International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 10 Issue: 03 | Mar 2023 www.irjet.net p-ISSN: 2395-0072

Graphical Password Authentication

Meher Gulhane, Amey Andurekar, Vaidehi Kute, Achal Maldhure, Sharwari Kale

Department of Computer Science Engineering, Sipna College of Engineering & Technology Amravati, Maharashtra, India
Professor A.V. Pande Department of Computer Science Engineering, Sipna College of Engineering & Technology Amravati, Maharashtra, India

---

Abstract - *Graphical password is one of technic for authentication of computer security. Nowadays digital/computer security is the most important thing in computer science for protecting user or customer data. And Shoulder-surfing is one of the threats where a criminal can steal a password by direct observation or by recording the authentication session. There are several techniques available for this authentication, the most prevalent and simple of which is the Graphical password technique. So, we suggest a new approach to combat this problem. We have developed two concepts to combat shoulder surfing attacks. First, the user must register if the registration does not exist. Second, you must log in with a valid user ID and password. The password is a grouping of characters and numbers. Third, the user has to cross image-based authentication where the user can choose their password and this method has higher chances to offset each other. You should choose a password according to the registration password, it must match at login time. In color base authentication, there should be several color base passwords, and depending on the color, you need to remember the password sequence. And it's like three-factor authentication. So, here is proposed a new graphical password authentication technique that is resilient to shoulder surfing and also to other types of probable attacks.*

Keywords: Graphical password, Authentication, Security, Text-based password, Recognition, Pictures

1. INTRODUCTION

Authentication is the process of determining that the person requesting a resource is the one who it claims to be. Most authentication system nowadays uses an integration of username and password . The problem with the password is that it requires the user to remember it and it should be kept secret. Each authentication system has its own guidelines and limitations like password length, password must contain alphanumeric and special characters. These passwords are mostly text-based passwords. Either user use passwords that are easy to remember like license plate numbers, parent names, phone numbers sometimes their own name which is very much predictable, or complex passwords that they overlook so they might be using the same password for different accounts or jot down their password somewhere. Moreover, the user is vulnerable to various attacks. Text-based passwords face security and usability matters.

To overcome these shortcomings of alphanumeric passwords, graphical password schemes have been proposed. In a graphical password authentication application by using the 6 passports scheme a password contains an image where the user can input the password with the help of mouse events like click and drag. Picture Superiority Effect Theory reveals that pictures can be recognized and recalled easily by the human brain, enhancing the ability to Strong passwords can be invented which are resistant to guessing, dictionary attack, and social engineering.

1.1 Problem Statement

An alphanumeric password is an old traditional common authentication method. Practically this traditional method is a too insecure system. For example, an attacker may choose an easily guessed user's password, if a user is not using a strong password. Users may use the same password for multiple devices or sites. These are all insecure characteristics for normal users. And authentication is one of the important security points where the user has active responsibility for their personal information security. If we use the old traditional password system then there may have the possibility of to dictionary attack, Brute Force Attack.

1.2 Objective

i. To design a Graphical Password Authentication implemented in the mobile application.

ii. To implement the Graphical Password Authentication application using the PassPoint technique

2. LITERATURE REVIEW

[1] In Dec 2021 author H. Gao proposed a graphical password scheme using color login. In this color, login uses a background color which decreases login time. The possibility of accidental login is high and the password is too short. The system developed by Sobrado is improved by combining text with images or colors to generate session passwords for authentication. Session passwords can be used only once and every time a new

password is generated. The advantages of this system are that it reduces the login time, and session passwords are also generated to improve security. The disadvantage of this system is that the possibility of accidental login is high and the password is too short.

[2] In this paper, M. Sreelatha proposed Hybrid Textual Authentication Scheme. This scheme uses colors and the user has to rate the colors in the registration phase. During the login phase, four pairs of colors and an 8*8 matrix will be displayed. As the color rating is given by the user, the password will generate. The first color shows the row number and the second shows the column number of the grid. The drawback of this system is intersecting element is the first letter of the password. The user has to memorize the rating and order of the colors. So it becomes very hectic for the user. The benefit of this system is that it is flexible and simple to use.

[3] A hybrid graphical password-based method is advised, which is a mixture of recognition and recall-based methods and has many advantages as compared to existing systems and is more suitable for the user. In this system, the user draws the selected object which is then stored in the database with the specified username. Objects may be symbols, characters, auto shapes, simple daily-seen objects, etc. Then the user draws pre-selected objects as his password on a touch-sensitive screen with a mouse. Then the system performs preprocessing. Then after stroke merging, the system constructs the hierarchy then the next step is sketch simplification, then the three types of features are extracted from the sketch drawn by the user. The last step is called hierarchical matching. The plus point of this system is it's a combination of recognition and recall-based techniques, hence providing flexibility. This system performs some complex actions like pre-processing and stroke merging. So it can be a weakness of this system.

