International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 05 Issue: 07 | July - 2021 ISSN: 2582-3930

Graphical Password to Avoid Shoulder Surfing

Arnold Bernard[1], Afshana Mondal[2], Prajakta Gaikwad[3], Pratik Deshmukh[4]

, Nishigandha Ghotmukle[5]

JSCOE Hadapsar, Pune-411028, Maharashtra, India.

---***---

Abstract- ***The proposed graphical password system is a potent alternative to the traditional text based alphanumeric password scheme. A graphical password is brought about in conformity with the user which has an alpha-numeric and color code that practically reduces shoulder-surfing attacks. At present, it presented a graphical shoulder-surfing safe arrangement during which the customer can successfully and effectively complete the login strategy without being stressed over shoulder surfing attacks. Information and Computer security is supported by passwords that area unit the principle a part of the authentication method. The most common Computer authentication technique is to use alphanumerical username and countersign that has important drawbacks. Therefore, the main focus of this report is to debate graphical watchword systems and the way they'll contribute to handle security issues that threaten authentication processes. One such threat is shoulder-surfing attacks, that is reviewed during this project.***

Keywords: ***Graphical password, authentication, shoulder-surfing, data and computer security.***

I. INTRODUCTION

With everything turning on-line, the chance of cybercrimes and privacy breaches is additionally increasing. Passwords play an enormous role keep your knowledge safe. Sadly, these passwords square measure broke unmercifully by intruders by several straightforward suggests that like masquerading, eaves-dropping and alternative rude means say dictionary attacks, shoulder surfing attacks, social engineering attacks. Hence associate improved system associated technique is required to make positive identification values that square measure each extremely tough for an entrant to compromise, while simultaneously simple for a user to use and maintain. Shoulder surfing exists to a substantial amount in globe. However, users aren't responsive to being discovered at intervals the bulk of

cases. Observers' unit opportunist and barely act out of reasons apart from curiosity and tedium. Moreover, they generally associate their conduct with negative feelings. Shoulder surfing puts authentication credentials like PINs, passwords and patterns in peril. Whether we log in to our phones, computers or some other device, the most frequent way to prove our identity is through entering a text-based password. This category of passwords is vulnerable to a range of attacks including the type called shoulder-surfing.

Such an attack is administered by someone watching the screen during authentication with the intent to find out the password. When entering a PIN or password to access a phone, computer or ATM machine you might try to perform the authentication process discretely in case someone is watching.

Graphical passwords have the potential to be more immune to these attacks than textual passwords.

Fig1.1 Shoulder-surfing

II. METHODOLOGY / WORKING

To address this problem, we have developed authentication methods that use pictures and objects as passwords. The past decade has seen a budding interest in using graphical passwords as a possible replacement to the traditional text-based passwords.

This method is useful for those who are interested in finding an alternative to text-based authentication method.

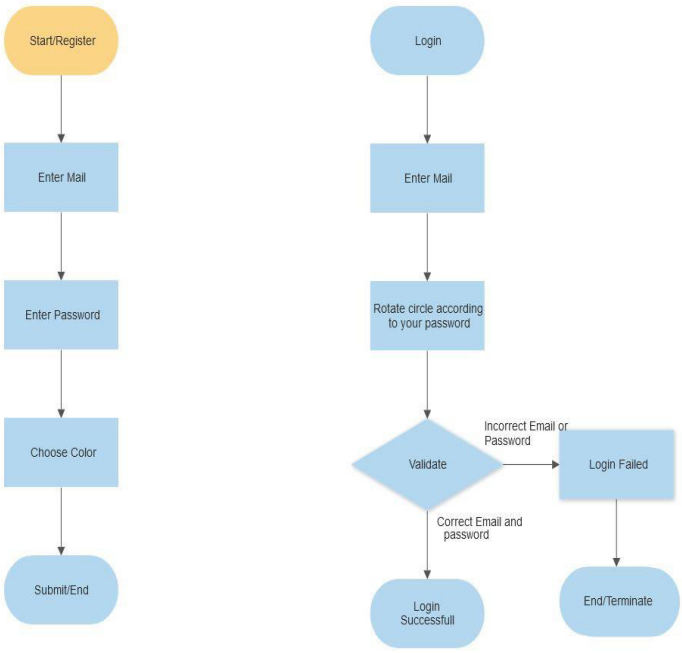
is an integral part of security. Authentication will give the customer greater security.

Usability testing of this method showed that novice users were able to enter their graphical password accurately and to remember it over time. The client asks to check in to the system, and therefore the application shows a hover consisting of 8 equally calculated zones. The colors of the circular parts of the 8 sections are special, and each section is identified by the hue of their curve.

Based on the color previously selected by the user, they have to rotate the circle according to which the character or the number should reside using the clockwise/anticlockwise button.

