# PASSCODE DETECTION USING THE COLOR GRID

[1]Y.Sairam,[2]V.Baby
[1]M-Tech student,[2]Associate Professor
[1]Department of Computer Science and Engineering,
[1]VNR Vignana Jyothi Institute of Technology, Hyderabad, India

***Abstract :*** In recent times, data over the internet increased enormously. Authentication is the only technique available and used for accessing data. Cyber attacks are also growing immensely, so security is the primary concern for each person. People are worried about their email passwords, cloud passwords, ATM pins, and different site passwords. Textual passwords are the extensively seen procedure used for verification. However, textual passwords are powerless against modern-day attacks such as shoulder surfing attack, key loggers, spyware attack, and social engineering attack. OTP's, Biometric authentication, draw-a-secret, and Graphical passwords evolved as alternative methods for the Textual Passwords, but OTP's require the secure and reliable network connection mobile, Biometric authentication require separate hardware, draw-a-secret, and most of the graphical password techniques are defenseless to shoulder surfing attack. To overcome these problems here presenting a session password-based method PDGC: Passcode detection using the color grid. In this PDCS technique user needs to analyze and enter session passcode based on actual password with the help of color matrix grid displayed during login.

***IndexTerms - passcode, authentication, graphical password, security, color grid, shoulder surfing.***

## I. INTRODUCTION

With the World Wide Web (www) everything has turned out to be less demanding, wherever we go there are online administrations, there we make accounts by using passwords, to keep up a specific association database. There are such huge numbers of types exists. Some of them are Text Passwords, Pins, Graphical passwords, Biometric passwords, Audio passwords, and face recognition passwords. All these are utilized for verification of the User. Among them text-based passwords are more often used. Text-based passwords are things which generally identify with the user like a telephone number or last or first name. Passwords are regularly blended of case sensitive letters, numbers, and special characters. These are powerless and simple to guess by anybody. Generally, these text passwords are helpless against dictionary attacks. So considering all these, it has been demonstrated that graphical passwords are superior to text passwords. Because pictures and passwords with a blend of colors are easy to remember than text passwords.

The real points of interest in utilizing graphical passwords are,

- They give greater security when contrasted with others.
- They are straightforward and simple to execute.
- Pictures are effectively recollected by the users as opposed to passwords.
- Not only images but also colors will attract user very much and persuade them to use passwords which involve colors.
- Graphical passwords are resilience to Dictionary attacks.

## II. RELATED WORK

Currently large number of graphical password authentication techniques are exist, some of them are based on image selection from the grid[3,8], image segmentation[2], change image technology[4], pair based authentication scheme[5], Image Discretization[11], multiple image selection authentication[6], Hybrid Textual Authentication Scheme[7,5], Cued image click points[10,12], and False Image selection from grid[9]. Most of the methods existing are not resilience to spyware or shoulder surfing attacks.


Fig 1: General familiar authentication types

Though the numerous types of graphical password authentication techniques exist, most common methods using for authentication [7] are Biometric, OTP's, Personal secret pins, Draw a secret pattern and facial recognition systems. Limitations in the Biometric systems are they require additional integration of hardware and once they get compromised then they cannot be reset. Limitations in OTP systems are the unavailability of devices, unavailability of services and delay in delivery of OTP's. shoulder surfing is the real issue with the draw-a-secret algorithm. Limitations in Facial recognition systems are processing time, requires large storage, image quality systems, and surveillance angle should also match.

## III. PROPOSED SYSTEM

By taking into consideration of the downtimes in the existing authentication strategies here presenting a secure session-based graphical password technique PDCS which is easily versatile for Mobile applications and web applications. And this PDCS system is high resilience to shoulder surfing attacks. This passcode detection using the color grid is a cued recall based graphical method where the user needs to generate session password based on hints provided in the color matrix grid.