[4] The authors proposed a system in which a password scheme uses colors and text for generating session passwords. They have introduced a session password scheme in which the passwords are used only once for each session and when the session is completed the password is no longer in use. In this system, two session password schemes pair-based textual authentication scheme and a color code-based authentication scheme are introduced In the pair-based textual authentication scheme the user submits his password during the registration. The password should contain a number of characters. When the user enters login an interface containing a grid is shown during the login phase. The grid is of size 6 x 6 and it contains alphabets and numbers. These are randomly placed on the grid and the interface changes every time. Depending upon the password which is submitted during the registration phase, the user has to enter the password. Users have to consider their password in terms of pairs. In the color code-based scheme, the user has to get his password with the help of colors. During the registration phase, the user should fill up all his information and also rate colors. The merit of this system is it provides much better security. The Demerit of the system is sometimes users may consider wrong password as they are supposed to consider the password in terms of pair .

[5] In Graphical password as an OTP proposed by authors, she used the scheme of OTP. As there are many drawbacks of using alphanumerical passwords, people tend to forget the password, or they may write the password somewhere. Hence they have developed authentication methods that use pictures as passwords known as a graphical passwords to solve this problem. They have provided an additional layer of security by generating a one-time password(OTP) which is sent to the user's mobile. Using the instant messaging service available on the internet, the user will obtain the One Time Password (OTP). The OTP will be the information on the items present in the image to be clicked by the user. The users will authenticate themselves by clicking on various items in the image based on the information sent to them. The main aim of this system is to avoid Shoulder surfing attacks. It also aims to avoid other attacks like a dictionary attacks, brute force attack and guessing attack. The OTP is sent to the user's mobile number from the database. The positive point of this system is it provides better security as it avoids shoulder surfing by using OTP. The negative point of this system is users must click within the tolerance of their chosen pixels and also in the correct sequence.

[6] The authors proposed four systems that mainly focuses on graphical password. The textual-based password system is a popular authentication system since ancient times. It has many advantages but at the same time, it has a few drawbacks too. Hence, the current graphical password techniques is classified into four techniques recognition-based, pure recall-based, cued-recall based and hybrid based. [A]In the recognition-based algorithm the user must memorize the portfolio of images during password creation. When the user logs in, the user must recognize the images from the decoys. Various images like faces, icons, everyday objects, random art, etc. can be used. In the pure recall-based system the user recalls the outline drawing on the grid which they have created or selected during the registration phase. In this system, the user usually draws their password either on the grid or on a blank canvas. The cued recall-based system is similar to the recall system but it is recalled with cueing. In this system, reminders are sent to the user to reproduce the password accurately. The Hybrid system is a combination of two or more password schemes. It is used to overcome the limitation of a single system, such as the hotspot problems. The advantage of this system is it provides a high authentication process as it is categorized in four techniques. The disadvantage of this system is it's a complex and long-term process.

[7] The authors proposed a scheme that mainly focuses on shoulder surfing. In this system, they proposed a new click-based color password scheme called Color Click Points (CCP). It can be viewed as a combination of Pass-Points, Pass faces, and Stories. A password consists of one click-point per Color for a sequence of Colors. The next Color displayed is built on the previous click-point.

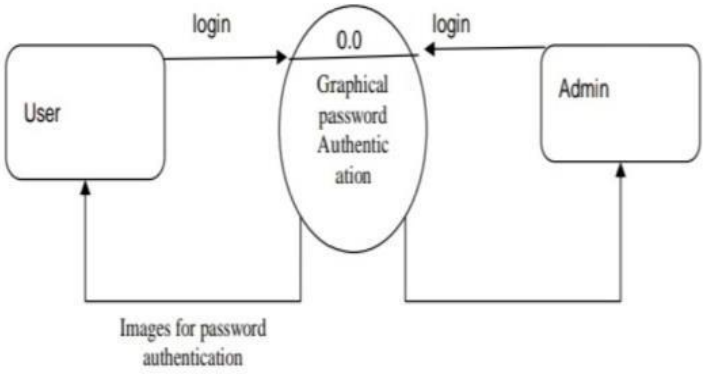
in this proposed scheme, we propose an improved text-based shoulder surfing-resistant graphical password scheme by using colors. In the proposed scheme, the user can easily and efficiently log in system. Afterward, we examine the security and usability of the proposed system and show the resistance of the proposed system to shoulder surfing and accidental login. The benefit of this system is that it reduces the login time & it is an efficient system.

3.Research Methodology

3.1 Proposed System

For reduce most common ways of hacking possibilities related with the text password i.e. Brute force and dictionary attack and Fishing. For more human friendly password. To increasing level of security. Create system which is easy to remember compared with text password. Providing more security. For password which would not be easy to guess. In this project here proposed we are going to use image position with some points. While login images appears in sequence in one by one manner. Click-based graphical password scheme, a cued-recall graphical password technique. Various graphical password schemes have been proposed as alternatives to text-based passwords. It can be used as password for folder lock, web-driven applications, desktop lock etc. In case if user fails to click right point for at least 3 times he will be blocked from login and a login link will be sent on users registered email.

