IARJSET

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

International Conference on Muti-Disciplinary Application & Research Technologies (ICMART-2023)

Geetanjali Institute of Technical Studies

Vol. 10, Special Issue 2, May 2023

Graphical Password Authentication

Akshat Garg[1], Aniruddh Singh Ranawat[2], Himanshu Singh[3], Dhiraj Lohar[4], Harshvardhan Singh[5]

UG Scholar, Dept. of Computer Science and Engineering, Geetanjali Institute of Technical Studies,

Udaipur, India[1,2,3,4,5]

Abstract— A graphical password is an authentication method that asks the user to choose from a set of images that are given to them in a certain order via a graphical user interface (GUI). Because of this, the graphical-password method is often known as graphical user authentication (GUA). The usage of alphanumeric usernames and passwords is the most popular computer authentication technique. It has been established that this approach has serious drawbacks. Users frequently select passwords that are simple to guess, for instance. On the other side, if a password is challenging to guess, it is frequently challenging to remember. Researchers have created authentication systems that use photos as a password to solve the issue of low security. In this study, we evaluate all of the graphical password methods that are already in use and offer a potential theory of our own. Given that humans recall images better than text and that images are typically easier to remember or recognize than text, graphic password schemes have been suggested as a potential replacement for text-based schemes. Keywords: Graphical authentication, e-mail alert, password generation.

I. INTRODUCTION

A secret password is used for authentication. In computer and communication systems, passwords are the most used way to identify users. Only the user is supposed to be aware of it. A graphical password is an authentication technique that requires the user to choose among images given in a Graphical User Interface, in a certain order (GUI). This is why the graphical password method is also known as graphic user authentication (GUA). A computer security system's weakest point is frequently thought to be human factors. Human-computer interaction is crucial in three key areas, according to Patrick: security operations, creating secure systems, and authentication. The authentication issue is the main topic here. One of the crucial and essential elements of the majority of computer security systems is user authentication. One of the key authentication strategies used to address the issues with conventional username-password authentication is biometrics. But in this case, we'll discuss a different option: using images as passwords. A recent story in Computer World said that the security team at a large corporation conducted a network password cracker and discovered roughly 80% of the passwords in under 30 seconds. On the other hand, it might be challenging to remember passwords that are challenging to guess or crack. Studies have shown that users tend to write down their passwords or reuse them across other accounts since they can only recall a finite number of passwords. Alternative authentication techniques, such biometrics, have been used to overcome the issues with conventional username and password authentication. But in this essay, we'll concentrate on a different option: utilising images as passwords. A graphical password scheme may also have a larger possible password space than text-based schemes, making it more resistant to dictionary attacks if the number of possible images is sufficiently big. There is rising interest in graphical passwords as a result of these (said) benefits.

II. LITERATURE SURVEY

M. Sreelatha proposed the hybrid textual authentication scheme in this study. In the registration process of this scheme, the user must rate the colors. Four color pairs and an 8 by 8 matrix will be shown during the login process.

The password will be generated based on the user's color rating. The grid's first color indicates the row number, and the second the column number. The disadvantage of this technique is that the password's first letter acts as an intersecting element. The user must commit to memory the color’s rankings and order. As a result, using it is quite stressful. This system's flexibility and ease of use are advantages.

She applied the OTP scheme suggested by the authors in Graphical password as an OTP. Alphanumeric passwords have a number of disadvantages, including the tendency for users to forget them or to write them down.

To address this issue, developers have created authentication techniques known as graphical passwords that employ images as passwords. They have added another level of protection by creating one-time passwords (OTPs), which are sent to users' mobile devices. The user will get the One Time Password by using the online instant messaging service (OTP). The OTP will have details on the objects in the image that the user is supposed to click. Based on the data supplied to them, the users will authenticate themselves by clicking on various things in the image.

This system's primary goal is to prevent shoulder surfing attacks. In addition, it seeks to defend against assaults like guessing, brute force, and dictionary attacks. The database is used to send the OTP to the user's mobile number. The positive point of this approach is it gives better security as \sit avoids shoulder surfing by employing OTP. The user must click within the tolerance of their chosen pixels and in the proper order, which is a drawback of this technique.

IARJSET

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

International Conference on Muti-Disciplinary Application & Research Technologies (ICMART-2023)

Geetanjali Institute of Technical Studies

Vol. 10, Special Issue 2, May 2023

III. EXISTING SYSTEM

Employing images (Graphical images) as passwords is referred to as using a graphic password. In theory, graphical passwords are simpler to remember because people can recall images more easily than words. Additionally, given that the search space is virtually endless, they ought to be more resistant to brute force attacks. The two primary categories of graphical password approaches are recognition-based and recall-based graphical procedures. In authentication methods based on recognition, a user is made to prove their identity by asking them to recognise one or more photos they chose during the registration process. A user is requested to duplicate something they chose or made earlier during the registration stage when using recall-based approaches. Pass faces is a recognition-based authentication method that tests a user's ability to recognise human faces.

