Scholars Journal of Engineering and Technology (SJET) **ISSN 2321-435X**
Sch. J. Eng. Tech., 2013; 1(4):191-194

(An International Publisher for Academic and Scientific Resources)
www.saspublisher.com

Research Article

Hybrid Scheme: Two Factor Authentication using Graphical password with Pass point scheme in Cloud computing

Harmeet Kaur*[1], Dr. RK Bansal[2]
[1]M.Phil (CA) Department of Computer Application Guru Kashi University, Talwandi Sabo (Bathinda) Punjab [2]Dean, Research of Guru Kashi University, Talwandi Sabo (Bathinda) Punjab.

***Corresponding author**
Harmeet Kaur
Email: hammywarraich@yahoo.com

Abstract: Cloud Computing is a completely new concept in the research area. Cloud computing focuses new challenging security threat. Hacking and data leakage are the common threats in cloud computing. As the security due to hackers increase over internet and the cloud computing is totally on internet. At this time, cloud computing demand the tight password protection and strong authentication and authorization procedure. We proposed a new strong authentication model named "Two factor authentications using graphical password with pass point scheme". Therefore, our authentication security scheme must solve the most security challenges of cloud computing.
Keywords: Cloud computing**,** login, Authentication, Recognition, Recall, Pass point, Cloud Provider, Service, Two Factor Authentication , security

INTRODUCTION

Cloud computing gets its name as a symbol for the Internet. Typically, the Internet is represented in network diagrams as a cloud. Cloud computing promises to cut operational and capital costs and, more importantly, Cloud technology provides computation, software, data access, and storage services that do not require end-user knowledge of the physical location and configuration of the system that delivers the services [1].

Passwords provide security mechanism for authentication and protection services against unwanted access to resources. I have proposed a new graphical password based system in the cloud computing. This system is based on recognition technique and pure recall based technique and that offers many advantages over the existing systems and may be more convenient for the user. In recognition technique a set of images is presented to a user from the cloud provider and the user is recognized and identified the images he selected during the registration stage. In recall based technique a user is to reproduce something that he created or selected earlier during the registration stage. Our scheme is proposed for smart devices (like smart phones i.e. PDAs, iPod, iphones, laptops and desktop computer systems etc) which are using the cloud services [2].

Authentication is generally used to represent both identification and authentication, and access control is used for authorization. It is the process of identifying the user to verify whether he/she is what he/she claims to be. Normally, identification is done with the help of information that is known to everyone (i.e., user name or user ID) and some personal information known only to the subject (i.e. password). But most organizations do not depend on user name authentication alone since username and passwords are an authentication solution for low-value transactions. Usernames and passwords provide relatively weak authentication because they can often be guessed or stolen [3].

So we present a hybrid scheme: Two Factor Authentication using Graphical password with Pass point scheme in Cloud computing. Our authentication model is used two factor authentication type. It is a combination of two techniques such as recognition technique and pure recall based technique. Then it uses the Pass Point Scheme, which comes under the recall based technique.

EXPERIMENTAL

Two Factor Authentications

Two factor authentications enable users to secure their logins and transactions. The two-factor system of authentication provides a much greater security shield against phishing and identifies theft. There are many two-factor authentication solutions on the market today, but for thousands of organizations worldwide[4].

How It's Work

First, users type in their usernames and passwords as usual. If primary authentication succeeds, then you enter the secondary authentication they are offered a choice of authentication method. It allowing users to

authenticate with whatever method is best for them such as use pin code, ID card and smart card etc. Then user login securely [5].

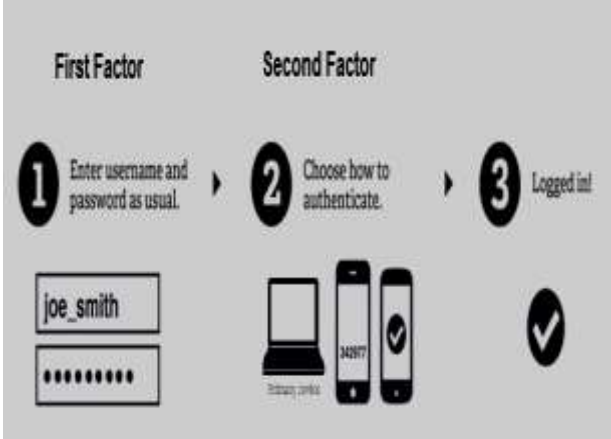

Figure 1: Working With Two Factor Authentication

Here we present image based and graphical password with the help of pass point scheme in the second factor. It provides the more tight security to user.

