Multi-level Graphical Password Authentication Scheme for Cloud (MGPASC)

Vijayakumari Rodda, Gangadhara Rao Kancherla, Basaveswara Rao Bobba

Abstract: *The usage and management of information technology resources and services are revolutionized with the arrival of Cloud Computing. But, the revolution always comes with problems. Authentication is one such problem. Especially for Graphical Password Authentication System, there is a threat of shoulder surfing attack. This research presents a multi-level graphical password authentication mechanism by extending an existing method. UGPSCCCT (User guided Graphical Password Scheme for Cloud using Caesar Cipher Technique) is the existing method and this method is extended in this paper such that another level of security is added. The user credentials in this method are transmitted to the server in encryption format. A key is generated for every login to encrypt user details. The analysis of the proposed method is done by calculating the computational cost and communication cost of the proposed method.*

Keywords: *authentication, graphical password, encryption, communication cost, computation cost.*

I. INTRODUCTION

Authentication is an important component of most computer systems, especially those used in services over the internet. In today's information & WWW age, every day millions of users' access various information services and applications over the internet which require secure authentication of valid users. There are many ways of authenticating one's legitimacy. The traditional way is to use a single factor authentication which requires the user to enter his ID and password to get authenticated. But this approach suffers with many weaknesses such as 1) Users tend to choose simple and easy to remember passwords as opposed to strong alphanumeric passwords which weakens their account security. 2) A User may have multiple online accounts with different service providers and since remembering username/password combination of all those accounts is difficult, user sometimes choose same password on all the accounts making the account vulnerable to insider attack, dictionary attack etc. or the user tends to write it on paper which may leak their secret information [1]. To address these issues, researchers have proposed image based password authentication techniques called graphical passwords [2] which are considered to be strong and user friendly. These are categorized as Recall based and Recognition based techniques respectively. In recall based techniques user is asked to draw his secret on a grid [3] or click on the pre-selected regions in sequence [4][5] where as the recognition based techniques requires the user to recognize and enter the pre-selected password images to get authenticated [6-8]. But, all these techniques are based on single factor i,e. only images as password. Moreover most of them suffer from serious drawbacks such as descretization problem [9], shoulder surfing attack [10], high bandwidth requirements etc. With an increase in the number of online attacks and frauds, single factor authentication is no longer considered to be secure, and the organizations are recommended to adopt two factor authentication mechanisms to secure their customers data [11]. A two-factor based authentication mechanism is the combination of two different factors (e.g.:- a Biometric and Password, or, a Smart card and PIN). This method delivers a higher level of authentication assurance and is called strong authentication which is essential for security of online accounts.

So, in order to provide secure and user friendly authentication, the security experts are strongly recommending the online service providers to deploy two factor authentication mechanisms to strengthen security without compromising user convenience. In this chapter, the above issues are addressed by proposing a user friendly multi-level authentication mechanism which allows the user to freely choose easy to remember passwords based on a description of users personal images. At login, users recall & enter their password by seeing their pre-selected images.

II. RELATED WORKS

Gokhale & Waghmare [12] proposed a two-step graphical password authentication scheme which combines two types – recognition-based and recall-based. During login of this method, user has to select images as password and three Region of Answers for three pre-selected questions. This system is vulnerable to malicious software which has the intention to take screenshot and record mouse clicks. Abuthalha et al [16] proposed an alignment based graphical password method in which user has to align images to get authenticated. Amish shah et al [17] proposed another graphical password scheme in which user has to align the password images and form a pre-registered phrase to be verified during login.

Manuscript published on 30 September 2019
* Correspondence Author

R. Vijayakumari*, Department of Computer Science, Krishna University, Machilipatnam, Andhra Pradesh, India. Email: vijayakumari28@gmail.com

G. Gangadhara Rao, Department of Computer Science and Engineering, Acharya Nagarjuna University, Guntur, Andhra Pradesh, India. Email: kancherla123@gmail.com

B. Basaveswara Rao, Department of Computer Science and Engineering, Acharya Nagarjuna University, Gubtur, Andhra Pradesh, India. Email: bbrao@alu.ac.in

Amol Bhand et al [18] proposed a click based authentication system in which user gets a system generated password on his/her email on based on RGB values of the chosen click points of the images. User has to provide this password to get authenticated.

