International Journal of Scientific Research & Engineering Trends
Volume 7, Issue 2, March-April-2021, ISSN (Online): 2395-566X

Literature Survey of Two-Way Authentication System

Mrs Dnyanada Hire, Monika Bhatt, Mohit Anand,Chaitanya Harde
Dr. D. Y. Patil Institute of Engineering Management & Research,
Akurdi, Pune,MH,India

***Abstract*- We all need to use stronger passwords which should not include our names, sequential number and birthdates even if these are easy to remember. But strong passwords are hard to remember so, the solution is Two-Factor Authentication (2FA). Two-factor authentication, also called multiple-factor or multiple-step verification, is an authentication mechanism to double check that your identity is legitimate, and this does not require transferring data over the internet. The two-factor authentication security feature has the following advantages: Enhanced security, helps in fraud prevention, Easy for users to understand and enable, Easier and quick account recovery.**

***Keywords*- Authentication; graphical passwords; Persuasive Cued Click Point (PCCP).**

I. INTRODUCTION

With so much of our lives happening on mobile devices and laptops, it's no wonder our digital accounts have become a magnet for criminals. Malicious attacks against governments, companies, and individuals are more and more common. And there are no signs that the hacks, data breaches, and other forms of cybercrime are slowing down. And as cybercrime gets more sophisticated, companies find their old security systems are no match for modern threats and attacks. Sometimes it's simple human error that has left them exposed.

All types of organizations—global companies, small businesses, start-ups, and even non-profits—can suffer severe financial and reputational loss. Password theft is constantly evolving as hackers employ methods like keylogging, phishing, and pharming. Cyber criminals do more than merely steal data. Often, they destroy data, change programs or services, or use servers to transmit propaganda, spam, or malicious code.

Two-way authentication is not important, its critical to protecting your critical assets. Passwords are regularly shared or stolen through phishing or simple guessed based attacks. Users are less and less cautious with the use of their password and more importantly completely unaware of the leaking of their digital identities in the dark web. As per the study results of the human psychology, the human brain is very efficient to remember the graphical passwords than of the text-based passwords. Also, the graphical passwords are recognizable to the user.

II. METHOD

The main objective of the project is to provide a two-way authentication scheme to the users by using Persuasive Cued Clicked point's technique and 5-bit OTP generation on user's registered device as input for each point.The two-way authentication needs to be developed for the users by using Persuasive Cued Clicked points technique and OTP which can be effectively used for any system for secure login but difficult to be guessed by attacker.

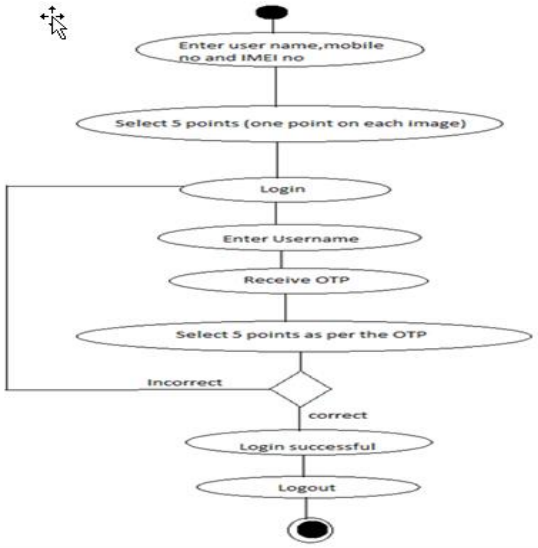

Fig 1.Flow Diagram.

Our system provides a two-way authentication to the users by using Persuasive Cued Clicked points technique and OTP.The user has to register him by entering his user's name, mobile number and email-id. Then will have to select the five images with which user wants to generate the password by clicking one point on each image. After the five clicks unique password is generated and the registration process is completed.

Now every time the user wants to login will have to enter the username and select the continue button. Fig.1 shows the flow chart of the processAfter user selects login; user will receive the OTP containing 5-bit binary code on his mobile. Now user want to select the same points which he had selected at the time of registration for the images when the bit in the OTP is 1 and select any other point

except the point select while registration for the image when the bit in the OTP is 0. Only if the user has followed this process correctly, he/she will get the access to the system using login.

III. LITERATURE SURVEY

One of the best passwordauthentication systems was text based or alphanumerical based password which has several problems. One of the main problems with text-based password is it was tiresome to remember several text passwords for different account. Then introduction of biometric password [1] and token-based password was considered as the alternative of the text-based password, but it again has several drawbacks like cost and unavailability issue.

To overcome the disadvantages of text-based password and token-based password the invention of graphical password is introduced. Initially there were following graphical password authentication systems: A. Pass point. B. Cued Click Point (CCP). C. Persuasive Cued Click Points (PCCP). But this system had again disadvantage of hot spot problem. To overcome the disadvantage of hot spot problem invention of cued click point is made.

1. Pass Point:
S. Wiedenbeck et al [2], have invented the pass point system for password authentication. The concept of the pass point was as simple as just clicking five point on single image and combination of this point as a password. In this system user has to select five points from single image and at the time of password selecting and during the time of login user has to repeat the same sequence of the points from single image. But the main security problem with this was the HOTSPOT, the area where the user clicks. User choose the easy to memorable passwords to which can be easily guessed by hacker. To avoid this problem the next method is implemented.

2. Cued Click Point:
To overcome the disadvantage of the pass point authentication system the cued click point is invented. Cued click points [3] has the same concept as of the pass point but the main difference between them is passing five points on five different image one point per image.

3. Persuasive-Cued Click Point (PCCP):
The persuasive cued click point [4][5] is the addition of the persuasive feature to cued click point. It allows user to select less portable password. It has two more function as shuffle and viewport, when users make a secret word, the images are a little monochromic except for viewport for to avoid known hotspots the viewport. The most useful benefit of PCCP is make complex system to hackers. Users have to choose a clickable area [6] within the area and cannot click outside of the viewport unless they press the shuffle button to randomly reposition the viewport. At the time of password creation users may shuffle as many times as he wants. Only during the password generation, the viewport & shuffle buttons are displayed. After the secrete word generation process, graphical images are presented to users casually without the viewport & shuffle button. Then user has to choose exact clickable area on particular image. Now a day's PCCP is a best technology but has security problems related with it.

4. A novel graphical method [8]:
This method of authentication that employs graphical coordinates along with a novel introduction of time interval between successive clicks. A novel Graphical Password scheme is proposed in this paper which tries to meet the criteria of ease of use and the security at the same time. The scheme has a large password space and the simple implementation makes it easy for the user to create her password and memorize it too.

IV. FUTURE SCOPE

In future it has great scope. It can be used everywhere instead of text-basedpassword. We can increase the security of this system by increasing thenumber of levels used; the number of tolerance squares used.

- In future development we can also add challenge response interaction. In challenge response interactions, server will present a challenge to the client and the client need to give response according to the condition given.
- To make this system more secure from malware attacks and threat.
- To use AI and ML to make it more efficient.
- To increase the processing speed and make it more UI friendly.

V. RESULTS

The system is designed in such a way that itthat the Improved Authentication Scheme Using Persuasive Cued Click Points system is very efficient to use. This system founds very secure andflexible to use. This system allows very attractive GUI to user so user finds veryattractive and convenient to use this type of password.

VI. CONCLUSION

The proposed Cued Click Points scheme shows promiseas a usable andmemorable authentication mechanism.By taking advantage of users' ability to recognize images and the memorytrigger associated with seeing a new image, CCP has advantages overPass Points in terms of usability. Being cued as each image shown and havingto remember only one click-point per image appears easier than having toremember an ordered series of clicks on one image.CCP offers a more secure alternative to Pass Points. CCP increases theworkload for attackers by forcing them to

first acquire image sets for eachuser, and then conduct hotspot analysis on each of these images.

REFERENCES

[1] S. Prabhakar, S. Pankanti, and A. K. Jain, “Biometric recognition: Security and privacy concerns,” IEEE Security Privacy Mag., vol. 1, no. 2, pp. 33–42, 2003

[2] S. Wiedenbeck, J. Waters, J.C. Birget, A. Brodskiy, N. Memon, “Design and longitudinal evaluation of a graphical password system”. International J. of Human-Computer Studies 63 (2005) 102-127.

[3] M .Swathi, M. V. Jagannatha Reddy, Authentication Using Persuasive Cued Click Points International Journal of Engineering Research & Technology (IJERT) Vol. 2 Issue 7, July-2013 IJERT ISSN: 2278-0181.

[4] Sonia Chiasson, Member, IEEE, Elizabeth Stobert, Alain Forget, Robert Biddle, Member, IEEE, and P.C. vanO or schot, Member, IEEE “Defenses Against Large Scale Online Password Guessing Attacks By Using Persuasive Click Points” IEEE Transactions on Dependable and Secure Computing, volume 03-No. 3. Issue 01 March 2012.

[5] L. Jones, A. Anton, and J. Earp, “Towards Under standing User Perceptions of Authentication Technologies,” Proc. ACM Workshop Privacy in Electronic Soc., 2007.

[6] Fatehah M.D., MohdZalishamJali&Wafa M.K., Nor Badrul Anuar, “Educating Users to Generate Secure Graphical Password Secrets: An Initial Study” 2013, IEEE.

[7] Muhammad Daniel Hafiz, Abdul Hanan Abdullah, NorafidaIthnin, Hazinah K. Mammi, “Towards Identifying Usability and Security Features of Graphical Password in Knowledge Based Authentication Technique”, 2008, IEEE.

[8] Smita Chaturvedi, Rekha Sharma, “Securing text & image password using the combinations of Persuasive Cued Click Points with the help of Improved Advanced Encryption Standard, International Conference on Advanced Computing Technologies and Applications (ICACTA-2015).

[9] Madhuri Achmani, Radhika Dehaley, Anuja Gaonkar, Anindita Khad, Two Level Authentication System Based on Pair Based Authentication and Image Selection, IJRASET Volume 4 Issue IV, April 2016 ISSN: 2321-9653.

[10] N. S. Joshi,"Session Passwords Using Grids and Colors for Web Applications and PDA" in International Journal of Emerging Technology and Advanced Engineering.

[11] H. Zhao and X. Li, "S3PAS: A Scalable Shoulder-Surfing Resistant Textual-Graphical Password Authentication Scheme," in 21st International Conference on Advanced Information Networking and Applications Workshops (AINAW 07), vol. 2. Canada, 2007, pp. 467-472.

[12] Mohd. Sarosh Umar and Mohd. Qasim Rafiq, "A Graphical Interface for User Authentication on Mobile Phones", in ACHI 2011: The Fourth International Conference on Advances in Computer-Human Interactions, Guadeloupe, France, February 23-28, 2011.