Pass Point Scheme

We used the recall based technique. In this technique user is asked to reproduce something that he created or selected earlier during the registration stage. This technique provides many types of authentication schemes such as Draw-A-Secret (DAS) Scheme, Pass Point Scheme and Grid Selection Scheme etc. I pick up the pass point scheme for our authentication procedure, which is used with two factor authentication. In pass point scheme user click on any place on an image to create a password. A tolerance around each chosen pixel is calculated. In order to be authenticated, user must click within the tolerances in correct sequence [6].

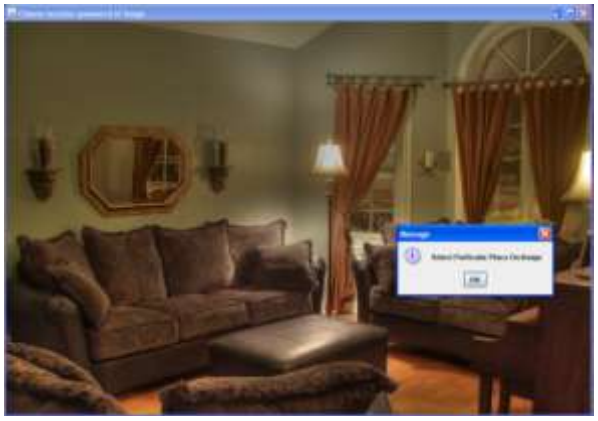

Figure 2: Using Pass Point Scheme

Pass point is based on the number of pixels or smallest units of a picture. In this technique the numbers of pixels are calculated as the password. It is hard to remember the specific location of the picture that provides the strong security.

Proposed Graphical Password authentication Model

The proposed graphical password authentication model used three-level defence system structure:-primary password authentication, graphical authentication and authentication with pass point technique. Show figure 3.

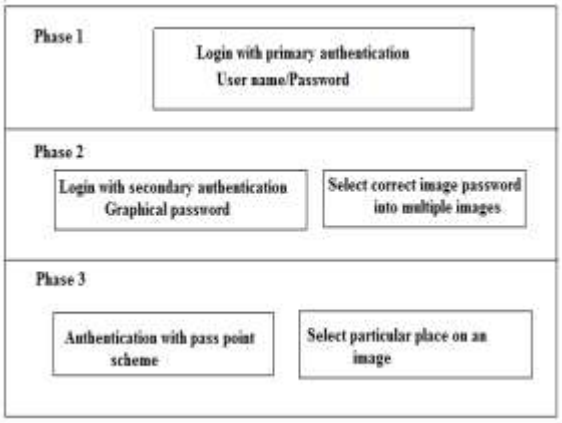

Figure 3: Proposed Graphical password authentication model in cloud computing

The first phase:

Primary authentication is achieved by using user name and password.

The second phase:

In graphical authentication we can say it secondary authentication, multiple images shows. Select a correct image, which is selected by you as a password.

The third phase:

It includes the pass point scheme authentication. If you select correct image as a password. Now click on particular place into that image which is your password. If you select the correct location you login successfully.

EVALUATION OF GRAPHICAL PASSWORD IN CLOUD ENVIORNMENT

The cloud user select company for cloud using which company provide better facilities to the users. Then create an account. Cloud provider upload user information in DB in cloud storage. Cloud Provider confirms user with his username and password. Then cloud user registers his image password and pass point scheme password. [7] Cloud provider uploads his information into the cloud database storage. When a cloud user requests his data, cloud provider provides him login page. User authenticates with the graphical password authentication scheme. The proposed graphical password authentication will work as follows.

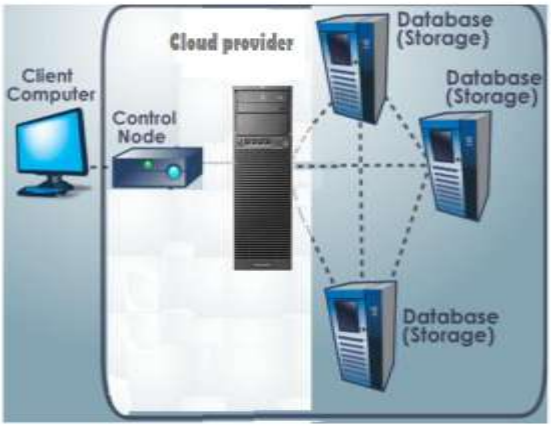

Figure 4: How Data Stored In The Cloud By Cloud Provider

Here we describe the authentication steps:-

In first phase, Authentication: -This is password based or primary authentication.

