(IJISE) 2018, Vol. No. 7, Jan-Jun **e-ISSN: 2454-6402; p-ISSN: 2454-812X**

DEVELOPING AN INTEGRATED FRAMEWORK FOR ENHANCED SECURITY FEATURES BASED ON COLOUR SELECTION COMBINATION

Saatvik Wadhwa

ABSTRACT

In previous days there was not much utilization of PCs. As improvements occurred in software engineering, every and huge business or even every individual began utilizing PCs. PCs are present in each field and each seemingly insignificant detail. Then, at that point, there comes a piece of the web for offering data to one another. The web is primarily utilized for informal communication, internet advertising, net banking, and online cash exchanges. With this, there comes the more obscure side of the web: web cheats, hackings, breaking, and so on. Whoever is utilizing the web, most importantly, wishes their well-being and security and this is finished by using confirmation. In the vast majority of the cases, the client is given USERNAMES and PASSWORDS for validation. Yet, programmers are presently assaulting validation frameworks for doing web cheats. We need more grounded answers to keep away from assaults that will be conceivable utilizing the "shading code combination forgot login" strategy.

I. INTRODUCTION

In case we are utilizing any web-based media sites or any internet-based exchange frameworks, or any web-based shopping site. Most normally, will tell us to set "username" and "secret phrase" for security reason.

Even after setting up the confirmation as Username-Password, a large portion of the occasions we see that there are numerous un-approved gets to because these Usernames and Passwords are ordinary texts. Furthermore, these text-based passwords can undoubtedly be gotten to or speculated. There is even a wide range of assaults likes: Eves Dropping, Shoulder Surfing and Dictionary Attacks, by which it is a lot conceivable for the assailant to hack or conjecture the secret phrase and gain the entrance for any client.

We can't make our passwords muddled because nowadays we have such countless distinctive web-based media accounts, banking accounts or even web-based shopping accounts; because of every one of these, we will be puzzled if we picked convoluted usernames or passwords. We can't utilize the same username or secret key wherever since supposing that somebody surmises the secret phrase for one record, then there are chances that we might lose every one of the records.

Maybe than utilizing simply basic literary passwords, it is smarter to use some unique strategy that will give us a superior method of setting a password. Password should be muddled to figure, and yet it ought to be not difficult to recollect.

II. OBJECTIVE

Secret word as text is the most widely recognized way utilized in client verification. Notwithstanding, literary passwords are risky against eves dropping, shoulder surfing and word reference assaults. The answer for this is Graphical passwords, which are utilized as an elective method for printed passwords. However, most of the graphical plans are exceptionally confounded and require a few rounds of the check, coming about convenience issues, and it requires some investment for preparing. In this paper, a crossbreed and diverse client confirmation method which joins text and shadings are proposed to produce passwords with further developed security, ease of use and strength.

III. PROPOSED SYSTEM

The first client needs to enrol themself with the framework. In the enrolment measure client will be approached to enter the subtleties as displayed in below Figure.

