# A Study on Graphical Password Authentication in Cloud Computing

**S. Kaushal[1*], Dr. B. Buksh[2]**
[1*]Computer Science Engineering, Ludhiana Group of Colleges, Ludhiana, India
[2] Computer Science Engineering, R N Engineering College, Kota, Rajasthan, India

***Abstract— Nowadays, Cloud computing, is the main and hottest topic in IT world, has tense large attention. lots of IT companies such as Google, Microsoft, flip kart, Amazon and many more dynamically expand cloud computing systems and associated products to customers. The coming out of modern ubiquitous IT (such as cloud computing, grid computing etc.) increases the handling of web services. All the web service providers use user's delicate information; (such as password, name) to authenticate the user .on the other hand these web service providers use different methods and tools to secure the user information. Moreover the security methods used by web services is not enough to provide security to the user data, spiteful attackers attack user personal information and successfully steal the information such as password, authentication user id, certificate id etc through keyboard hooking. This paper represents the authentication set to cloud by using the graphical password and protected password input method using authentication pattern and puzzle. The proposed password input method is based on entering the password using with mouse.***

***Keywords— cloud computing, authentication, graphical password, pattern, puzzle***

## I. INTRODUCTION

Many Researches have shown that the security of the data has really significant aspect of value service: While cloud computing offers latest dimensions in data service, its approach to data storage and managing security issues for individuals companies allowing for making use of cloud facilities. By using a public host server all the time was a threat to business, whether it is by a database management system on the host or a file system provided by the operating system of the server. Cloud computing makes in performance field bigger and traverses general boundaries, apparently transporting a company's data further out of its control. The objective of the cloud organization provider is to make use of the resources successfully and finish the most extreme benefits. The Users computer may include very few software or data, serving as an essential display terminal connected to the Internet. yet as the cloud is the fundamental release means cloud in which application and services might support any form of software application or examine in use nowadays

The major concerns in cloud computing be the chance of invasion of confidentiality Invasion may be either Intentional or unintended Staff and the cloud server can influence or reveal a company's private information. Such harm to the company's status and wealth as a result in order to prevent attack of privacy, consumers of cloud services might choice to information encryption. though encryption in securing data sooner than getting stored in service is efficient other than it cannot be practical in services processing data for the reason that unencrypted data should be executed in host memory and it is probable that a part of computing process leftovers in the host memory [1].

Anyone requests to access the network, for the security purposes only each and every web application provides individual user authentication. From past day's private data or code is used for hiding and provide security to crucial information. In user authentication process we need to pass through password and username. To authenticate the process is separated into Token based authentication, biometric based and information based authentication. The major part of the net application gives information based confirmation which has alphanumeric code word while as graphical password. In current scenario changing the world as we are having measure of networks and private version some sort of trouble-free authentication [5] scheme have to to be provided.

In adding together current spotlight introduces Shoulder-Surfing-Attack (SSA). The attack method is such that, the attackers monitor what type of data user enters above the shoulder of the user and remember it. Shoulder-surfing-attack is known as high risk .high risk attack hijacking confidential information. Contradict trial against SSA was proposed by Zhao et al. (S3PAS) [2], KISA (SecurePass) [3], Wiedenbeck (Convex hull click) scheme [4].The paper is about how we securing cloud by using the graphical password. In this paper, a security mechanism based on Password authentication is proposed for protecting clouds security, which can monitor confidential and highly confidential data.
Rest of the paper is organized as follows.

## II. RELATED WORK

A. Figure Based Scheme

Image-based schemes use images contain artificial pictures, photo graphics, or any other kind of the images as background. Based on the numeral of images displayed, we can further divide the image-based schemes into two subclasses:
Single-image schemes and multiple-image schemes.[6]

1) Single-image based: Single-image based schemes, only image is provided to client they have to select the particular points.

2) Multiple-image based: In many –image scheme number of images will provide to client they must have to select one or more than one.