1. Cloud user request login page
2. The cloud provider displays login screen
3. Cloud user login with username and password
4. A cloud provider check is valid username and password by searching in DB in cloud storage.
5. If user information not valid display error message else display second phase of authentication.

In second phase authentication steps: Then user enters the graphical password authentication.

1. Cloud provider displays graphical login screen, in which multiple images showed.
2. The cloud user chooses his password image into the multiple images.
3. A cloud provider check is valid graphical image by searching in DB in cloud storage. If user image is not valid display error message else display the full image.
4. Then user clicks on the specific place (location) on the image.
5. Cloud provider check is valid graphical image location password by searching in DB in cloud storage.
6. If user password is valid you will successfully authenticated with cloud server. Otherwise display error message

Flow Chart of Graphical Password Scheme

The following flow chart describe the procedure of Graphical password authentication with pass point scheme:-

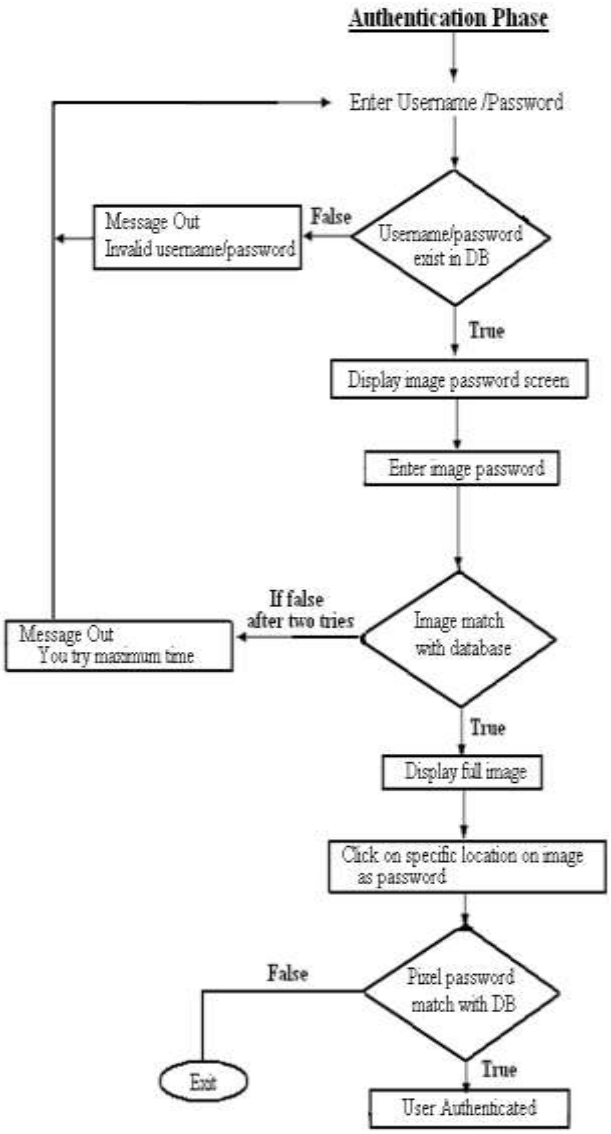

Figure 5: Flow chart of Graphical password authentication scheme

REFRENCES

1. Bhavana A, Alekhya V, Deepak K., Sreenivas V; Password Authentication System (PAS) for Cloud Environment. International Journal of Advanced Computer Science and Information Technology, 2013; 2(129-33.
2. Ray PP; Ray's Scheme: Graphical Password Based Hybrid Authentication System for Smart Hand Held Devices. Journal of Information Engineering and Applications, 2012; 2(.2):1-11.
3. Asha M; Security And Privacy Issues Of Cloud Computing; Solutions And Secure Framework" International Journal of Multidisciplinary Research, 2012; 2(4):182-193.
4. Available online at http://www.entrust.com/two-factor.html

5. Available online at https://www.duosecurity.com/product
6. Bhargavi M; Graphical password Authentication, Available online at www.slideshare.net/akhilrocker143/558-11294069
7. Eman MM, Abdelkader HS; Data Security Model for Cloud Computing. The Government of Egypt, 2013 Used by permission to IARIA. ICN 2013: The Twelfth International Conference on Networks, 2013: 64-74.