Based on the type of action necessary to remember the password, graphic password schemes can be broken down into three main categories: recognition, recall, and cued recall. Human memory is best at recognition, however pure recall is hardest because it requires accessing the material directly from memory without any prompts. Cued recall lies in the middle of these two options since it provides a cue that should build context and activate the stored memory. CCP most closely resembles Pass faces, Story, and Pass Points among current graphical passwords. Conceptually, CCP combines all three; in terms of execution, Pass Points is the closest match. Additionally, it does away with the complicated user training requirements that can be seen in some graphical password proposals, such Wrenshall's.

IV. PROPOSED SYSTEM

Users with graphical passwords can select portions of the screen, which the computer subsequently transforms into an authentication code.

Photograph Password

The user is shown a grid of images (photographs) or portions of an image, and after clicking on a series of images, each segment of the grid is connected to a value matrix.

There are three basic categories in which authentication techniques currently fall:

A. Token-based authentication is one

B. Authentication via biometrics

C. Authentication based on knowledge

Key cards, bank cards, and smart cards are examples of token-based technologies that are often utilized. To increase security, several token-based authentication systems also include knowledge-based approaches. For instance, PIN codes are typically used in conjunction with ATM cards. The use of biometric identification methods like fingerprint, iris, or facial recognition is still relatively uncommon. The main disadvantage of this strategy is the potential cost of such devices, as well as the potential for sluggish and frequently unreliable identification. The maximum level of security is provided by this kind of method, nevertheless. The most popular authentication methods involve knowledge-based strategies, which include both picture- and text-based passwords. The graphical techniques that use images can be further broken down into the categories of recognition-based and recall-based procedures.

4.1 Techniques Based on Recognition: By detecting and identifying the photos they chose during registration, users authenticate themselves by being shown a selection of photographs using recognition-based techniques. A user is requested to duplicate what they chose or made earlier during the registration stage using recall-based strategies.
We suggested a graphical password system for portable electronics. A user chooses a theme comprised of photographs of their thumbnails during the enrolment process and then registers a series of images as a password. The user must enter the registered photographs in the proper order during authentication.

4.2 Cued Click Points

Pass Points are being replaced with Cued Click Points (CCP). Instead of clicking five points on one image, users in CCP click one point on each of the c = 8 images. It provides cued recall and adds visual cues that immediately notify legitimate users if they entered their most recent click point incorrectly (at which time they can terminate their attempt and retry from the beginning). Additionally, it increases the difficulty of strikes depending on hotspot analysis. Users can only choose their photos to the extent that the next image is determined by their click-point. If they don't like the images that are produced, they can make a new password that uses various click-points to produce alternate images. To access an online server, a user needs a client device that displays images,

IARJSET

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

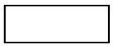
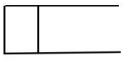
International Conference on Muti-Disciplinary Application & Research Technologies (ICMART-2023)

Geetanjali Institute of Technical Studies

Vol. 10, Special Issue 2, May 2023

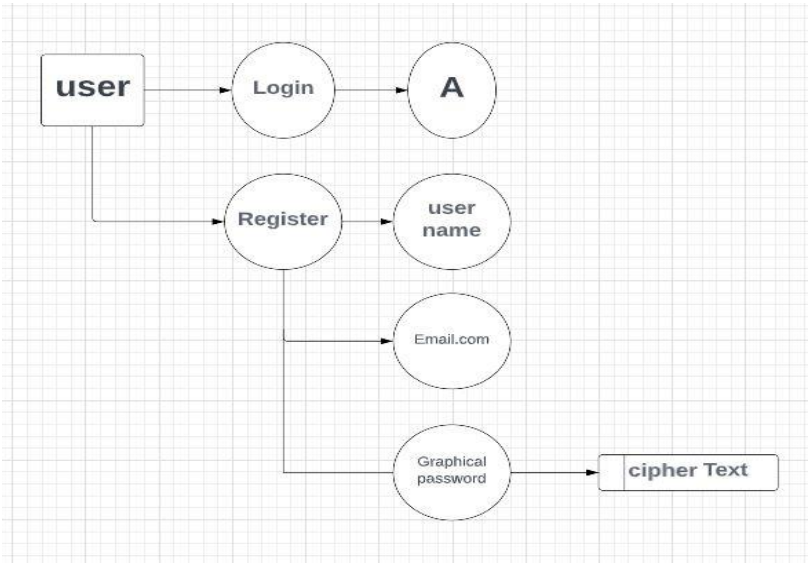
and we think that CCP fits into that authentication model (which authenticates the user). We presume that client communications use SSL/TLS and that the photos are stored server-side.

Data flow diagram:

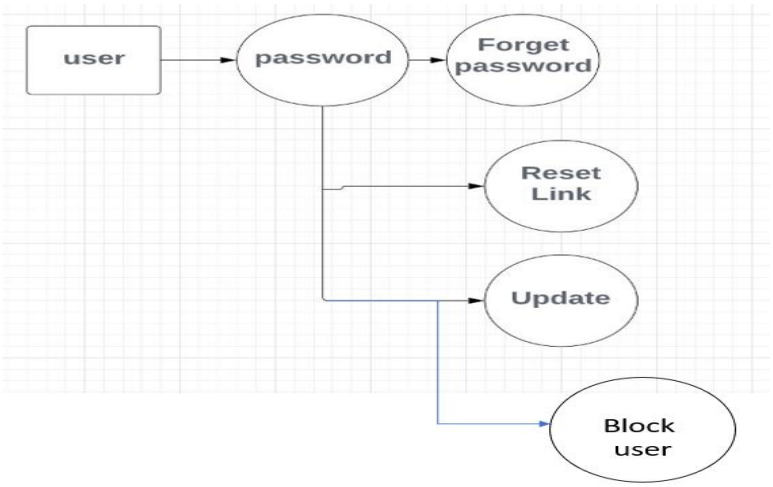
SYMBOLS	DESCRIPTION
	An **entity**. A source of Data or a destination for data
	A **process** or task that is performed by the system.
	A **Data store** , a place where data is held between processes
	A **Data Flow**

DFD Diagrams Level:

Level 0



Level 1



Level 2

IARJSET

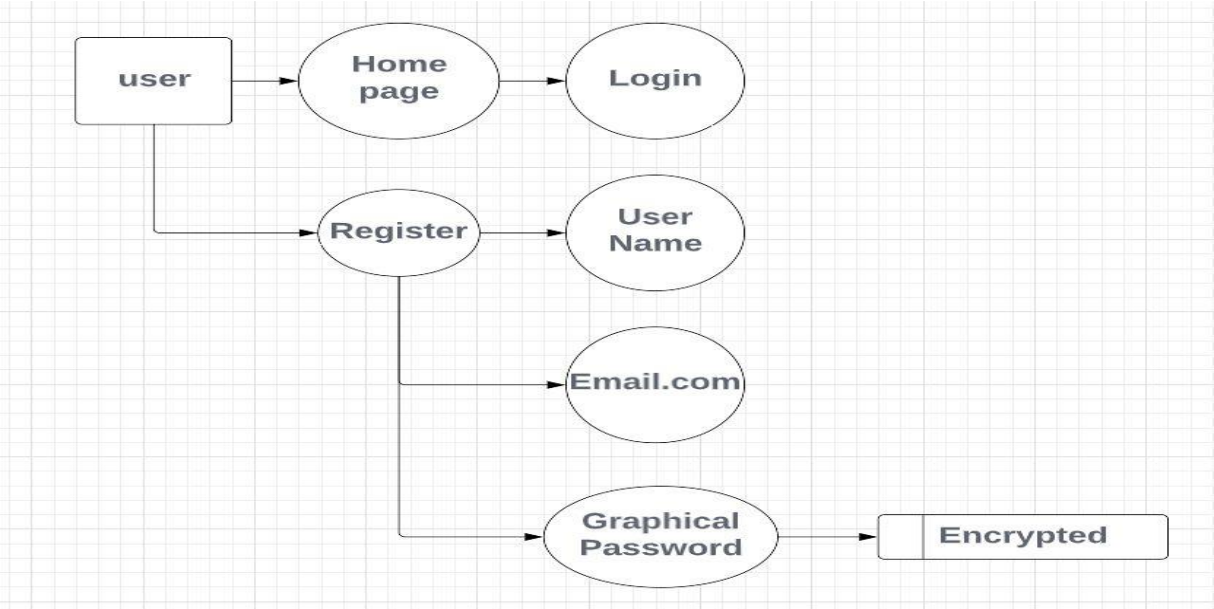
ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

International Conference on Muti-Disciplinary Application & Research Technologies (ICMART-2023)

Geetanjali Institute of Technical Studies

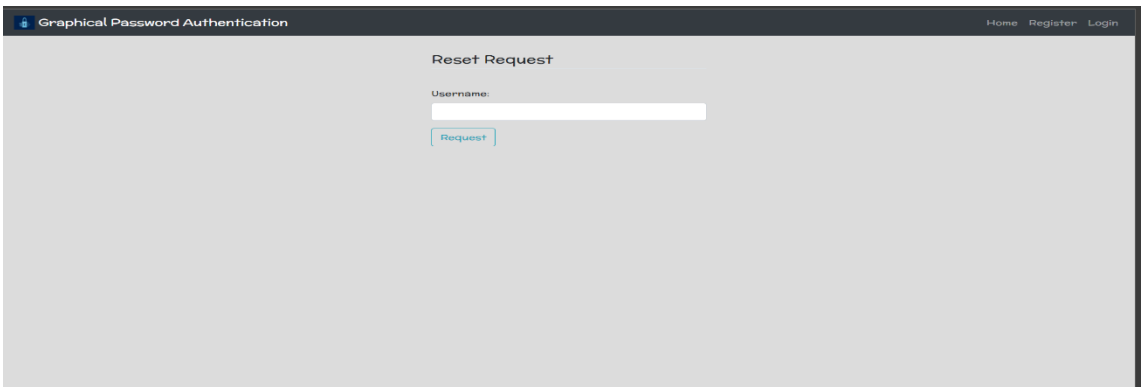
Vol. 10, Special Issue 2, May 2023



V. OUTCOMES AND ADVANTAGES

Home Page: basic user-interface

Forget Password: basic user interface



Home Page:

IARJSET

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

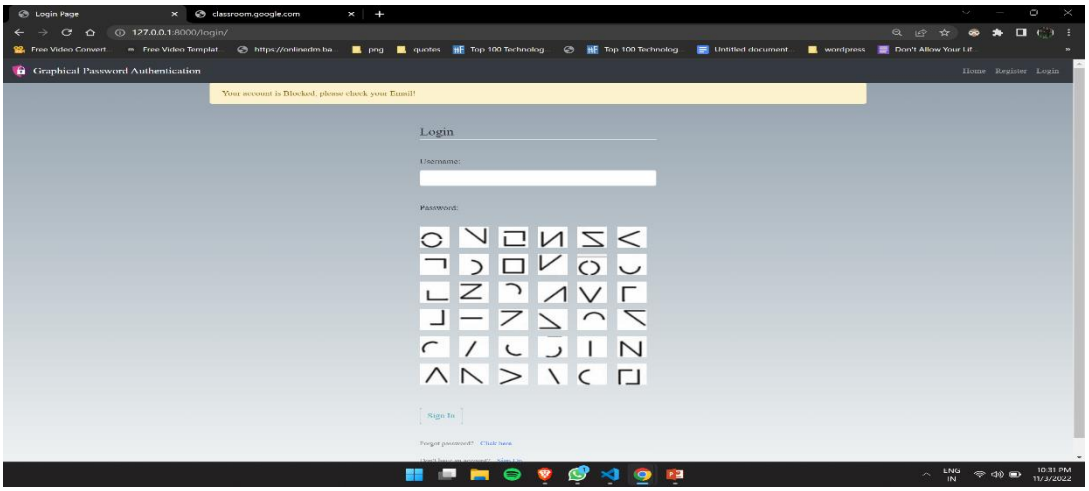
International Advanced Research Journal in Science, Engineering and Technology

International Conference on Muti-Disciplinary Application & Research Technologies (ICMART-2023)

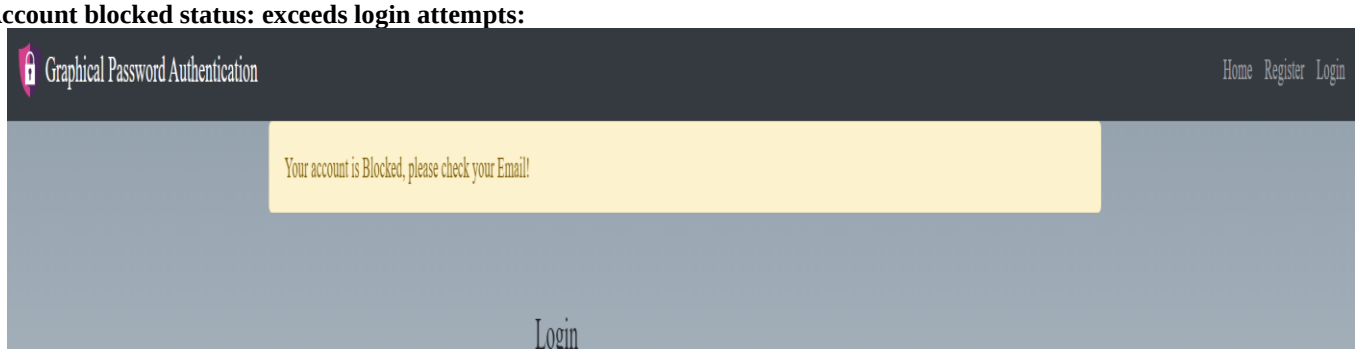
Geetanjali Institute of Technical Studies

Vol. 10, Special Issue 2, May 2023

login:



Account blocked status: exceeds login attempts:



Advantages:

- Graphical passwords schemes provide a way of making more human friendly passwords.
- Here the security of the system is very high.
- Dictionary attacks and brute force search are infeasible.

VI. Conclusion And Future Work

The use of graphical passwords as an alternative to conventional text-based passwords has gained popularity during the past ten years. We have undertaken a thorough analysis of the graphical password approaches that are currently in use in this work. Although the primary benefit of graphical passwords is that they are easier to remember than text-based passwords, there is currently little data to support this claim due to the paucity of user research. According to our preliminary investigation, standard attack techniques like brute force search, dictionary attack, or malware are less effective at cracking graphical passwords. The existing methods for graphical passwords are still in their infancy. Graphical password approaches require a lot more development and user studies to reach greater levels of maturity and use.

An alternative to text-based alphanumeric passwords is a picture password. The majority of the current authentication systems have certain flaws. For this reason, graphical passwords are the most popular type of user authentication that involves clicking on images. While passwords are generated using authentication methods, they are still vulnerable to attacks like dictionary attacks, brute force attacks, and shoulder surfing.

Supporting users in choosing a stronger password is a key usability objective of an authentication system. Strong system given passwords are challenging to remember, but user-created memorable passwords are simple for an attacker to guess. So, researchers in the current era have investigated several alternative techniques and come to the conclusion that graphical passwords are the most preferred authentication scheme. One can increase security by using hashing and encryption algorithms to save and retrieve images and points. The suggested method combines the already used cued click point technique with a persuading feature to influence user choice, urging user to select more arbitrary click points that are challenging to estimate. Further research is needed in this area because picture passwords are still in their infancy.

VII. REFERENCES

[1] G. Eason, B. Noble, and I. N. Sneddon, “On certain integrals of Lipschitz-Hankel type involving products of Bessel functions,” Phil. Trans. Roy. Soc. London, vol. A247, pp. 529–551, April 1955. (references)

[2] J. Clerk Maxwell, A Treatise on Electricity and Magnetism, 3rd ed., vol. 2. Oxford: Clarendon, 1892, pp.68–73.

[3] I. S. Jacobs and C. P. Bean, “Fine particles, thin films and exchange anisotropy,” in Magnetism, vol. III, G. T. Rado and H. Suhl, Eds. New York: Academic, 1963, pp. 271–350.

[4] Patel, Mayank, and Ruksar Sheikh. (2019). "Handwritten Digit Recognition Using Different Dimensionality Reduction Techniques." International Journal of Recent Technology and Engineering 8(2) pp. 999-1002.

[5] R. Nicole, “Title of paper with only first word capitalized,” J. Name Stand. Abbrev., in press.

[6] Patel, M., Choudhary, N. (2017). Designing an Enhanced Simulation Module for Multimedia Transmission Over Wireless Standards. In: Modi, N., Verma, P., Trivedi, B. (eds) Proceedings of International Conference on Communication and Networks. Advances in Intelligent Systems and Computing, vol 508. Springer, Singapore. https://doi.org/10.1007/978-981-10-2750-5_17

[7] Shekhawat, V.S., Tiwari, M., Patel, M. (2021). A Secured Steganography Algorithm for Hiding an Image and Data in an Image Using LSB Technique. In: Singh, V., Asari, V.K., Kumar, S., Patel, R.B. (eds) Computational Methods and Data Engineering. Advances in Intelligent Systems and Computing, vol 1257. Springer, Singapore. https://doi.org/10.1007/978-981-15-7907-3_35

[8] Y. Yorozu, M. Hirano, K. Oka, and Y. Tagawa, “Electron spectroscopy studies on magneto-optical media and plastic substrate interface,” IEEE Transl. J. Magn. Japan, vol. 2, pp. 740–741, August 1987 [Digests 9th Annual Conf. Magnetics Japan, p. 301, 1982].

[9] M. Young, The Technical Writer’s Handbook. Mill Valley, CA: University Science, 1989.