Misbahuddin et al [13], Himika Parmar et al [14], and Vijayakumari Rodda et al [19] also proposed two-factor authentication schemes using images as password. But these methods have limitations like user credentials can be stolen over the wire during transmission. Multi-step authentication can also be found in [20] [21]. Vijayakumari et al [15] proposed an authentication scheme UGPSCCCT (User Guided Graphical Password Scheme for Cloud using Caesar Cipher Technique) that contains variable size grid for inputting images as password. The password is selected in encrypted format using Caesar Cipher Technique during login phase. But this method doesn't provide encryption for user credentials during transmission.

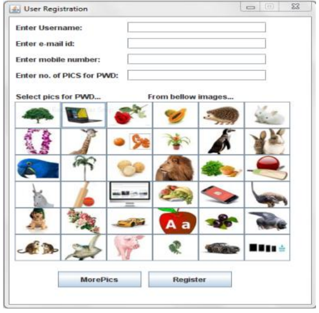

Figure 1: Registration interface of UGPSCCCT [15]

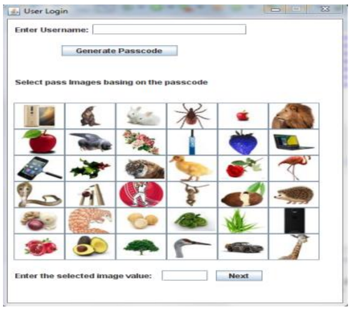
User Login
Enter Username:
Generate Passcode
Select pass images basing on the passcode
Enter the selected image value:
Next

Figure 2: Login interface of UGPSCCCT [15]

In order to rectify and overcome the drawbacks specified above, we are proposing an authentication method which authenticates in two levels. In first level a user enters his / her password by recognizing three images. These images are recognized in disguise. In the second level user enters textual password and that is transmitted in the encrypted format to the server.

The chapter is organized in such a way that, in Section 3, the related work is discussed. In Section 4, description of the existing system is given and in Section 5, the proposed method is introduced. The algorithms for registration, login, encryption of textual password, and decryption of textual password is also discussed here. In Section 6, the results are discussed and analyzed. The computation and communication cost of the proposed algorithm are also computed over here. Finally, in Section 7, the conclusion of the chapter is given.

III. PROPOSED SCHEME - THE MGPASC

MGPASC is the extension of UGPSCCCT [15]. Extra level is added to UGPSCCCT. But the password images in MGPASC are fixed to three. A user in this system has two passwords – Graphical and Textual. Images used for passwords are considered of low resolution for better efficiency and performance. Each and every password image is associated with a word that describes it. That word may contain 3 to 5 letters. The related words should be registered by the user at the time of registration. During login, user has to recall and provide that information as textual password. A key is generated using the locations in the image grid and username and with that key textual password is encrypted and sent to the server.

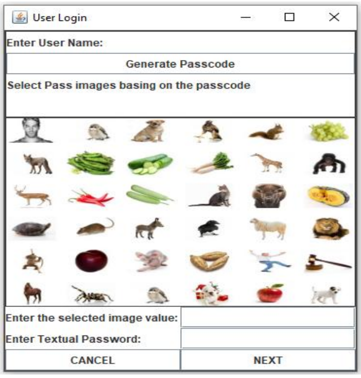

Figure 3: Login interface for Proposed Method (MGPASC)

To login to the system user has to enter his username in the beginning and then click on the "Generate Passcode" button. By clicking on that a pass code for user password encryption is generated by the system and is automatically sent to user's registered e-mail id and mobile number. Based on the received pass code, user has to recognize the password images for authentication [UGPSCCCT]. After recognizing the images, user has to enter the textual password, i.e., the words that are associated with the password images in the given field. The notations used in this MGPASC are summarized in table-1.

