IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Vol.-7, Special Issue-12, May 2019 E-ISSN: 2347-2693

Secure Authentication For Data Protection In Cloud Computing Using color schemes

Gulafshan Shaikh Hasan[1*], Pranjal Dhore[2], Monali Gulhane[3]

M.Tech, Department of Computer Science & Engineering, Jhulelal Institute of Technology, Nagpur, India

Corresponding Author: gulafshansk13@gmail.com

Available online at: www.ijcseonline.org

***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*—** cloud; textual password; graphical password; pictographic; authentication; challenge response.

I. INTRODUCTION

Authentication system 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 its 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.

Cloud security mostly depends on authenticating the User by using passwords. The key requirements of password is, it should be easy to remember and secure. In case studies of password by Moris it is found that users are not selecting and handling text based passwords in insecure manner.

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.

Today, authentication is achieved through the use of password technique. To prove and maintain the identity every user uses a password authentication. The traditional method of password is a textual (alphanumeric) password. It is the combination of alphabets, digits and special symbols. But it has various limitations.
Computer/network security hinges on two very simple goals:

- Keeping unauthorized persons from gaining access to resources
- Ensuring that authorized persons can access the resources they need

Authentication and security:
Authentication is an absolutely essential element of a typical security model. It is the process of confirming the identification of a user (or in some cases, a machine) that is trying to log on or access resources. There are a number of different authentication mechanisms, but all serve this same purpose.

Authentication vs authorization:

It is easy to confuse authentication with another element of the security plan: authorization. While authentication verifies the user's identity, authorization verifies that the user in question has the correct permissions and rights to access the requested resource. As you can see, the two work together. Authentication occurs first, then authorization.

Forms of Authentication (combinations are possible):

- password-based
- address-based
- cryptographic

II. RELATED WORK

Researchers developed pictographic passwords to improve security. When USer log in, it has to click on the images or a part of images. The user will be authenticated if it clicks on valid image. The pictographic password is easy to remember than text based password. In [4]-[5] it is presented that human are memorizing pictographic password very effIciently as compared to text passwords. Susan Wiedenbeck [6] proposed forming convex hull by selecting the icons from set of icons displayed on the screen. As such it carries out 4 rounds. The USer will be authenticated if they can be able to form the convex hull. This approach prevents shoulder surfIng. But its authentication method takes longer time.

Most of the graphical passwords are implemented using challenge response system (CRS). In CRS USer has to register the responses with the system and then system will give a challenge to the USer for which only USer has to answer. In case of pictographic password, users selected image at the time of registration is the response. The system will give challenge to the user with many images. The user has to give its answer by selecting correct image. The drawback of such system if there is a series of challenges then it will take more time. Another drawback is that at the time of registration several USers may select same image [7] as their password. In this case system entropy will be reduced, resulting in insecure authentication.

The challenge response system is used by Deja Yu [8]-[9], and Passfaces [10]. In Passfaces it gives challenge to the user with nine faces of human out of which only one is correct. 978-1-5090-1022-6/16/$31.00 ©2016 IEEE 424 2016 International Conference on Computational Systems and Information Systems for Sustainable Solutions Such four rounds are conducted. If user responded correct answer to each round then authentication is successful otherwise failed. Deja Vu uses random images. It displays twenty five images at a time. Password consists of five images. User has to click on these five images. Sobrado and Birget [11] proposed a scheme as "triangle scheme". In this scheme user needs to select any three object as a part of their registration process.

At the time of authentication user needs to identify these three objects and form a virtual triangle. Then user needs to click on any object inside this triangle which is formed by preselected three objects.Some of the researcher uses two step authentication to overcome shoulder surfing. S. Balaji et al. [12] proposed color and text based authentication scheme. They have proposed authentication using two levels. At first level it uses text based and second level it uses graphical scheme. Sreelatha, M., et al [13] proposed a scheme using colors and images. It uses pair based and hybrid text based approach for authentication.

III. METHODOLOGY

Graphical password is an alternative to alphanumeric passwords in which users click on images to authenticate themselves rather than typing alphanumeric words. Graphical passwords are more memorable compared to the alphanumeric passwords, because it is easier to remember an image of flower than a set of alphabets and numbers. We will develop a secure and robust mechanism for authentication using pictograph and geographical password. We use Java J2EE for developing the system. We will design a banking web application with the purposed authentication scheme to demonstrate the usability of system.

Text based password are susceptible to dictionary attack, shoulder surfing, eavesdropping. To overcome some of these problems pictographic password will be introduced. In this paper we propose a pictographic based authentication Scheme which includes

• Color Code Authentication Scheme
• Geographic Authentication Scheme

IV. RESULTS AND DISCUSSION

In this paper we intend to provide a new and more secure graphical password system which will be designed using Java. We will combined Color code and geographical based password to provide a robust and more secure graphical password scheme on cloud application. The purposed system will provide a safe guard against Dictionary Attack, Guessing Attack, Shoulder Surfing etc. A banking application will be developed to demonstrate the use of purposed scheme.

V. CONCLUSION AND FUTURE SCOPE

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.

FUTURE SCOPE

As compare to plain text authentication scheme, the purposed scheme provide more robust and secure mechanism. We integrated color code and geographical functionality to build this system. This system still need few updates to provide a complete authentication framework for cloud based application. In future work we implement fingerprint, face recognition using ires sensor of android smartphone.

Currently this scheme is suitable for user authentication only, in future we provide this scheme for payment, ticketing system, and other form of security application where authentication system is needed.

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.