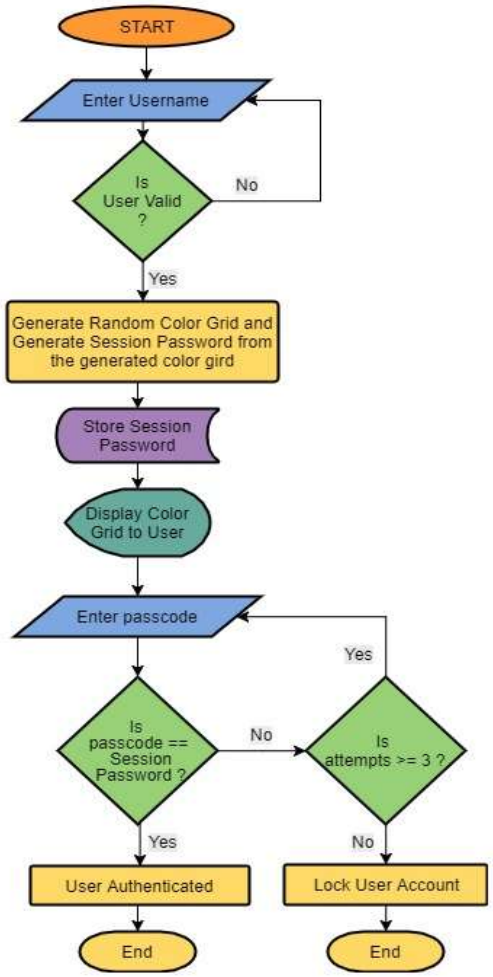


Fig 2: working principle of proposed work

After successful registration of the user with required details such as unique username, password(minimum 8 letters), date of birth, valid email and valid mobile number. User authentication takes places in two steps.


Fig3: User name verification

**1) User-name verification:** The user needs to enter his/her unique user-name in the User ID field and need to click on Next button as displayed in Fig 3. If the user-name entered by the user exists in database then he has redirected to passcode verification page else it shows invalid user-name please enter valid user-name.

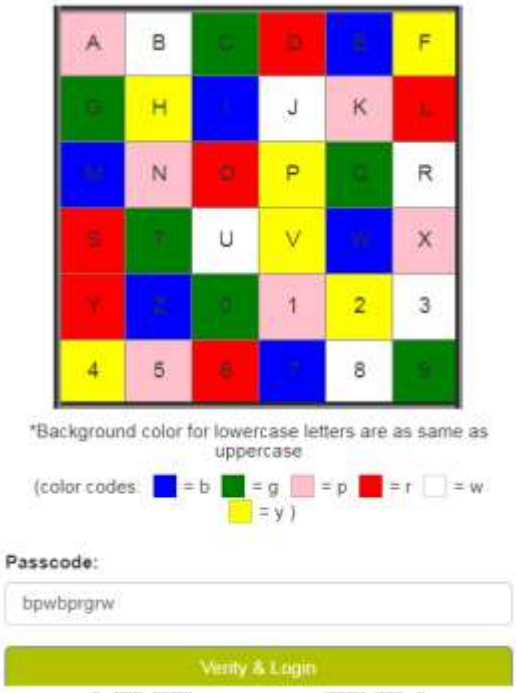


Fig4: Random color Grid1

**2) Passcode verification:** After successful verification of user name a 6*6 square random color grid is displayed to the user. That 6*6 grid contains 26 alphabets and 0-9 numerals. The colors are randomized in the 6*6 squares matrix grid using 6 different colors (y-yellow, p-pink, r-red, w-white, b-Blue, and g-Green) as shown in fig4. The user needs to enter the first letter of the squares of the color in which his password letters lie. For example, let his/her password is 'marias963' then he/she need to type 'bpwbprgrw' (the background color 1st character of each of his password letter) and click on verify & Login. Then validation of the entered passcode and actual password is carried out by conducting a Comparison in the background. If the first letter of the colors of the password entered by the user match with the first letters of the colors of the password in the database the user will be authenticated else he is asked to enter valid passcode again. For providing better security If the user fails to enter correct passcode within 3 attempts then his/her account will be locked, he/she can recover his password by clicking forgot password button.

