ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

IJARCCE

International Journal of Advanced Research in Computer and Communication Engineering

ICRITCSA

M S Ramaiah Institute of Technology, Bangalore

Vol. 5, Special Issue 2, October 2016

A Reliable Authentication with Graphical Password for Cloud Data

Shivanna K[1], Dr. Prabhu Deva S[2]

Asst Professor, Computer Science and Engineering, G.M.I.T, Davanagere, India [1]

Professor, Information Science and Engineering, J.N.N.C.E, Shivamogga, India [2]

Abstract: In today's cloud computing technology, protecting data from unauthorized access is the major issue. The numerical passwords named as traditional authentication techniques are widely popular. The passwords consists of alphanumeric characters have their own drawbacks by shoulder surfing and dictionary attacks. To jump on such attacks, graphical passwords are implemented to make longer memorable and easy to use. In this paper, we will propose reliable authentication using graphical password for securing cloud data. We enable the platform for users to click on images as a password rather than group of alphanumeric character.

Keywords: Authentication, Cloud Computing, Graphical Password, Click Points.

1. INTRODUCTION AND RELATED WORK

Authentication is concerned with all aspect of accessing information by legitimate user through online by meanse of username and password. Security of the confidential information on shared data is major issue and it is based on how much that data is valuable. Password used for accessibility of data may be text or alphanumeric characters. But these passwords are difficult to memorize if it is larger in lenght and also vulnerable in shoulder surfing, dictionary attacks.

Recently many reseach work have proved that human brain can easily memorize the graphical password rather than other textual password and it is better solution for shoulder surfing. So the set of click points on pool of images are acts as a paasword to share resources in cloud computing.

In [1], the researcher have proposed a graphical password technique for authentication using pictures of ramdom tracks and this method does not require data base of larger number of images.

The random geometric graphical password(RGGPW) technique proposed by the auther is works againest to brute force and shoulder surfing attacks.

In [2], researchers have proposed a Yet Another Graphical Password technique. The model includes 48x64 grid for drawing secret images that enough to resist shoulder surfing. Due to fixing of threshold value of secret image, there is a drawback of redraw the earliar password.

In [3], multifactor authentication using graphical password have been described by author. It is a user friendly solution that includes two factor authentication. The model does not require lengthy password setup procedure and no need of security risk for lost of handheld devices.

In [6], author has presented ColorLogin password scheme that avaid the complexity and boring features of user community.
The model is efficient technique for shoulder surfing and uses the backgroud color to decrease login time. The author uses multiple colors to confuse the attacker but not the authenticated users.

In [8], researcher have proposed image authentication that addresses Pair and Text oriented, these techniques are implemented to access PIN number, account number from PDA.

In a pair based technique, user has to selects eight pairs of images from a pool of images in the system. So eight pair is equal to sixteen images and user has to select three key positions are randomly placed in a grid.

Ming-Huang Guo[9], proposes authentication mechanism for accessing cloud services in a secure manner using graphical password. Author has to feels that internet user can access cloud resources for that authentication is mandatory and done the comparative study with respect to the different attacks.

Abdul Rahim M [12], proposes a image based password authentication for accessing mail server securely.

Basically text and alphanumeric characters are used for authentication, which are vulnerable for various attacks. To overcome such limitations auther has to presented graphical user interface to remember passwords.

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

IJARCCE

International Journal of Advanced Research in Computer and Communication Engineering

ICRITCSA

M S Ramaiah Institute of Technology, Bangalore

Vol. 5, Special Issue 2, October 2016

2. PROPOSED SYSTEM

In this paper we can work on matching of original and predefined password. It means that both password have identical images as well click points.

In such a case, the authentication is completed successfully. Mismatching is also verified by checking passwords have identical images but any one click point is differ, it will be considered as a failure.

