given to the user's email address when the image has been placed. This key must be entered to complete the last step of the login process. Your password can be cracked by an attacker, but you don't hold the key. A user will be alerted to an impending attack if they get an unexpected email that contains an encrypted key. The user will thus have another opportunity to save his account. The highest level of protection and most danger are undoubtedly provided by graphic passwords and encrypted key layers.

REFERENCES

[1] Manjula Shenoy K and Supriya A. 2019. Authentication using alignment of the graphical password. In Proceedings of the Third International Conference on Advanced Informatics for Computing Research (ICAICR '19). Association for Computing Machinery, New York, NY, USA, Article 21, 1–5. https://doi.org/10.1145/3339311.3339332

[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] X. Suo, Y. Zhu, and G. S. Owen, "Graphical passwords: A survey," in Computer security applications conference, 21st annual, IEEE, 2005.
[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] S. Wiedenbeck, J. Waters, L. Sobrado, and J.-C. Birget, "Design and evaluation of a shoulder-surfing resistant graphical password scheme," in Proceedings of the working conference on Advanced visual interfaces, pp. 177–184, ACM, 2006.
[6] Z. Zheng, X. Liu, L. Yin, and Z. Liu, "A stroke-based textual password authentication scheme," in Education Technology and Computer Science, 2009. ETCS'09. First International Workshop on, vol. 3, pp. 90–95, IEEE, 2009.
[7] A. F. Syukri, E. Okamoto, and M. Mambo, "A user identification system using signature written with mouse," in Australasian Conference on Information Security and Privacy, pp. 403–414, Springer, 1998.
[8] 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.
[9] 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.
[10] A. Danish, L. Sharma, H. Varshney, and A. M. Khan, "Alignment based graphical password authentication system," in Computing for Sustainable Global Development (INDIACom), 2016 3rd International Conference on, pp. 2950– 2954, IEEE, 2016.
[11] N. A. A. Othman, M. A. A. Rahman, A. S. A. Sani and F. H.
[12] M. Ali, "Directional Based Graphical Authentication Method with Shoulder Surfing Resistant," 2018 IEEE Conference on Systems, Process and Control (ICSPC), 2018, pp. 198-202, doi: 10.1109/SPC.2018.8704157.
[13] Haichang, G., Zhongjie, R., Xiuling, C., Xiyang, L., & Aickelin, U. "A New Graphical Password Scheme resistant to shoulder surfing", International Conference on CyberWorlds. University of Nottingham, 20-22 October 2010



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY