Graphical Password Authentication System

Mr. Harisha
Dept. of Computer Science & Engineering
Sahyadri College of Engineering & Management
Mangalore, Karnataka, India
harisha.cs@sahyadri.edu.in

Ms. Sandhya Ramesh Naik
Dept. of Computer Science & Engineering
Sahyadri College of Engineering & Management
Mangalore, Karnataka, India
sandhyarameshnaik12@gmail.com

Ms. Shettigar Sarvani Vasudeva
Dept. of Computer Science & Engineering
Sahyadri College of Engineering & Management
Mangalore, Karnataka, India
sarvani.v.s@gmail.com

Ms. Shrilakshmi K
Dept. of Computer Science & Engineering
Sahyadri College of Engineering & Management
Mangalore, Karnataka, India
shrilakshmi1810@gmail.com

Ms. Vaishnavi Kothwal
Dept. of Computer Science & Engineering
Sahyadri College of Engineering & Management
Mangalore, Karnataka, India
vaishnavikothwal2@gmail.com

***Abstract*—Text-based password authentication is a common method used to verify the identity of users who are trying to access a secure system or service. In order to use this authentication method, the user must input a password or other secret phrase that is then compared to a server-side copy of the same password. Access is given if the password typed matches the one saved. Graphical password authentication is a type of user authentication that involves using images or visual elements instead of alphanumeric characters to verify the identity of the user. Unlike traditional text-based passwords, graphical passwords offer an intuitive and user-friendly way of authentication, as they rely on the user's ability to remember pictures, shapes, and patterns. This technology has been developed to address the limitations of traditional text-based passwords, such as the difficulty of creating and remembering complex passwords, and the vulnerability to brute-force attacks. Compared to conventional text-based passwords, graphical password authentication has a number of benefits, including better usability and higher security.**

***Index Terms*—Authentication, security, graphical passwords**

I. Introduction

In this generation of information technology, the most growing part is the data itself. On a daily basis, trillions of bytes are exchanged as messages, resources, and assets, and they are stored in the form of information. The most widely used strategy for making it secure is by assigning it a password. There are many other kinds of passwords, but alphanumeric passwords are the most popular because there are more than a trillion possible combinations. In order to make our passwords easier to remember, we typically employ some sort of personal relevance. It creates yet another risk of personal information being leaked through our password in the event that it is compromised or stolen. We frequently use merely numbers as our passwords or PINs, which makes it simple for someone who has been in contact with us for a while to guess them. The use of brief, meaningful passwords has both advantages and disadvantages; on the one hand, they are simple to remember, but on the other, they are simple to guess. The use of "graphics as a password" has proven to be one effective strategy to date in overcoming these issues. Graphical passwords are no different from alphanumeric passwords, and merely uses pixels or patterns as input instead of characters and numbers. Using your own fingerprints, retina, face, or other uniquely identifiable features as your password is a further option that has been very popular in recent years. Although biometrics has gained considerable popularity over the years, one drawback is that installing devices is very expensive. A retina scanner has the same issue as well. Since people tend to use short, simple passwords that are easy to remember and use frequently, graphic passwords have given users an option to get around the challenge of remembering alphanumeric passwords as well as reduce the risk of password theft. People frequently use the same password for multiple accounts at the same time, making it very dangerous. In front of a sea of random images, it is frequently simple to recall and recognise images, patterns, or any other graphical passkeys. Another benefit of utilising graphical passwords is that they eliminate the issue of personal information leaking that has traditionally plagued text-based passwords.

The purpose of this Project is to implement Picture Password Scheme for user authentication. This is to provide an alternative to traditional text-based passwords that can be difficult to remember, easy to guess, or susceptible to brute-force attacks. A general graphical password system uses images, shapes, colors, or other visual elements as the basis for creating a password, which can make it easier to remember, and harder for attackers to guess or crack.

The main scope of developing the Graphical Password Authentication system is to enhance security, improve user satisfaction, and provide a user-friendly authentication technique that is less vulnerable to attacks.

II. LITERATURE SURVEY

The literature survey helps in understanding the existing research done on the Graphical Password Authentication System.

In [1], P.C. Golar *et al.* proposed that Every authentication technique starts out with requesting approval of a secure system that is straightforward, adaptable, and simple to use. One of the authentication methods that has secure password memory as its cornerstone is graphical knowledge-based authentication. The focus of this study is on the recall type authentication system, which is one of its two types—the other being recognition-based. The primary goal of the research project is to evaluate the usability of the available recall knowledge-based authentication methods. On the basis of the information and conclusions from the current system, the steps of the proposed authentication procedure are to be created. The next stage is to choose the criteria for evaluating usability in light of the specified authentication procedure.

In [2], J.A. Jaffar *et al.* One of the various authentication techniques used is alphanumeric usernames and passwords. Due to the method's well-known shortcomings and because of how quickly and effectively humans can retain visual information, graphics-based passwords have been proposed as a replacement. In-depth analysis of graphical password systems is conducted in this study, and each system is evaluated in terms of its usability and resilience to attacks.

In [3], J.G. Kaka *et al.* stressed that User authentication must be a part of information security. Alphanumeric passwords are the most popular and commonly used user authentication technique. However, Alphanumeric forms of identification have a number of disadvantages. Users often choose easy-to-guess passwords (such their names, dates of birth, or licence plate numbers) in order to remember them because complicated passwords are more difficult to do so. As a result, graphical passwords were created as an alternative because studies have shown that individuals can recall pictures better than text. This article examines the usability and security issues of 10 recognition-based graphical password algorithms and the systems that employ them. Recommendations for more research are also included in this study.

In [4], W.Z. Khan *et al.* Data must be secured against alleged "nefarious people" in order to remain safe. Text-based, graphical, biometric, pin, and other authentication techniques for security are available. The drawbacks of these are that users usually use easy-to-remember passwords that are therefore easily and smoothly cracked. This study's main focus is on the image password authentication system, a brand-new alternative authentication technique. This technique encourages users to select passwords that are challenging to guess but easy to remember because humans can more easily recall images than text. This study focuses on addressing and overcoming numerous Persuasive Cued Click Points (PCCP) shortcomings in addition to enhancing the system's security. The suggested approach takes five images and extracts a segment from each one. For a successful login, users just need to choose the specified components on each image. Users can therefore be validated without having to enter any characters. To avoid brute force and other bypass techniques, users are only allowed three consecutive unsuccessful tries. The user account will be locked if these tries are not answered correctly, and it can only be unlocked by answering the predetermined security questions.

In [5], Chiasson. S *et al.* proposed this paper. The study suggests Cued Click Points (CCP), a cued-recall graphical password approach, and assess its usability and security. For a series of photos, users click on one point each image. The previous click-point is used to inform the subsequent image. It discusses the findings of a preliminary user study that produced promising outcomes. Performance in terms of speed, accuracy, and error rate was excellent. Users liked CCP to PassPoints because choosing and remembering just one point per image was simpler and because viewing each image brought to mind the location of the matching point.

In [6], Vikas K. Kolekar *et al.* stated that Security breaches are a serious problem while using desktop applications or online services. Old password methods have some downsides, including the potential for password stealing, shoulder-surfing attacks, internet password guessing attacks, and relay attacks. Therefore, there needs to be a system that offers an effective defence against password cracking assaults. There are numerous methods for it as well as numerous password schemes that can be used to accomplish this. In this research, it suggests an authentication method that uses a captcha challenge image that is based on a graphical password. It includes graphical password schemes as well as captchas.

In [7], Khetani. v *et al.* stated that, Most modern Internet applications still employ classic text-based passwords to achieve user authentication. Security researchers have long sought to create password-based systems that are both safe

and simple to use. On the one hand, there are password management applications that make it possible to generate site-specific strong passwords from a single user password in order to reduce the memory load caused by having many passwords. Studies are being done to see whether graphical passwords are a viable option that is both more secure and user-friendly. In this research, it suggests a brand-new graphical password scheme named "Secure Web Account Access by Recognition Based Graphical Password by Watermarking" for gaining access to online accounts. Here, the user chooses how many images will serve as their password. To log in, they must input the random code that is created beneath each image. Here, the system's security is highly good and each time a user logs in, a new set of codes must be entered for authentication, making dictionary attacks, brute force attacks, and other attacks impossible.

In [8], Prathyusha Reddy Thumma *et al.* stated that Passwords for common texts and photos are frequently used in computer and mobile applications. This generic, handy password is insufficient for maintaining data privacy and computer security. Typically, this strategy leads to shoulder surfing. Applications can be accessed from a local host to remote servers at any time and from any location. These generic passwords are vulnerable to intrusion by atypical users and can expose personal information. We suggest a pass-matrix-based authentication mechanism to solve this issue. A n*n matrix that includes alpha-numeric combinations is constructed using the user's provided login information. Alpha-numeric grid generation with time-based updates. The attacker has no idea how to get the original password due to the grid generation's pattern-oriented selection and time-changing event. It has been demonstrated that the prototype can withstand shoulder surfing more effectively.

In [9], Shikhar Singh Patel *et al.* mentioned that Any system can employ authentication to determine whether a user is legitimate or not. At the moment, one of the biggest problems with information technology is user authentication. Alphanumeric passwords are incredibly difficult to remember. Most frequently, the user will select a brief and simple password, which weakens the password. According to psychological research, learning visuals is simpler than learning letters and numbers. This is one of the primary causes behind the rise in popularity of graphical passwords. In this study, a solution that offers a more secure authentication system that is nearly impervious to shoulder attacks, covert cameras, and spyware attacks is suggested. The advantages and limitations of graphical password authentication with different techniques are discussed in this review paper. A roadmap is also provided in this survey for the future enhancement of various graphical authentication schemes.

In [10], S. Arun Kumar *et al.* The most well-known authentication techniques for security are credentials, OTP, LTP, etc., but these techniques are more vulnerable to brute-force attacks, shoulder surfing attacks, and dictionary attacks. A shoulder surfing attack (SSA) is a method of data theft used to peek over the user's shoulder or utilise external recording and video-capturing devices to gain their personal identifying numbers or passwords. Since SSA happens in a benign manner, it frequently goes unreported. One of the simplest and easiest ways for hackers to steal someone's private information is through this method. Without much effort, the hacker just needs to sneak a glance while the user writes the password. As a result, the majority of people around the world are unaware of this phenomenon. Text-based passwords are widely used in the modern world. Applications for the web and mobile devices require strong passwords containing at least one capital letter and one special letter. People frequently use easy-to-remember passwords that are vulnerable to shoulder surfing. In order to get around this, more secure passwords are provided using graphical password approaches. Users click on target images from a challenge set in the graphical authentication system to authenticate themselves. In comparison to existing authentication methods, a number of graphical solutions have been presented over the years and have shown to be more secure. This document provides a summary of various graphical authentication solutions.

III. PROBLEM STATEMENT

To build a Graphical Password Authentication System to provide a more secure and user-friendly alternative to traditional text-based passwords. Alphanumeric passwords are the most popular type of password out of all the numerous types or forms. In order to make our passwords easier to remember, we typically employ some sort of personal relevance. It creates even another risk of personal information being leaked through our password in the event that it is compromised or stolen. We frequently use merely numbers as our passwords or PINs, which makes it simple for someone who has been in contact with us for a while to guess them. The use of brief, meaningful passwords have both advantages and disadvantages; on the one hand, they are simple to remember, but on the other, they are simple to guess. For easier recall and frequent usage, people typically choose short, easy passwords. People frequently use the same password for multiple accounts at once, making all but one of them dangerous.

IV. OBJECTIVES

- The primary objective of building a Graphical Password Authentication system is to provide a more secure and user-friendly alternative to traditional text-based passwords.
- Graphical passwords are designed to be more resistant to attacks such as brute force and dictionary attacks, as they require users to remember a sequence of images or symbols instead of a string of characters.

- Another objective of building a Graphical Password Authentication system is to increase user satisfaction and ease of use. Graphical passwords can be easier to remember and quicker to enter than traditional text-based passwords, especially for users who struggle to remember complex passwords.
- Additionally, graphical passwords can provide a more personalized and engaging experience, as users can choose images or symbols that are meaningful to them.
- Overall, the main objectives of building a Graphical Password Authentication system are to enhance security, improve user satisfaction, and provide a user-friendly authentication method that is less susceptible to attacks.

V. Methodology

In our suggested method, if a person does not already have an account, they must first register. After registration the user will be prompted to login page. If the user is already an existing user then he/she can directly login.

During the registration process, the user needs to provide a unique username and their email id. Then the user needs to select a theme by searching a keyword in the search space provided. The search results in images related to the keyword which are displayed in a 4*4 grid. The user must select an image from the grid, then the grid is refreshed and new images of the same theme are displayed again. This occurs 4 times in a row. This results in the selection of four images which is taken as the graphical password. User must remember the order in which the images are selected. The flowchart of the process is as shown in figure below.

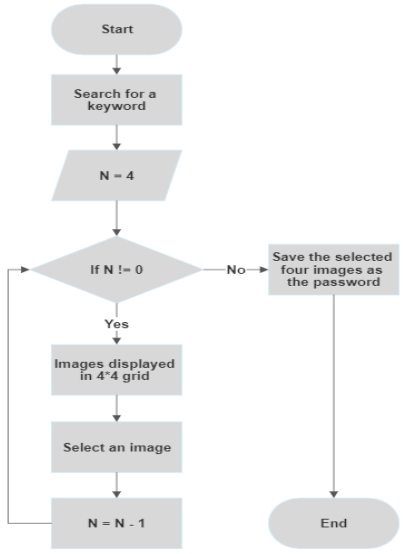

Fig. 1. Flow chart of Registration process

A. Algorithms

Following are the two algorithms that explain the registration and login process of the proposed system.

Algorithm 1: Graphical Password Authentication : Registration Process

Input: $userName$, $email$
$N \leftarrow 4$
$pattern$
if $userName$ *and* $email$ *are valid* **then**
  search $keyword$
  while $N \neq 0$ **do**
    display 16 images related to keyword in 4*4 grid
    select an image i
    $pattern$.append(i)
    $N \leftarrow N - 1$
  end while
  save $userName$, $email$ and $pattern$ in database
else
  show("Invalid username or email")
end if

Algorithm 2: Graphical Password Authentication : Login Process

Input: $userName$, $email$
$N \leftarrow 4$
$new\_pattern$
Enter $userName$
if $userName$ *exists* **then**
  while $N \neq 0$ **do**
    display 16 images related to keyword in 4*4 grid
    select an image i
    $new\_pattern$.append(i)
    $N \leftarrow N - 1$
  end while
  if $new\_pattern$ == $pattern$ *given by the user during registration* **then**
    Grant access to the account
  else
    show("Invalid credentials")
  end if
else
  show("User does not exists")
end if

B. Password Strength

$$No.\ of\ Rounds\ =\ n$$

$$Images\ per\ round\ =\ m$$

$$Complexity\ =\ n\ *\ {}^{m}P_1\ *\ {}^{m}P_1\ *\ {}^{m}P_1\ *\ {}^{m}P_1$$

For our proposed system,

$$No.\ of\ Rounds\ =\ 4$$

$$Images\ per\ round\ =\ 16$$

$$Complexity\ =\ 4\ *\ {}^{16}P_1\ *\ {}^{16}P_1\ *\ {}^{16}P_1\ *\ {}^{16}P_1$$

Hence,

$$Strength\ =\ 262144$$

$$Order\ =\ 10^6$$

VI. Results and Discussion

This approach can be more secure than traditional text-based passwords. Brute force attacks that rely on guessing passwords by trying different combinations of characters are less effective with graphical passwords, which require users to remember a specific sequence of images. Additionally, by using a theme-related search for images, it can be more challenging for attackers to guess which images the user selected. This approach can be more user-friendly and memorable. Users may find it easier to remember a sequence of images than a complex password with a mix of characters, numbers, and symbols. Moreover, by allowing the user to choose a theme and search for images that are meaningful to them, the graphical password can be more personalized, which can improve the user experience. This approach provides a more engaging and interactive user experience during the registration process. Users can enjoy searching for images that match their interests and preferences, which can make the registration process more fun and enjoyable. This can lead to a more positive perception of the authentication process and the overall security of the system. In summary, the advantages of using this system include enhanced security, improved user experience, and increased engagement during the registration process.

A. System Testing

For our proposed system, 25 volunteers performed trials. In the first week, they were asked to create their own account using both alphanumeric and graphical passwords. The volunteers were asked not to set an alphanumeric password which has any kind of personal reference. Then in the following week, the volunteers had to try to log in to their accounts. The observations and feedback obtained are given in the following tables.

No. of Successful Log in	No. of Unsuccessful Log in	Total no. of Log in
14	11	25

TABLE I
Observation on Alphanumeric password entered by volunteers during login in the 2nd week

No. of Successful Log in	No. of Unsuccessful Log in	Total no. of Log in
23	2	25

TABLE II
Observation on Graphical password entered by volunteers during login in the 2nd week

Volunteer	Time taken to enter Alphanumeric password (in sec)	Time taken to enter Graphical password (in sec)
1	30	13
2	35	15
3	40	22
4	28	14
5	25	13
6	30	25
7	32	18
8	39	16
9	35	23
10	27	25

TABLE III
Time taken(in seconds) by 10 of the volunteers to enter the passwords

Avg. Time taken to enter Alphanumeric password (in sec)	Avg. Time taken to enter Graphical password (in sec)
27	18

TABLE IV
Average Time taken(in seconds) by 25 volunteers to enter the passwords

We found that our volunteers hold positive views in general. Most of our volunteers think that the login success rate of this scheme is acceptable, and it is not hard to use it.

Index	Statement provided	Average Score (out of 5)
1	I would like to use this scheme	4.3
2	I think scheme is very annoying	1.8
3	I think this scheme is hard to use	2.1
4	I think this scheme can be used widely	4.5

TABLE V
Feedback from the Volunteers

VII. Conclusion and Future Scope

The proposed approach can be more secure than traditional text-based passwords. Brute force attacks that rely on guessing passwords by trying different combinations of characters are less effective with graphical passwords, which require users to remember a specific sequence of images. Additionally, by using a theme-related search for images, it can be more challenging for attackers to guess which images the user selected. This approach can be more user-friendly and memorable. Users may find it easier to remember a sequence of images than a complex password with a mix of characters, numbers, and symbols. Moreover, by allowing the user to choose a theme and search for images that are meaningful to them, the graphical password can be more personalized, which can improve the user experience. This approach provides a

more engaging and interactive user experience during the registration process. Users can enjoy searching for images that match their interests and preferences, which can make the registration process more fun and enjoyable. This can lead to a more positive perception of the authentication process and the overall security of the system. In summary, the advantages of using this system include enhanced security, improved user experience, and increased engagement during the registration process. In the future, we want to conduct a survey among the novice users to find the reliability of the graphical password authentication when compared to other existing password authentication systems. We also want to develop a mobile application with graphical password authentication security, with mechanisms to capture the attacker's face.

In future, Should conduct a survey among the novice users to find the reliability of the graphical password authentication when compared to other existing password authentication systems. Developing a mobile application(Android, iOS) with graphical password authentication security. Developing mechanisms to capture the attacker's face in mobile application system.

REFERENCES

[1] P. C. Golar and B. Khandelwal, "Study of Usability Parameter for Graphical Based Authentication System," 2020 9th International Conference System Modeling and Advancement in Research Trends (SMART), Moradabad, India, 2020, pp. 23-26, doi: 10.1109/SMART50582.2020.9337116.

[2] J. A. Jaffar and A. M. Zeki, "Evaluation of Graphical Password Schemes in Terms of Attack Resistance and Usability," 2020 International Conference on Innovation and Intelligence for Informatics, Computing and Technologies (3ICT), Sakheer, Bahrain, 2020, pp. 1-5, doi: 10.1109/3ICT51146.2020.9312011.

[3] J. G. Kaka, O. O. Ishaq and J. O. Ojeniyi, "Recognition-Based Graphical Password Algorithms: A Survey," 2020 IEEE 2nd International Conference on Cyberspac (CYBER NIGERIA), Abuja, Nigeria, 2021, pp. 44-51, doi: 10.1109/CYBERNIGERIA51635.2021.9428801.

[4] W. Z. Khan, Mohammed Y Aalsalem and Yang Xiang, "A Graphical Password Based System for Small-Mobile Devices", IJCSI International Journal of Computer Science Issues, 2011, doi: https://doi.org/10.48550/arXiv.1110.3844

[5] Chiasson, S., van Oorschot, P.C., Biddle, R. (2007). Graphical Password Authentication Using Cued Click Points. In: Biskup, J., López, J. (eds) Computer Security – ESORICS 2007. ESORICS 2007. Lecture Notes in Computer Science, vol 4734. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-540-74835-9-24

[6] Vikas K. Kolekar and Milindkumar B. Vaidya, "Shuffled Input Graphical Password Authentication Schemes Built on Captcha Technology", IJIERT, ICITDCEME'15 Conference Proceedings

[7] Khetani, Vinit, Jennifer Nicholas, Anuja Bongirwar and A. S. Yeole. "Securing Web Accounts Using Graphical Password Authentication through Watermarking." International Journal of Computer Trends and Technology 9 (2014): 269-274.

[8] Prathyusha Reddy Thumma, (2020). "Password Authentication using Pass Matrix to Avoid Shoulder Surfing.", IRJET International Research Journal of Engineering and Technology, 2020

[9] Patel, Shikhar & Jaiswal, Akarsh & Arora, Yash & Sharma, Bharti. (2021). Survey on Graphical Password Authentication System. 10.1007/978-981-15-8530-2-55.

[10] Kumar, S. & Ramya, R. & Rashika, R. & Duggal, Renu. (2021). A Survey on Graphical Authentication System Resisting Shoulder Surfing Attack. 10.1007/978-981-15-3514-7-57.