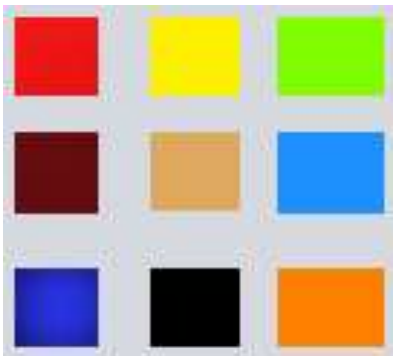

Figure 1

Figure 2

3) Advantages

- Client can easily remember the password as it given in images.

4) Disadvantages

- Figure based password is very long process user include to pass through the selection of digit of images.
- It consumes user's time also

B) Triangle scheme

In this user is provided with rounded surface. Users have to pick the points from that forming exacting triangle.

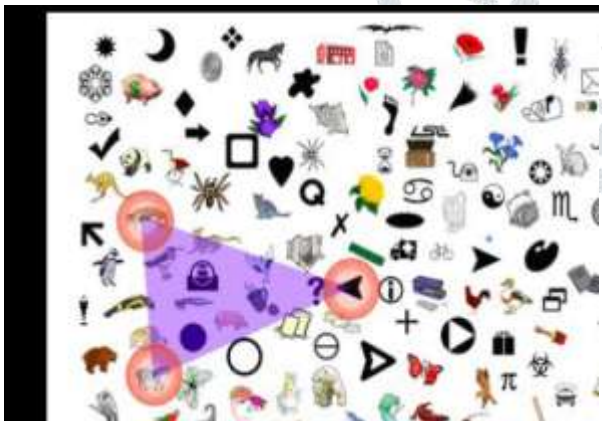

Figure 3

Advantages

- In this system the display is very crowded so not able to guess the password.
- Numbers of images shown are almost the same, it is difficult to distinguish.

2) Disadvantages

- As it has rounded surface assigning process takes longer time and number of attempts.

*C.* Hybrid textual authentication

In hybrid scheme user have to rate the number so is simply to find the particular color sequence and have to remember that.

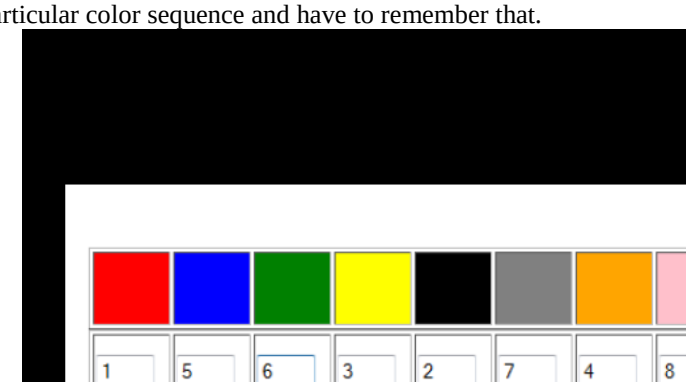


Figure 4

1) Advantages

- In this process colors are already given client only have to remember the rating.
- Very easy to assign no special algorithm is used.

2) Disadvantages

- It is somewhat difficult to remember colors with series

D) Grid based scheme

In this scheme graphical password is at grid background.

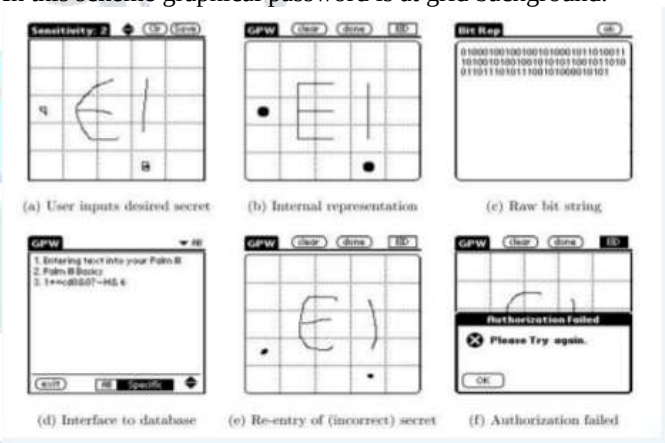


Figure 5

1) Advantages

- There no need to store graphical database at the server side.
- Grid is straightforward object there are no extra displays are needed.