A. Algorithm for Registration Phase

To access the cloud services, user has to registrared with server has following steps:

i) User A has to run proposed model in his machine.

ii) User A has to enter his identity ID_A

ιιι) The system presents set of images(here it is five) and user A has to click (Xi ||Yj) points on each images, all images have its own serial number.

iv) Range of each image is calculated by A=(Xi || Yj)
where i=0, 1, 2, ...last pixel along X axis.
J=0, 1, 2,..... last pixel along Y axis.

v) At the end of calculating click points on each image, authentication server generates a password PW_A and compute PW_A= (Xi || Yj).

vi) The intended server stores PW_A and registration completes.

B. Algorithm for Login Phase

To access the cloud resource, registrared user has to login with following steps:

i) The registrared user A has to enter his identity ID_A to login page.

ii) The server shows set of images with serial number as it done in the registration.

iii) User A has to enter password PW_A as a click points (Xi ||Yj) on each image.

iv) The authentication server compare the entered password is same as password stored in the database. i.e

$$PW_{Anew}(Xi \,||Yj)= = PW_{Aold}(Xi \,||\, Yj).$$

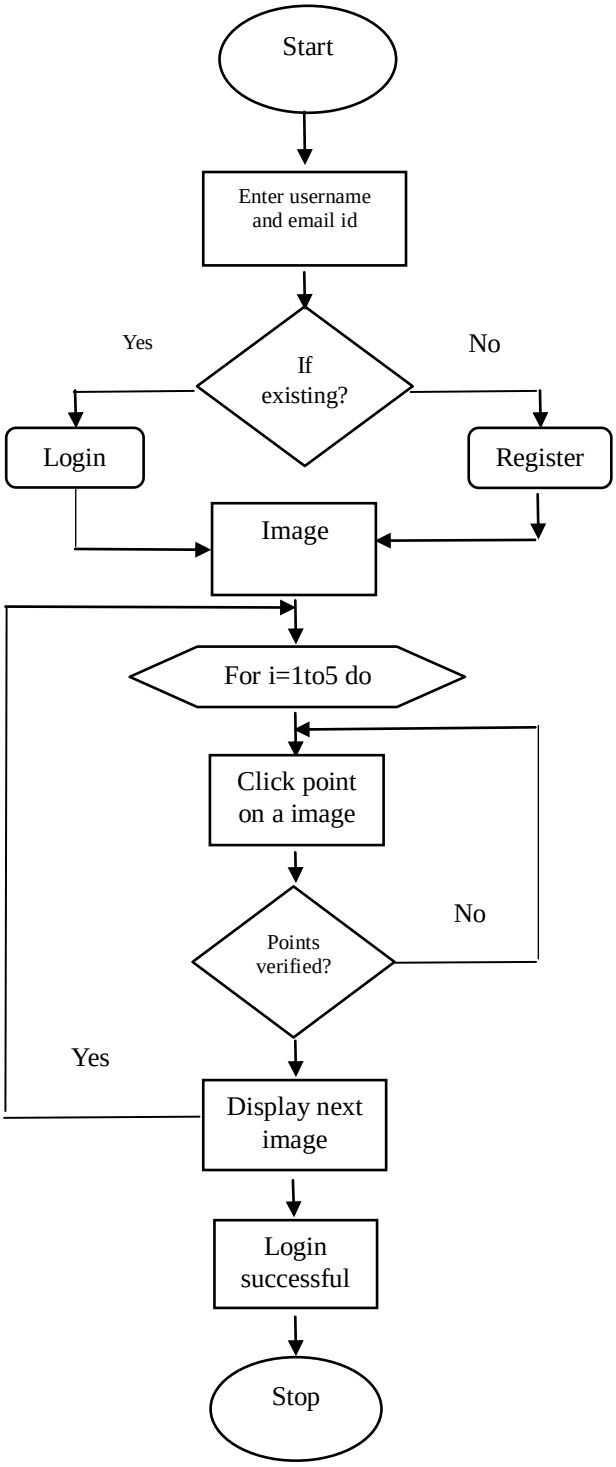
If it is true, login successful.

C. Algorithm for Password Recovery Phase

ι) If user A lost his password, it is recovered by entering his mail-id MID_A on the recovery page.

ii) The server matches mail-id is same as mail-id entered during registration. i.e $MID_{A\ new}$= = $MID_{A\ old}$, if it is true, server immediately sent password to intended user.