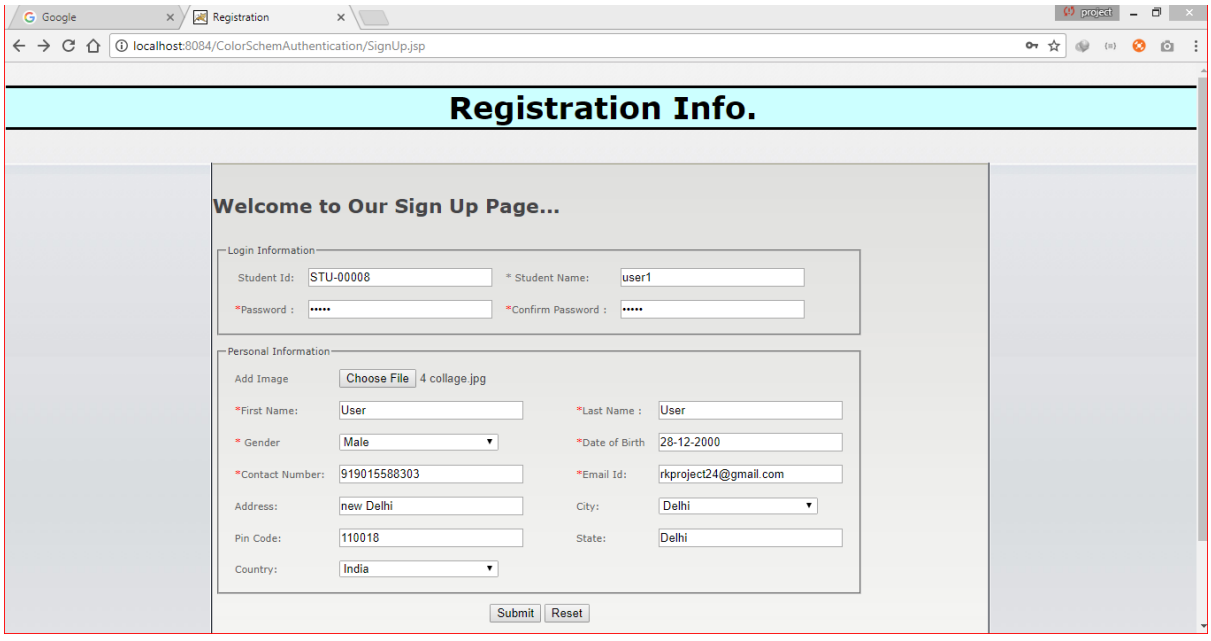

Fig 1: User Signup

In typical frameworks, we choose to choose passwords as text, numbers, or barely any images. Without much of a stretch, these kinds of passwords can be speculated and hacked; in the proposed framework, as we can see above. Figure 1; we can choose a secret phrase which is the blend of shading and codes. During the enlistment stage, the client should top off

all of the data needed in the enrolment structure, choose three distinct tones, and rate them exclusively. The client should rate every one of the tones, particularly from 0 to 9, as a secret phrase. Chosen techniques and their appraisals are put away in the data set. See the accompanying Figure to find out with regards to shading code blend.

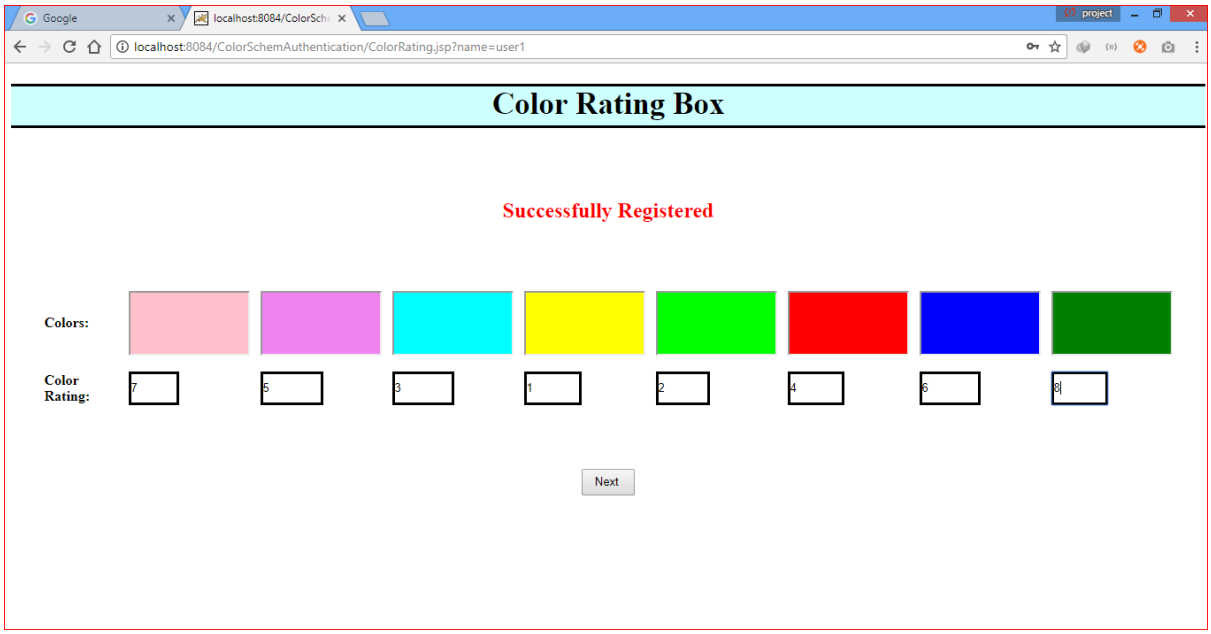

Fig 2: Color Segment

As we can see in the above chart, the client has chosen three distinct shadings: Yellow, Green, and Blue and likewise chose the codes like 5, 4, 3. Presently this shading code blend will be put away as Yellow-5, Green-4, Blue-3. After the client is finished choosing the shading code blend, the client needs to tap on submit to complete the enlistment interaction; if the enrolment is effective, it will show a notification message.

The client needs to enter an enlisted email address during the login stage to proceed with the login cycle. The framework will check from the data set if that client is a current client. The tones chose by the client during the enrollment stage will be shown naturally and haphazardly, and afterwards, the client needs to rate them effectively for a fruitful login. Then, at that point, the client needs to tap on the login button for productive verification. Then, at that point, the framework will check from the information base whether that username and secret key matches or not. Consider the accompanying figures to comprehend the login interaction.

Client Karan enrolled himself with the Email helloworld@gmail.com and colours Green, Black and Red.

Presently framework will look at this Email in the data set; assuming the client is enrolled, he will be coordinated to the next stage to enter the secret key as displayed below.

Assuming the client signs in sometime later will show the shading in various mixes, each haphazardly as displayed below.