2) Disadvantages

- During confirmation the sequence can be changed or grids may be different as it is a drawing.

E) Signature based scheme

In this scheme user signature is used for key which is mentioned in scheme.

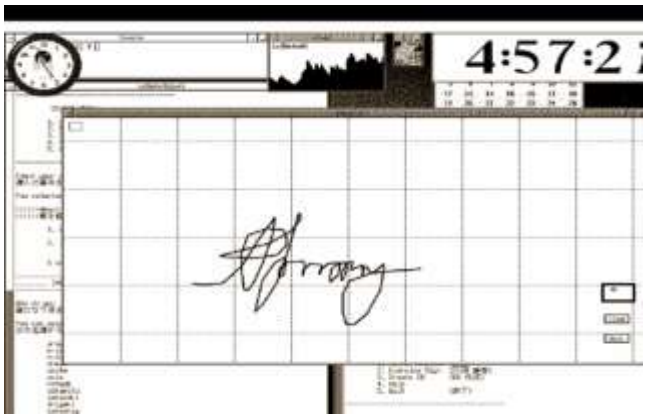

Figure 6

1) Advantages

- Signature of anyone cannot be copied as it is.
- Little mistake in signature can without the access.

2) Disadvantages

- Remembering the grid of signature is not a simple task.

## III. PROBLEM FORMULATION

Cloud computing is a recent advancement in IT infrastructure and applications are provided to users as "services". Cloud computing needs to address three main security issues: confidentiality, integrity plus availability. It offers scalability, availability and different services as important benefits. But as this new technology expanding it also discovers new risks and vulnerabilities too. In spite of reality that various structures and cloud services are growing, the perception of cloud computing has not been visualized. In the main necessities the meaning of cloud computing is to access and store the information and programs that all over the internet that instead of that we use own hard drive. Consumers are using cloud services to avoid IT infrastructure purchasing and maintenance cost. Business-critical data requires protection and continuous monitoring of its access. A large amount of data can be stored on the cloud. If the information moves to a cloud model further than an on idea personal cloud, clients could lose supreme control of their responsive data. So, the data security is always the main challenging threat for excellence of services and it also stops the users to adopt cloud services. In cloud storage, all kinds of data are stored on servers through two storage methods. The first method is to store data on servers without encryption. The second method is to encrypt the received data and store them on cloud servers. These methods of data storage can face the issue of data confidentiality. In a cloud environment, a clients information are stored on inaccessible servers that are not actually known by the user and there is at all times the high probability of confidentiality leakage. This paper basically focuses on the threat of confidentiality of data when it is stored on a cloud. When a dataset is being stored to cloud, it passes through a security mechanism, such as data encryption without understanding the needs of data or directly being stored on servers without encryption. All data have different kinds of sensitivity levels. So, storing data interested in a cloud without understanding its security requirements is not a valid and technical approach

In this learning various security aspects of security issues have been analyzed and then will propose a framework to mitigate security issues at the level authentication and storage level in cloud computing. Efficient security mechanisms should be deployed by means of encryption, authentication, and authorization or by some other method to ensure the privacy of consumer's data on cloud storage.

- Confidentiality: This incorporates two primary ideas: Data Confidentiality which alludes that staff or private data of client in the cloud should not be unveiled to unapproved client. Security includes individual control implies what data is gathered and who can see this data.
- Integrity: A loss of integrity means complete loss of unique of data. Moreover, integrity can be an information integrity and system integrity
- Availability: It says that reliable and timely access is vital factor. However, a loss of availability means the loss of data access.

## IV. PROPOSED WORK

### I) How we start

When the person is going to start the cloud service they will be provided with many of options that he has to select. For login the user has to go by the authentication process. In which they have to enter the username, the process will be ongoing at the server-side. The set of images which will be given to the user are based on product of calculation.

USERNAME Jklmn

### II) Calculations on the basis of username

At the server-end site of username's alphabet in the alphabet series will be calculated. Then totaling of all the positions is done. The initial number of that sum will be used for further calculations.