DFD Diagram



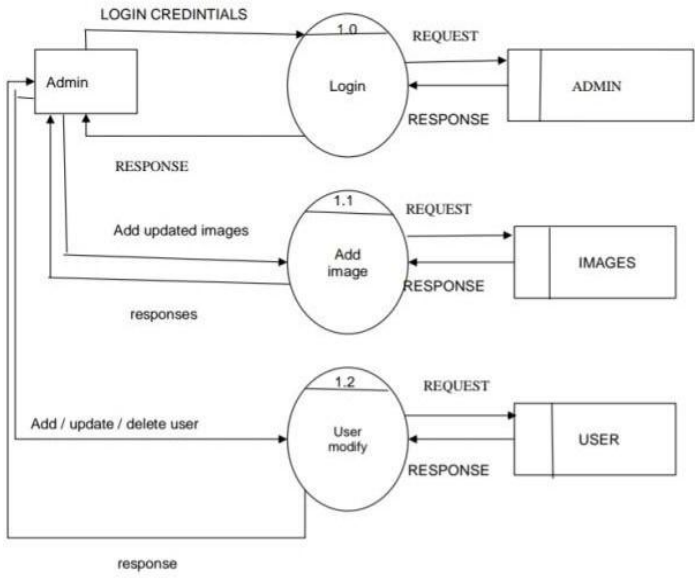


Fig.Flowchart of Login phase

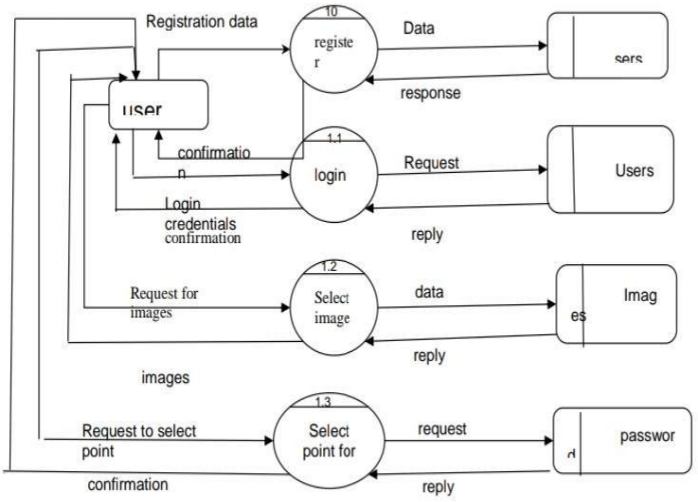


Fig.Flowchart of Graphical Password

4. CONCLUSION

Digital devices are becoming part of our life day by day. By using digital devices, we have able to know about the authentication process. Validation is an integral part of security. Authentication will give the customer greater security. Specific review articles research in the same field about the specific assaults found during validation. Printed hidden-term authentication is an excellent testing device. It is more useful and secure compared to previous old base graphical password authentication systems. Since the password space is very large, it offers security against brute-force attacks. It's easy to use. Passwords can be easily created and recalled. The randomization in both

authentication systems provides strong security against shoulder surfing. To have a good system, you need high security and good usability, and can't be separated them. Shoulder navigation attack is subject to safety precautions. However, the proposed methods for the shoulder surfing problem still need to be improved. This system can also be used to add a higher level of security to the text-based password system. This system is very cheap compared to a biometrics system.

5.REFERENCES

[1] Dec 2020, H. Gao proposed a paper on a "graphical password scheme using color login".

[2] In May 2021, M. Sreelatha proposed Hybrid Textual Authentication Scheme.

[3] Er. Aman Kumar, Er. Naveen Bilandi, Department of Computer Science and Engineering, DAV University, Jalandhar, Punjab, India "Graphical Password-Based Authentication Based System for Mobile Systems".

[4] Miss.Swati Tidke, Miss Nagama Khan, Miss.Swati Balpande Computer Engineering, RTM nagpur university, M.I.E.T Bhandara, "Password Authentication Using Text and Colors".

[5] Veena Rathanavel, Swati Mali, Student M. Tech, Department of Computer Engineering, K J Somaiya, College of Engineering Mumbai, "Graphical Password as an OTP".

[6] Veena Rathanavel, Swati Mali, Student M. Tech, Department of Computer Engineering, K J Somaiya, College of Engineering Mumbai, "Graphical Password as an OTP".

[7] In 2021 Aayush Dilipkumar Jain, Ramkrishna Khetan Krishnakant Dubey, Prof. Harshali Rambade K. Elissa, Department of Information Technology Vidyalankar Institute of Technology, Mumbai, "Color Shuffling Password-Based Authentication".