D. Flow Chart for Proposed System



3. RESULTS AND DISCUSSIONS

Fig. 1 shows the Login page for the user to login into account by entering their user name and email-id. If he is an existing user, click login button, otherwise he has to register by clicking sign up button.

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

IJARCCE

International Journal of Advanced Research in Computer and Communication Engineering

ICRITCSA

M S Ramaiah Institute of Technology, Bangalore

Vol. 5, Special Issue 2, October 2016

Fig.1.Login Interface

Fig. 2 describes registration page for the user. The user needs to enter the name, city, date of birth, contact number, email id. These data are stored in the database and every registration is given with a session id, which is unique for every user.

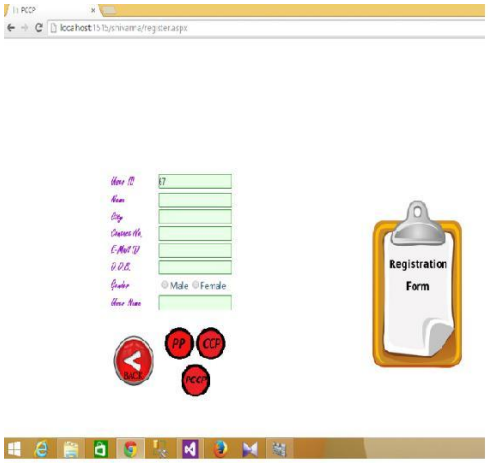


Fig .2.Registration Interface

Fig 3-7 illustrates the click point interface where it displays one image at a time and user need to click a point on an image.

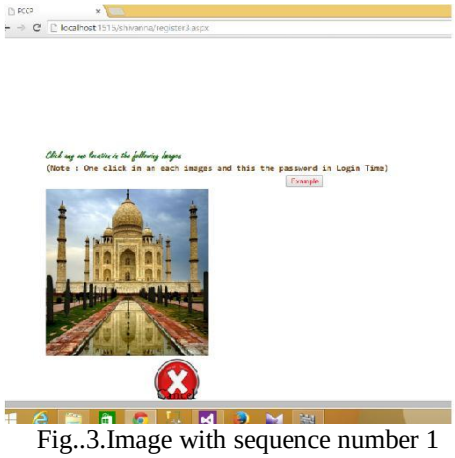


Fig..3.Image with sequence number 1

Next consecutive images are displayed sequentially and user has to click a consecutive points on each image illustrated below.

Fig.4. Image with sequence number 2

Fig.5. Image with sequence number 3

Fig.6. Image with sequence number 4

Fig.7. Image with sequence number 5

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

IJARCCE

International Journal of Advanced Research in Computer and Communication Engineering

ICRITCSA

M S Ramaiah Institute of Technology, Bangalore

Vol. 5, Special Issue 2, October 2016

Fig. 8 describes a file sharing interface, this allows the user to share the resources which they want to share with others. User has to share the file by providing name of the file and uploading the file.

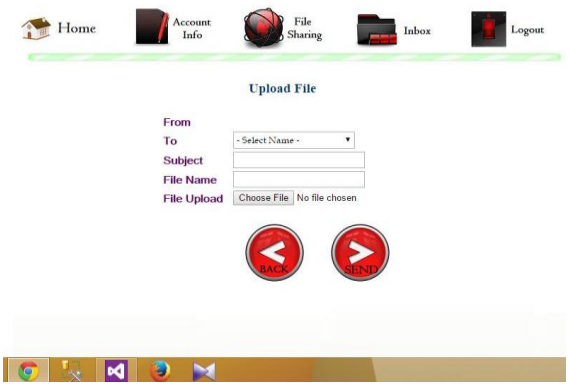


Fig.8.File sharing interface

Reliability is obtained by recovering the password if it lost from memory is shown in Fig 9. The system would ask the email-id of the person who lost his password. Peson will get the click points only after entering his name and unique code.

