International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169
Volume: 5 Issue: 3 88 – 90

Security Enhancement using Color Based Alphanumeric on Cloud

[1]Bharani. M, [2]Naveena. R, [3]Priyadharshini. V
[1,2,3]Computer Science and Engineering
University College of Engineering
Thirukkuvalai
bharaniram23@gmail.com, naveenaram97@gmail.com,
dharshapriya555@gmail.com, sridharanauttc@gmail.com

Sridharan. S
Assistant Professor
Head of the Department
Computer Science and Engineering
University College of Engineering
Thirukkuvalai

Abstract- Cloud computing is where computing resources are accessed from a virtual machine "cloud" rather than a local desktop or organizational data center. While enjoying the convenience brought by this cloud, users also start worrying about losing control of their own data. The only solution is authentication. The password is the most common authentication method. Text based, patterns, pictographic and graphical passwords are suffering from some security attacks. This paper uses color code authentication in which the OTP is generated after the two steps of authentication. This color scheme tests with different kinds of security attacks. It is used for secure authentication for data protection in the cloud.

Keywords- *cloud; textual password; graphical password; color grid;*

*****

I. INTRODUCTION

In cloud computing to access data one has to authenticate the system. Cloud computing is an internet-based model for enabling convenient, on-demand network access to a shared pool of configurable computing resources. While enjoying the convenience brought by this cloud, users also start worrying about losing control their own data. To protect cloud from malicious user and unauthorized access, we use the color code authentication. The paper is divided into five sections. In section two related works in the area of graphics and color based password are presented. Section three describes the implementation of the proposed scheme. Security and performance analysis of the proposed scheme is elaborated in section four. Section five concludes and gives directions for future work in this area.

II. RELATED WORK

Text based password and Patterns are the most common authentication method. The weakness of the textual password authentication system is that it is easy to break and vulnerable to dictionary attack or brute force attacks. Pictographic password requires to click on selected regions in the image. Pictographic password schemes suffered from shoulder surfing. Implement triangle Scheme user needs to select any three objects as a part of their registration process. Graphical password requires a long time to perform.

Implement the color code authentication (CCA) scheme prototype with a numerical grid approach using ECC encryption. In numerical grid, we can arrange color values and shade values. Has to memorize only the sequence of three colors and three shades selected at the time of registration to provide OTP security with alphanumeric and special characters. The CCA provides solution to avoid the SQL injection attack. Difficult to provide chance to retrieve data from the database. The Complexity is less to construct a framework against SQL injection attacks.

III. IMPLEMENTATION

The color 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 a challenge response system (CRS). General structure ofCRS.

- Register their details such as first name, last name, password and mobile number.
- Randomly click on any three colors on the Colors grid and memorize it with its sequence.
- Also randomly click on the shades - White, Gray and Black. These random sequences of shades need

 ISSN: 2321-8169
88 – 90

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**.**

The user needed input at the time of registration is encrypted using the ECC algorithm and is stored in a file. For every user's encryption is done with different keys. Different keys are maintained in a separate database file. In case of encrypted file is compromised, the information stored by the users is not exposed. The major role of this proposed scheme is to form the nine characters along with special character one time password with these combinations.

Fig. 1 User Registration

The following steps are performed for authentication:-

1. Specify the username and provide the same sequence of shades(White, Gray, Black).

2. Authentication is terminated, if username or shade's sequence is incorrect.

3. Select the color displayed (First,Second,Third) in the COLOR GRID and it must similar to the color sequence at the time of registration.

4. These color sequences represent the column number in the NUMERICAL GRID.

5. In CHARACTER GRID the first, second and third rowsare marked with White, Gray and Black shades and the row is identified according to the sequence chosen at the time of registration.

6. Select the three special characters available in the CHARACTER GRID using an identified row and column in step 3 and 4.

7. Initially OTP Password box is empty and concatenate the three special characters retrieved from CHARACTER GRID to the One Time Password Box.

