IOSR Journal of Engineering (IOSRJEN) **www.iosrjen.org**
ISSN (e): 2250-3021, ISSN (p): 2278-8719
Vol. 09, Issue 5 (May. 2019), ||S (XI) || PP 67-70

Secure Authentication For Data Protection Using color schemes (In cloud computing)

Gulafshan Shaikh Hasan, Mr. Pranjal Dhore, Ms. Monali Gulhane
M.Tech, Department of Computer Science & Engineering,
Jhulelal Institute of Technology, Nagpur, India

Abstract: *Due increase in the usage of cloud based systems there is an increase in the amount of information on the cloud and as a result there is need for confidentiality. Most common method used for authentication is textual password. But these passwords are susceptible to shoulder surfing, dictionary attack, eavesdropping. Generally the passwords tend to follow patterns that are easier for attackers to guess. A literature survey shows that text-based password suffer this security problem. Pictographic passwords are provided as replacement to text based passwords.*

Pictographic passwords may prone to shoulder surfing. Pictographic passwords may suffer with the usability issue. This paper uses color code authentication which provides two step authentication to the user. Each time user logged in with generated one time password.

This scheme is tested with different kinds of security attacks. User has to memorize only the sequence of three colors and three shades selected at the time of registration. This scheme is useful for secure authentication method for data protection on cloud.

Keywords: *Authentication; Cloud; Challenge response; Graphical password; Pictographic; Textual password.*

I. Introduction

Authentication systems play an important role in every application. Its allow application to authenticate user and provide him access control for the application. A weak authentication system leads to various vulnerable attacks. When it's come to user authentication, the first Scheme comes in minds is Text based authentication.

In cloud computing to access data one has to authenticate the system. The common authentication method used to access data on cloud is password. The major drawbacks of text based passwords are weak password, forgot password, stealing of password etc. So it requires strong and secure authentication method for the protection of data on cloud.

Dhamija et al concluded that humans can only memorize very few passwords due to this fact user are writing down, share or User the same passwords for many accounts. The solution to this may be the pictographic password. The first graphical password is described by Greg Blonder.

In this scheme user requires to click on selected regions in image that is displayed on screen. The user has to select the same regions for login. But such scheme suffers from stability problem due to its static image selection.

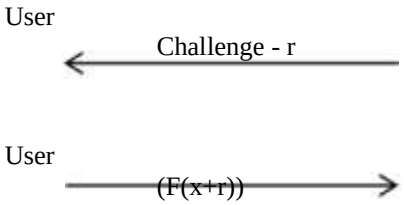
Text based password are susceptible to dictionary attack, shoulder surfing, eavesdropping. To overcome some of these problems pictographic password are introduced. The dictionary attack is not possible with such password. But it suffers from shoulder surfing. Man et al. added a small layer of patter graphics along with alphanumeric characters to prevent shoulder surfing.

II. Implementation

The colour code authentication (CCA) scheme prototype is implemented on private cloud - Tiger cloud in the institute. It is developed using PHP, JavaScript, HTML, jQuery, CSS and MySQL. The CCA prevent against shoulder surfing or any type of capturing activity of users. It uses challenge response System (CRS).

General structure of CRS is given in fig. 1

Login request
User ⟶ System



X is known to User and System

Fig.1 - Challenge Response System

CRS is depending on "one-way hash" function. In such a function from its calculated hash value it is computationally an infeasible to calculate original value. In above case f is a function which is public.

In CCA instead of graphical elements colors and three shades are used. The registration or sign up procedure consists of following steps.

1. Give the input - First Name, Last Name, User Name or User ID and contact number.
2. Randomly click on any three colors on the COLORS GRID and memorize it with its sequence.
3. Also randomly click on the shades - White, Gray and Black. These random sequence of shades need to be memorized by the user. It is required at the time of login. If User failed to provide correct sequence it will not be authenticated.

Fig 2: home page

Registration process is shown in the fig. 3.

The input provided by the user at time of registration is encrypted using AES algorithm and it stored in a file. For each user the password generated at the time of registration is encrypted with different keys. These keys are maintained in separate database file. This database file is encrypted by using AES algorithm with salt. So in case of encrypted file is compromised still the information stored by the users is not exposed. The main objective of this proposed scheme is to form the nine digit one time password with all these combination.

Fig. 4 User Registration to color code authentication

The following steps are performed for authentication -
1. Specify username and provide the same sequence of shades (White, Gray, Black)
2. If Username or Shade's sequence is incorrect then authentication process terminated.
3. Select the number displayed on (First/Second/Third) color in the COLOR GRID. It represents respective Column number in the NUMERAL GRID.
4. First, second and third row of NUMERAL GRID is marked with White, Gray and Black shades respectively. Respective Row is identified as per the sequence of shade chosen at the time of registration.
5. Select the three digit number available in the NUMERAL GRID by using identified row and column number in step 3 and 4.
6. Concatenate the three digit number retrieved from NUMERAL GRID to the One Time Password Box. Initially it is empty.

III. Conclusion

We presented a 2 level pictographically scheme for authentication system. First we use color code authentication scheme using color features for password where user have to select a color code as password items in terms of their uniqueness and reliability with which they can be entered. In the second, we implemented a geo graphical based password which is s self-selected location from the map provided to the user. In summary, this paper proposed improving the security of graphical password systems by integrating color code and geographical approach. It then illustrates that user performance is equivalent to that attained in standard password systems through a usability study assessing task time, error rate ultimately.

References

[1]. Morris, Robert, and Ken Thompson. "Password security: A case history." Communications of the ACM 22.11 (1979): 594-597.
[2]. Blonder, G. "United States Patent 5559961." Graphical Passwords (1996).
[3]. Man, Shushuang, Dawei Hong, and Manton M. Matthews. "A Shoulder Surfing Resistant Graphical Password Scheme-WIW." Security and Management. 2003.
[4]. Wiedenbeck, Susan, et al. "PassPoints: Design and longitudinal evaluation of a graphical password system." International Journal of Human-Computer Studies 63.1 (2005): 102-127.
[5]. Thorpe, Julie, and Paul C. van Oorschot. "Graphical Dictionaries and the Memorable Space of Graphical Passwords." USENIX Security Symposium. 2004.
[6]. Wiedenbeck, Susan, et al. "Design and evaluation of a shoulder-surfing resistant graphical password scheme." Proceedings of the working conference on Advanced visual interfaces. ACM, 2006.
[7]. De Angeli, Antonella , et al. "Is a picture really worth a thousand words? Exploring the feasibility of graphical authentication systems". International Journal of Human-Computer Studies 63.1 (2005): 128-152.
[8]. Dhamija, Rachna. "Hash visualization in user authentication." CHI'OOExtended Abstracts on Human Factors in Computing Systems. ACM,(2000).
[9]. Dhamija, Rachna, and Adrian Perrigo "Deja Vu-A User Study: Using Images for Authentication." USENIX Security Symposium. Vol. 9.(2000).

[10]. Brostoff, Sacha, and M. Angela Sasse. "Are Pass faces more usable than passwords? A feild trial investigation." People and Computers XIVUsability or Else!. Springer London, 2000. 405-424.Sobrado, Leonardo, and Jean-Camille Birget. "Graphical passwords."
[11]. The Rutgers Scholar, an electronic Bulletin for undergraduate research 4(2002): 2002.
[12]. Balaji, S. "Authentication techniques for engendering session passwords with colors and text." Advances in Computer Science and its Applications 1.3 (2012): 189-195.
[13]. Sreelatha, M., et al. "Authentication schemes for session passwords using color and images." International Journal of Network Security & Its Applications 3.3 (2011): 111-119.