Fig.9.Password Recovery Page

4. CONCLUSION

Cloud computing is a vast area where mellions of user per day has to compute and manipulate the resources through internet. Security of resources stored in cloud is the major issue, because data and information are distributed on internet. As we sharing and accessing the resources in a cloud, an efficient authentication procedure is needed. In this paper, we have proposed cloud security by means of graphical password. By this we are trying to shows that set of click points on images ensures better authentication. The proposed model is implemented by ASP.NET as a coding language and C# as a interfacing tool.

REFERENCES

[1] Mithuna.R and Suguna.M, "Integrity Checking over Encrpted Cloud Data", IEEE 3rd International Conference on Signal Processing, Communication and Networking (ICSCN), 978-1-4673-6823-0/15, 2015.

[2] Haichang Gao, Xuewu Guo, Xiaoping Chen, Liming Wang and Xiyang Liu,"YAGP: Yet Another Graphical Password Strategy", IEEE Annual Computer Security Applications Conference, 1063-9527/08, 2008.

[3] Alireza Pirayesh Sabzevar and Angelos Stavrou, "Universal Multi-Factor Authentication Using Graphical Passwords", IEEE International Conference on Signal Image Technology and Internet

[4] Based Systems, 978-0-7695-3493-0/08, 2008.

[5] Kemal Bicakci, Nart Bedin Atalay, Mustafa Yuceel, Hakan Gurbaslar and Burak Erdeniz,"Towards Usable Solutions to Graphical Password Hotspot Problem", 33rd Annual IEEE International Computer Software and Applications Conference, 0730-3157/09, 2009.

[6] Madoka Hasegawa, Yuichi Tanaka and Shigeo Kato, " A Study on an Image Synthesis Method for Graphical Passwords", International Symposium on Intelligent Signal Processing and Communication Systems (ISPACS 2009) December 7-9, 978-1-4244-5016-9/09,2009.

[7] Haichang Gao, Xiyang Liu, Sidong Wang and Honggang Liu, "Design and Analysis of a Graphical Password Scheme", Fourth International Conference on Innovative Computing, Information and Control, 978-0-7695-3873-0/09, 2009.

[8] Wei Hu,Xiaoping Wu and Guoheng Wei, "The Security Analysis of Graphical Passwords", IEEE International Conference on Communications and Intelligence Information Security, 978-0-7695-4260-7/10, 2010

[9] M Sreelatha, M Shashi, M Roop Teja, M Rajashekar and K Sasank, "Intrusion Prevention by Image Based Authentication Techniques", IEEE International Conference on Recent Trends in Information Technology(ICRTIT), 978-1-4577-0590-8/11, 2011.

[10] Ming-Huang Guo, Horng-Twu Liaw, Li-Lin Hsiao and Chih-Yuan Huang, "Authentication Using Graphical Password in Cloud", IEEE International Conference, 2012.

[11] Mahmud Hasan and Kamruddin Md. Nur, " A Novel 3-Layer User Authentication System for Remote Accessibility", IEEE International Conference, 978-1-4673-4836-2/12, 2012.

[12] ShraddhaM. Gurav, Leena S. Gawade, Prathamey K. Rane and Nilesh R. Khochare, "Graphical Password Authentication",IEEE International Conference on Electronic Systems, Signal Processing and Computing Technologies, 978-1-4799-2102-7/14, 2014.

[13] Abdul Rahim M and Anandhavalli, " Implementation of Image Based Authentication to Ensure the Security of Mail Server ", IEEE International Conference on Advanced Communication Control and Computing Technologies (ICACCCT), 978-1-4799-3914-5/14, 2014.

[14] Abrar Ullah, Hannan Xiao, Trevor Barker and Mariana Lilley, "Graphical and Text Based Challenge Questions for Secure and Usable Authentication in Online Examinations", IEEE 9th International Conference for Internet Technology and Secured Transactions(ICITST), 978-1-908320-39/1, 2014.

[15] Rosanne English and Ron Poet, "Measuring the Revised Guessability of Graphical Passwords", IEEE International Conference, 978-1-4577-0460-4/11, 2011.