Table-1: Notations Used in MGPASC

U_i	i^{th} user
CS	Cloud server
ID_i	Unique identity of i^{th} user
GP_i	Graphical password of i^{th} user
TP_i	Textual password i^{th} user
K_g	Key generated from grid locations
K_u	Key generated from user identity
K_e	Key for encryption
K_d	Key for decryption
$\oplus$	The Exclusive OR operator
$\|$	The Concatenation operator
ASCII(x)	ASCII value of password string 'x'
Bin(x)	Binary equivalent of password string 'x'

1.1. REGISTRATION PHASE

In the registration phase new user registers him/her self by entering user-id, graphical password, and textual password. Registration process consists of:

1. U_i chooses his/her identity ID_i and sends it to CS for checking availability. Minimum number of characters in the ID_i should be six. If the ID_i ex+ists server grants the ID_i or else requests for new ID_i.
2. U_i has to select GP_i from existing images in the system. A GP_i should contain three images.
3. U_i has to select TP_i. TP_i consists of three words. Three words represent one password images in GP_i respectively.

3.1.1 ALGORITHM FOR CREATION OF TEXTUAL PASSWORD TP_I

A text password can contain 9 or 12 or 15 characters based on user's choice. If a user selects 3 characters to represent an image then his/her text password should be of length 9. If user selects 4 or 5 characters to represent an image then his/her text password should be of length 12 or 15 respectively.

```
1. Start
2. Select number of characters, n to represent an image.
   'n' can take any value from {3,4,5}.
3. If n == 3 then
          $TP_i$ = AAABBBCCC
   Else if n == 4 then
          $TP_i$ = AAAABBBBCCCC
   Else if n == 5 then
          $TP_i$ = AAAAABBBBBCCCCC
4. Stop.
```

The letters A, B, and C in the above algorithm are variables. For example if the user selects images of Grapes, Radish, and Apple as his/her password images in Figure 3, then her textual password can be anything like: GRAPERADISAPPLE or GRAPRADIAPPL or GRARADAPP or CATRATMAT or TABLECHAIRRACKS or BALLBOOKBIND or XXXYYYZZZ etc.

1.2. LOGIN PHASE

The login phase is invoked whenever user wants to access cloud resources. During login a user has to enter user-id, graphical password, and textual password.

1. U_i enters ID_i
2. U_i selects grid size for displaying images
3. U_i generates pass-code (PC), for selecting password images [15]
4. U_i selects GP_i from the image grid using PC [15]
5. U_i enters TP_i
6. U_i sends his/her credentials to CS by clicking on submit button

1.3. ENCRYPTION AT USER'S SIDE

The GP_i in this system is given in the encryption format using Caesar Cipher technique. To encrypt the textual password a key is generated by the MGPASC using the grid locations that display password images of the user and user-id.

```
1. k1 = three grid locations of password images
2. $K_g$ = Bin (k1)
3. Get last three characters from user's unique ID
      k2  = substr (IDi, -1, 3)
4. $K_u$ =  Bin(ASCII(k2))
5. If length($TP_i$) == 9
          $K_e = K_g \| K_u \| K_g$
   Else if length ($TP_i$) == 12
          $K_e = K_g \| K_u \| K_g \| K_u$
   Else if length ($TP_i$) == 15

          $K_e = K_g \| K_u \| K_g \| K_u \| K_g$
6. Tpwd = Bin(ASCII ($TP_i$))
7. Epwd = $K_e \oplus$ Tpwd
```

The Epwd, K_g are sent to CS for verification of user authenticity.