8. Repeat step 3 to 6 for second and third selected color value.

9. Once nine characters are collected, Press submit button for authentication.

10. If the combination of correct charactersis retrieved, User will be authenticated.

Fig. 2 Authentication process step 1

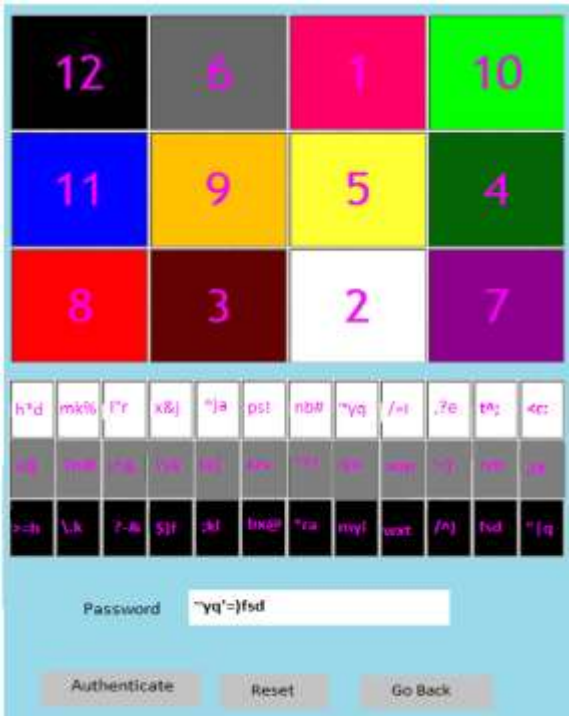

Fig.3 Authentication process step 2

SECURITY AND PERFORMANCE ANALYSIS:

The proposed CCA scheme not only prevents shoulder surfing, but also other security aspects given below.

- **POSSIBLE PASSWORD SPACE:** The space for the password is very large. The possible number of passwords can be created is 12C3.

It is further taken combinations 3 shades so the possible number of combinations is 220C3.

- **BRUTE FORCE ATTACK:** It is not possible with this CCA scheme. In each and every time the color grid is created with a different set of random numbers. The combined set is very large, so Attackers may carry out video recording and observe it, it will get a failure.
- **DICTIONARY ATTACK:** This attack is not possible for the proposed CCA scheme. The requirement of dictionary attack is a set of probable words. This kind of attack is also possible with text based password.
- **SQL INJECTION:** The set of color code values and shade values are not stored in a plain text. The password is encrypted by using the ECC algorithm. This type of attack is not possible for this CCA scheme.
- **SHOULDER SURFING:** It is not possible because randomization in position of numbers because with every time of login all the numbers will be randomized. Because of the so many stages , the attacker would not be able to guess it, even if the attacker is keeping an eye on the user who is entering a password.
- **EAVESDROPPING:** It is the unauthorized real time interception of a private communication, such as a phone call, instant message, voice conference or transmission. So it does not possible in the CCA scheme.

IV. CONCLUSION

The propose scheme is easy to learn and use. It provides better usability and it does not affected by shoulder surfing, dictionary attack, eavesdropping, SQL injection, brute force attacks. This scheme is used for authentication by using text and colors. It stores the password is encrypted format using anElliptical Curve Cryptography algorithm. The database file is also encrypted by using the ECC algorithm. These reasons, it will be highly secured .

REFERENCES

[1] Manish M. Potey, C.A. Dhote, Deepak H. Sharma. "Secure Authentication for Data Protection in Cloud Schemes" proceeding of International Conference on Computational Systems and Information Systems for Sustainable Solutions at 2016.

[2] Dhamija, Rachna. "Hash visualization in user authentication." CHI'OO Extended Abstracts on Human Factors in Computing Systems. ACM, 2000.

[3] Dhamija, Rachna, and Adrian Perrigo "Deja Vu-A User Study: Using Images for Authentication." USENIX Security Symposium. Vol. 9. 2000.

[4] Brostoff, Sacha, and M. Angela Sasse. "Are Passfaces more usable than passwords? A field trial investigation." People and Computers XIVUsability or Else!. Springer London, 2000. 405-424.

[5] Sobrado, Leonardo, and Jean-Camille Birget. "Graphical passwords." The Rutgers Scholar, an electronic Bulletin for undergraduate research 4 (2002): 2002.

[6] Man, Shushuang, Dawei Hong, and Manton M. Matthews. "A ShoulderSurfing Resistant Graphical Password Scheme-WIW." Security and Management 2003.