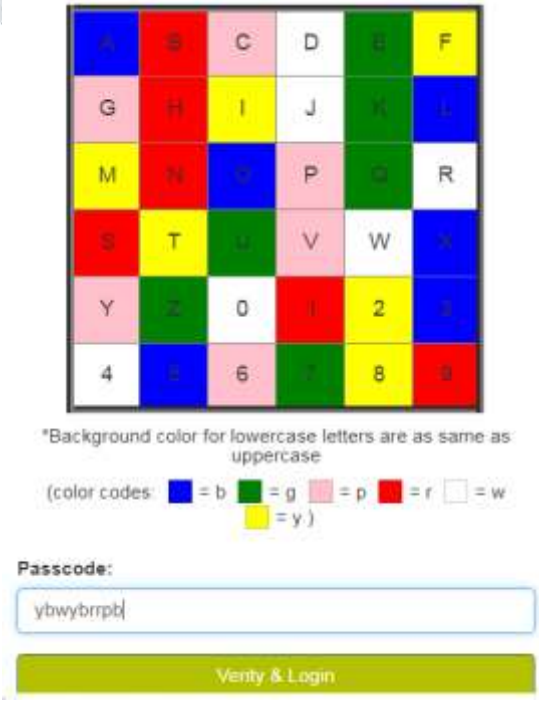


Fig5: Random color Grid2

For each login session, the colors in the 6*6 squares matrix grid are randomized as shown in fig5. But the alphabets and numbers are kept in same place for the convenience of the user. According to Fig5 the passcode for 'maris963' is 'ybwybrrpb', so for each login session, the password is different for the same user and the attacker doesn't know the actual password of the user even if he tries to guess the password using color entered by the user there is similar color behind the six letters in the grid. Generally in the existing session passwords techniques user need separate hardware to get OTP's or session password, but in this PDCG: passcode detection using color grid technique no separate hardware is required for the user to get session password, user himself/herself will identify the session password with the help of random color grid provided during authentication.

## IV.CONCLUSION:

Authentication plays a pivotal role everywhere. But Authentication attacks are growing rampant currently. At this moment a vast number of authentication strategies available. However, every authentication strategy has their own particular focal points and drawbacks. This Passcode Detection using the Color Grid system explains the new Authentication strategy which resembles cued-recall based graphical authentication technique and session-based password technique. This Passcode Detection Using Color Grid technique provides new passcode color grid for every login which is session-based. So this technique is profoundly resilience to modern-day attacks such as shoulder surfing, key loggers, and phishing attacks.

**References:**

[1]. Dhiviyaa, rakshitha, k. Vijayabharathi, "Authentication- Overview Of Graphical passwords", " International research journal of engineering & technology", vol-5, issue-02, feb-2018.

[2]. Rohitkumar kolay, vinaykumar yadav, animesh vora, , "Graphical Password Authentication Using Image Segmentation", "International research journal of engineering and technology", Vol-4, issue-03, mar-2017.

[3]. Aakansha s, s.waghmare gokhalea , vijaya, "The shoulder surfing resistant graphical password authentication technique", "7th international conference on communication, computing and virtualization", feb-2016.

[4]. RoshniRajavat, BhavnaGala, AsmitaRedekar, "Textual and graphical password authentication scheme resistant to shoulder surfing", "International Journal of Computer Applications", vol-114, No-19, mar-2015.

[5]. N.S.Joshi, "Session passwords using grids and colors for web applications and pda", "International journal of emerging technology and advanced engineering" , vol-3, Issue-5, may-2013.

[6]. Awadesh kumar, sonkar s.k, paikrao r.l, , "Graphical password authentication scheme based on color image gallery", "International journal of engineering and innovative technology (ijeit)", vol-2, issue-4, oct-2012.

[7]. Salendra prasad, nilesh a. lal, , mohammed farik, "A review of authentication methods ", "International journal of scientific and technology research", vol-5, issue-11, nov-2016.

[8]. Sukhvinder kaur," Three level authentications using graphical password with pass point scheme", "International journal of advanced research in computer science and software engineering", vol-6, issue-06, jun-2016.

[9]. Rahul jadhav, aditya mishra, shubham patil, "A shoulder-surfing resistant graphical password system ", "International research journal of engineering and technology", vol-5, issue-03, mar-2018.

[10]. Israrul haq, towseef akram , vakeel ahmad, monisa nazir , "Graphical password authentication ", "International journal of computer science and mobile computing", vol-6, issue-06, jun-2017.

[11]. Archana mr, keerthana m.m, "Implementation of graphical authentication system for shoulder surfing attacks ", "International journal of innovative research in computer and communication engineering", vol-6, issue-02, feb-2018.

[12]. samiksha thakur, p.d.thakare, "Graphical-based password keystroke dynamic authentication system", "International research journal of engineering and technology", vol-5, issue-06, feb-2018.