1.4. DECRYPTION AT SERVER'S SIDE

The server CS first composes key with the help of the received key from user and user-id to decrypt the password. The encrypted password Epwd, received by Server is decrypted to verify with the existing textual password.

```
1. Get last three characters from user's unique ID
      t1 = substr (IDi, -1, 3)
2. $K_u$ = Bin(ASCII(t1))
3. Length of user's textual password is retrieved from the
      server database into a variable lpwd
4. If lpwd == 9
          $K_d = K_g \| K_u \| K_g$  [$K_g$ is received from $U_i$]
   Else if length (lpwd) == 12
          $K_d = K_g \| K_u \| K_g \| K_u$
   Else if length (lpwd) == 15

          $K_d = K_g \| K_u \| K_g \| K_u \| K_g$
5. Dpwd = $K_d \oplus$ Epwd
```

The Dpwd is verified with the existing password in the server database. If it matches with that then U_i is allowed to access cloud resources. Otherwise user is rejected to access cloud resources.

IV. RESULTS AND DISCUSSIONS

The proposed method is based on hybrid approach which uses more than one security module. The greatest strength of this approach is no module woks independently. For example, if an attacker obtains either textual or graphical password of a user, it alone doesn't work. The second password also is essential for login. The system always performs randomization of size of display grid and images that are displayed in the grid. Due to this constrained the proposed method minimizes different types of attacks like guessing attack, shoulder-surfing attack, brute-force attack and dictionary attack. Another security aspect in this method is, for every three consecutive failures of user U_i , the authentication shuts down and the ID_i is blocked for 24 hours without any previous caution given to the user. Therefore, the proposed method provides greater security against shoulder-surfing attack.

In this section the communication and computation cost of the proposed method is estimated in order analyze the efficiency of the algorithm. In the proposed method X-OR operations and concatenation operations are used at client as well as server side. The computation and communication cost of proposed method are given in Table-2.

Where ‘x’ represents time required for performing one basic operation
T_{ipl} – Time required for giving inputs to login
T_a – Time required for conversion into ASCII
T_b – Time required for conversion into binary
T_c – Time required for concatenation operations
T_x – Time required for X-OR operations
M – Memory required for password
C_c – communication cost of password

The communication cost includes the capacity of transmitting message involved in the authentication scheme. At the user side the capacity of transmission is:

For text password it varies from 72 bits to 240 bits.

The image database consists of 1000 images and each and every image has a unique sequence number associated with it. For graphical password the images are not transmitted over the channel to the server. But, the numbers of images are sent to the server and the server matches them with the existing image password in the database. Therefore, the communication cost of image password is 30 bits (10 bits per image; totally three images to form a password).

All the input given to the proposed method, MGPASC is validated in order to prevent SQL injection attacks. Cloud based Web Application Firewalls (WAF) like Imperva can be employed for extra protection from SQL injection attacks. Methods such as Escaping, validating input, and Sanitising can also be used to prevent X-Scripting or Cross Site Scripting attacks.

1.1. COMPARISON WITH THE EXISTING SCHEMES

The schemes introduced by Misbahuddin et al [13], Gokhale & Waghmare [12], Himika Parmar [14] et al and others are claimed to be secure against shoulder-surfing attack and other attacks. These schemes may be sufficient for the standalone systems. But for the webbased systems like cloud, the security should be extended over the transmission channel also.

In cloud environment, each and every information relating to user authentication are sent from user to the cloud server for verification and confirmation. In such a case, there is a lot of chance for the attacker to intrude. In order to prevent this, the proposed method gives protection by transforming the password with some encryption technology. The password is later decrypted by the server upon receiving the session key from the user. The session key is genenrated basing on the input parameters during login.