(IJISE) 2018, Vol. No. 7, Jan-Jun e-ISSN: 2454-6402; p-ISSN: 2454-812X

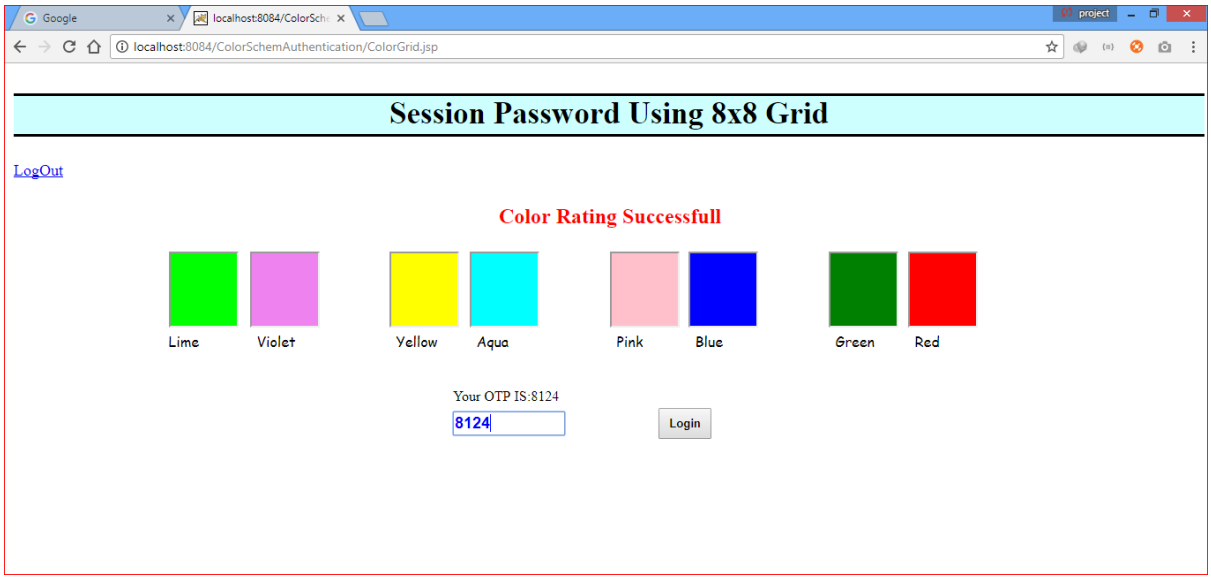

Fig 3: Login

This enjoys excellent upper hands over a customary strategy for secret word setting utilizing just a message.

IV. METHODOLOGY

The thought utilized is to save the username and secret word in the data set. The secret word will be the mix of COLOR-TEXT. When the username is coordinated effectively in the data set, the shading will show up haphazardly. We utilized just 3 tones here, so there are absolutely 3*3*3=27 potential mixes. In short, that implies you will set your secret word once, yet it is comparable to setting 27 passwords all at once. Each time when you log in, you will get anyone to mix out of 27. We need to recall the shadings and related appraisals or text. If we are setting evaluations, we need to recollect three tones and three numbers, which is simple yet exceptionally confounded for the programmers due to its haphazardness.

V. CONCLUSION

The secret word is as shading and text mix, and the tones will show up haphazardly at the hour of login.

Due to this haphazardness, code utilized as a secret phrase will likewise be entered as needed. So, all the time, requests will vary, making it difficult for the aggressor to figure the secret word. This strategy generally gives excellent protection from various assaults like Eves Dropping, Shoulder Surfing and Dictionary Attacks. In previously mentioned assaults, programmers attempt to figure the passwords and break the passwords. Still, the irregularity in this framework makes it extremely hard and hard for programmers to the passwords. We

can expand the intricacy of the framework by increasing the number of shadings in the secret word field.

REFERENCES

[1]. Zheng, Z., X. Liu, L. Yin and Z. Liu, 2010. A hybrid password authentication scheme based on shape and text. Journal of Computers, 5: 765-772.

[2]. Sreelatha, M., M. Shashi, M. Anirudh, M.D.S. Ahamer and V.M. Kumar, 2011. Authentication schemes for session passwords using color and images. International Journal of Network Security & Its Application, 3: 111-119.

[3]. Joshi, N.S., 2013. Session password using grids and colors for web applications and PDA. International Journal of Emerging Technology and Advanced Engineering, 3: 248-253.

[4]. Mathur, A., 2011. Improved password selection method to prevent data thefts. International Journal of Scientific & Engineering Research, 2: 1-2.

[5]. Patel, J., S. Padol, B. Kankariya and K. Kotecha, 2013 Authentication for session password using colour and images. International Journal of Computer Applications, pp: 5-10.

[6]. Lokhande, K.P. and V.M. Gajbhiye, 2014. Extended text and color based session password security against shoulder surfing and spyware. Journal of Emerging Technologies and Innovative Research, 1: 665-669.

[7]. Tidke, S., N. Khan and S. Balpande, 2015. Password authentication using text and color. International Journal of Scientific Research Engineering & Technology, 4: 278-281.