SR NO	PROJECT TITLE	AUTHORS	YEAR
1	Graphical Password to avoid Shoulder-Surfing.	Bharatepudi Himaja, Sajja Chand, Uday Teja, Maddirala Kashyap	(2020)
2	Graphical Password to Avoid Shoulder Surfing	Harshada Shitole, Priyanka Chaure, Pradnya Thorat, Ashwini Gaikwad	(2019)
3	Graphical password: prevent shoulder-surfing attack using digraph substitution rules.	Lip Yee, Chin Soon, Amanul, Tan Fong	(2017)
4	The Shoulder Surfing Resistant Graphical Password Authentication Technique.	Mrs. Aakansha S. Gokhalea , Prof. Vijaya S. Waghmare	(2016)

2.1 Block Diagram of Proposed System:



Input: The user would provide email id, password and choose a specific color during registration. In the login phase user needs to enter email id and rotate

the circle according to the password. To enter the password, user must rotate the inner and outer orbit in clockwise or anticlockwise direction until the color and the character are aligned.

Output: Once the password is entered correctly, the user is authorized to access the system. In case the user forgets the password, a mail would be sent to the user's registered email id for authentication.

III. LITERATURE SURVEY

[1] In this particular paper, the user talks about how vulnerable shoulder surfing can be by giving us a specific scenario. Now, this scenario is when the malpractitioner individual attempts to get the credentials of a user utilizing an electronic device i.e., Camera. It's fairly easy for a spectator to find out the PIN as the Pins require only a few amounts of numeric characters. The second scenario given is while someone is opening their Mobile phone at a busy public place such as the main city square or Local station for an instance. In such cases, shoulder-surfing can be favored as it's safe for a spectator to stand close to the victim while neglecting their attention.

[2] This report is to draw attention to the Graphical password system to secure the authentication process. One such probability is shoulder surfing which is also reviewed in this project. The most used authentication method is the text method such as a combination of alphabets and numbers(alphanumeric). But such passwords provide less security and are difficult to remember. To overcome this drawback/difficulty we used a barcode image as a password.

[3] This paper proposes a replacement theme that uses letter substitution rules to hide the mechanism or activity needed to derive password-images. During this projected methodology, a user is simply needed to click on one amongst the pass-image rather than each pass-images shown in every challenge set for 3 consecutive sets. whereas this activity is straightforward enough to scale back login time, the photographs clicked seem to be random and might solely be obtained with complete information of the registered positive identification beside the activity rules. Thus, it becomes not possible for shoulder-surfing attackers to obtain the knowledge

[4] The core plan of this paper is to set a password by selecting from the number of images. This password is called a 'secret pass'. The secret pass must contain 6 or more images. Also, the no. of images must always be even to make sure that the pairs of images are formed. Based on this secret pass a session password would be created. Thus, a password was generated as the first step of authentication. These passwords were the modifications in their existing system. The secret

pass and session password was used to make the system more secure.

IV. EXPECTED OUTCOMES

Password ensures that computer or information can be accessed by those who have the right to view or access them. But these textual passwords can be cracked into easily through various types of cyber-attacks. So, to overcome these vulnerabilities, this graphical identification technique is introduced. The system meets crucial conflicting requirements which makes the passwords easy to remember and hard to decrypt. The passwords are presented in the form of graphical user interface which helps the users to better interact with the system. The project also ensures more security against obtaining authentication sequence to potentially avoid shoulder surfing.

TABLE 1
COMPARISON OF PASSWORD TECHNOLOGIES

Comparison	Password Authentication Systems		
	Text Based	Biometric/Token Based	Graphical Password
Security	Least	High	Highest
Required Cost	Nothing	Higher	Less
Usability	Easy	Complex	Easiest
Availability	Always	Not Always	Always
GUI	User Friendly / Not attractive	Not user friendly / Attractive	User Friendly / more Attractive

Table 4.1 Comparison of Password technologies

V. CONCLUSION AND FUTURE SCOPE

Graphical passwords are an alternate to text-based alphanumeric password. It fulfills both conflicting requirements i.e., it is easy to recall & it is difficult to assume. With the solution to the shoulder surfing problem, it becomes more secure & easier password scheme. It is harder to crack graphical passwords using the standard attack methods such as brute force search, dictionary attack or spyware.

We further look towards making a conventional graphical password authentication system, which will be novice friendly. We intent to make certain upgrades in system with a combination of objects and alphabets to increase the complexity.

VI. REFERENCES

[1] Bharatepudi Himaja-Graphical Password to avoid Shoulder-Surfing 2020

[2] Harshada Shitole - Graphical Password to Avoid Shoulder Surfing 2019

[3] Graphical password: prevent shoulder-surfing attack using digraph substitution rules 2017

[4] Mrs.Aakansha S. Gokhale The Shoulder Surfing Resistant Graphical Password Authentication Technique 2016