The encryption time required for is given in table-2. The time required to execute the proposed method can be deduced from table-2 and is given as:

At client side: 4x + d + 18x + 168x + 288x + 240 x
At server side: 4x + 18x + 168x + 288x + 240 x

‘x’ in the above expression represents the time required for one basic operation and ‘d’ represents the time required to travel over the network that contain gateways. The numerical values given in the expression are taken approximately. Therefore, the numerical values can be considered as a constant C_1. Then, the expression can be written as:

$x.C_1$ for time taken by the server and
$x.\ C_1 + d$ for time taken by the client machine

The value of ‘d’ in the above expression, varies from time to time due to the availability of network or the delay, congestion, signal strength in the network etc. To recognize a graphical password, a user receives a piece of information for encryption from the server in the form of OTP during login. Sometimes the OTP may be delayed in the network transmission and user may request for resend of the OTP. Therefore, ‘d’ depends on inclusive of all the above said factors in the network.

The communication cost in the proposed method is 30 bits for graphical password and 72 to 240 bits for textual password, which is less than that obtained in [13]. Though the time required for the proposed scheme is more to execute than the existing methods, it provides better security to the user credentials in the cloud environment than the existing methods in [12][13][14].

V. CONCLUSION

Cloud computing is the most happening thing in the present digital era. In this context, a strong and secure authentication mechanism is direly needed to protect the cloud resources from malicious users. The method proposed in this chapter is a promising one which validates a user in two-levels. This method also shields the user’s personal information during transmission along the wire. It is resistant to almost all possible attacks. As the method uses randomization of grid and images in the grid, it withstands shoulder-surfing attack vigorously.

REFERENCES

1. Adams, A., & Sasse, M. A. (1999). Users are not the enemy. Communications of the ACM, 42(12), 41-46.
2. Suo, X., Zhu, Y., & Owen, G. S. (2005, December). Graphical passwords: A survey. In 21st Annual Computer Security Applications Conference (ACSAC'05) (pp. 10-pp). IEEE.
3. Jermyn, I. H., Mayer, A., Monrose, F., Reiter, M. K., & Rubin, A. D. (1999). The design and analysis of graphical passwords. USENIX Association.
4. Blonder, G. E. (1996). Graphical passwords. lucent technologies, inc., murray hill, nj. US patent, ed. United States (June 1996).
5. Wiedenbeck, S., Waters, J., Birget, J. C., Brodskiy, A., & Memon, N. (2005, July). Authentication using graphical passwords: Effects of tolerance and image choice. In Proceedings of the 2005 symposium on Usable privacy and security (pp. 1-12). ACM.
6. Perrig, A., & Song, D. (1999, July). Hash visualization: A new technique to improve real-world security. In International Workshop on Cryptographic Techniques and E-Commerce(pp. 131-138).
7. Dhamija, R., & Perrig, A. (2000, August). Deja Vu-A User Study: Using Images for Authentication. In USENIX Security Symposium (Vol. 9, pp. 4-4).
8. De Angeli, A., Coutts, M., Coventry, L., Johnson, G. I., Cameron, D., & Fischer, M. H. (2002, May). VIP: a visual approach to user authentication. In Proceedings of the working conference on advanced visual interfaces (pp. 316-323). ACM.
9. Birget, J. C., Hong, D., & Memon, N. D. (2003). Robust discretization, with an application to graphical passwords. IACR Cryptology ePrint Archive, 2003, 168.
10. Wiedenbeck, S., Waters, J., Sobrado, L., & Birget, J. C. (2006, May). Design and evaluation of a shoulder-surfing resistant graphical password scheme. In Proceedings of the working conference on Advanced visual interfaces (pp. 177-184). ACM.
11. Council, F. F. I. E. (2005). Authentication in an internet banking environment. Retrieved June, 28, 2006.
12. Gokhale, M. A. S., & Waghmare, V. S. (2016). The shoulder surfing resistant graphical password authentication technique. Procedia Computer Science, 79, 490-498.

13. Misbahuddin, M., Premchand, P., & Govardhan, A. (2008, December). A user friendly password authenticated key agreement for web based services. In 2008 International Conference on Innovations in Information Technology (pp. 633-637). IEEE.
14. Parmar, H., Nainan, N., & Thaseen, S. (2012). Generation of secure one-time password based on image authentication. Journal of Computer Science and Information Technology, 7, 195-206.
15. Vijayakumari, R., Rao, K. G., & Rao, B. B. (2017). Enhancement of Shoulder-Surfing Resistant Graphical Password Scheme for Cloud using Caesar Cipher Technique. IJCSIS, 15(9).
16. Danish, A., Sharma, L., Varshney, H., & Khan, A. M. (2016, March). Alignment based graphical password authentication system. In 2016 3rd International Conference on Computing for Sustainable Global Development (INDIACom) (pp. 2950-2954). IEEE.
17. Shah, A., Ved, P., Deora, A., Jaiswal, A., & D'silva, M. (2015). Shoulder-surfing resistant graphical password system. Procedia Computer Science, 45, 477-484.
18. Bhand, A., Desale, V., Shirke, S., & Shirke, S. P. (2015, December). Enhancement of password authentication system using graphical images. In 2015 International Conference on Information Processing (ICIP) (pp. 217-219). IEEE.
19. Rodda, V., Kancherla, G. R., & Bobba, B. R. (2017). Shoulder-Surfing Resistant Graphical Password System for Cloud. International Journal of Applied Engineering Research, 12(16), 6091-6096.
20. Rao, K. G., Vijayakumari, R., & Rao, B. B. (2017). 4-STAGE GRAPHICAL PASSWORD AUTHENTICATION SCHEME FOR CLOUD. Journal of Theoretical & Applied Information Technology, 95(1).
21. Rao, M. K., Switha, T. U., & Naveen, S. (2016). A Novel Graphical Password Authentication Mechanism for Cloud Services. In Information Systems Design and Intelligent Applications (pp. 447-453). Springer, New Delhi.

AUTHORS PROFILE

R.Vijayakumari received M.Tech Degree in Computer Science and Engineering from Acharya Nagarjuna University, Guntur. She is pursuing Ph.D from Acharya Nagarjuna University. She is working presently as Assistant Professor in Department of Computer Science, Krishna University, Machilipatnam. She has published research papers in various National and International journals.

K. Gangadhara Rao received his Doctoral degree in Computer Science under faculty of Engineering in the year 2011 from Acharya Nagarjuna University. He did his M.Tech from Andhra University, Vishakhapatnam and B.Tech from Acharya Nagarjuna University. Currently he is working as Professor in Department of Computer Science and Engineering, Acharya Nagarjuna University. His areas of interest include Data Mining, Cloud Computing, Computer Networks and Software Engineering. He has published several papers in national and international journals.

B. Basaveswara Rao received his Doctoral degree in Computer Science under faculty of Engineering in the year 2010 from Acharya Nagarjuna University. He did his MCA from Madurai Kamaraj University in the year ---. Currently he is working as Web Administrator and System Programmer in the university Computer Centre, Acharya Nagarjuna University. His areas of interest include Data Mining, Cloud Computing, Computer Networks and Software Engineering. He has published several papers in national and international journals.

Table – 2: Analysis of proposed method

	Tipl	Ta	Tb	Tc	Tx	Cct	Cci
Client Side	4x+d	18x	168x	288x	240x	72 to 240 bits	30 bits
Server Side	4x	18x	168x	288x	240x		

Table – 3: Comparison of MGPASC with the other existing methods

	Multi-level	User friendliness	Memorization capacity of user	Resistant to guessing attack	Encryption of password	Complexity level of login procedure
Abutalha et al scheme [16]	NO	AVERAGE	HIGH	NO	NO	LOW
Amish Shah et al scheme[17]	NO	LOW	AVERAGE	YES	NO	AVERAGE

MK Rao et al scheme [21]	YES	AVERAGE	LOW	YES	NO	HIGH
Vijayakumari et al scheme [15]	NO	HIGH	AVERAGE	YES	NO	AVERAGE
MGPASC	YES	HIGH	AVERAGE	YES	YES	AVERAGE