Table 1: Finding the set to be assigned

| □□□□□□□□ | □ | K | L | M | N |
|---|---|---|---|---|---|
| □□□□□□□□ | □□ | □□ | □□ | □□ | □□ |

**Calculation of result: J+K+L+M+N=1+2+3+4+5=15**

This first digit is 1, forwarded for next calculation.

### III) Assigning place of images

There are full 26 alphabets in alphabet series. We know that every two digits number must start with number 1-9 them. The server has previously made place of images. Set of images willpower be assigned according to outcome of calculation which server has acquire at the second step. 1-9 numbers will be assigned to that sets be shown:

Table 2

| J | K | L | M | N | O | P | Q | R |
|---|---|---|---|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |

This means that what ifthe very first digit is 1,then assigned place to it will set of J . If the first digit is 2, then set assigned to it will be K.

D. Selection of password

In this absolute password is separated in two sections initial is based on user selection and the second is based on server provided sets of images. For the user selection, from identified set of images user has

to select two images as the password. From the sever side two images will be given to user to form full password.

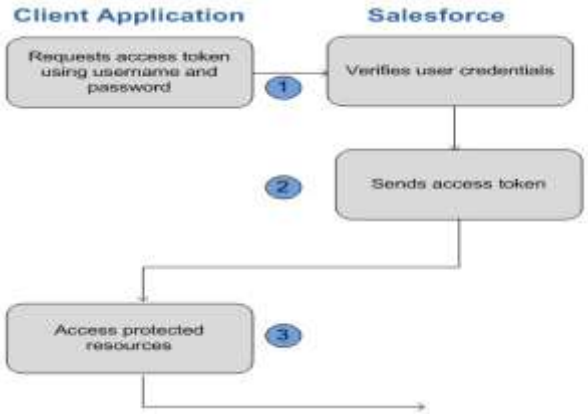


Figure 7

**SECURITY ANALYSIS**

A. Keyboard hooking

Keyboard hooking is a technique of hacking anywhere client entered data using keyboard between the user and system. At the time as attacking, attackers cut off user's vital information. We suggest a puzzle based password input scheme using mouse to enter the password, where, puzzle pixels consist of an image. This scheme will protect user's password picture while the user enter the password by mouse and user's password proxy puzzle matrix inside value. Proposed password input method protected keyboard hooking, as we are via mouse click and password substitute inside value.

B. Shoulder Surfing Attack

SSA is a method of attack, where, attackers steal through a password incoming moment by a user, and remember the password. It is recognized to be extremely dangerous hacking practice hence, various researchers' proposed special methods to protect SSA. Several such examples are S3PAS, secure pass convex hull click scheme etc. But, convex hull click scheme and S3PAS posses a only some risk against crossroads attack using SSA. However, the proposed scheme also poses a number of risks of SSA using crossroads attack. To stop this, a reissue of the authentication pattern for an exacting period is required.

*C.* Replay Attack

In this replay attack, the attackers interrupt a past session user authentication data and try to reuse it. User authentication pattern in the login phase is applicable for one login session. Every session arrange new 6 matrix puzzle at random with unusual mapping for the puzzle image. The puzzles have main 4 direction group freedoms, and in every session, here is special prototype for the puzzle image. Thus puzzle properties influence the password incoming method to user's puzzle pattern, and this type of properties influence a user entering puzzle pattern is unusual to the earlier entered pattern. so the opportunity of same patterns is very small and the replay attack is hard

**Flowchart of the proposed system**

In this process when some user aims to access the cloud services they will have two options sign in and login. At the server end computation login is made for client .client must have to enter the username which is based on that exacting image set which will be given to them on the origin of the algorithm. In the algorithm firstly the username is checked. After every calculation of the set of images will be done is offer to client .client has to choose two images one is on the client end and other on server end selection. So that complete password will be stored in the database of server. In login in the user have to provide username which he or she has specified during sign in and choose the password from the specified set of images. Validation of client is done next cloud access is given to particular client They access their account downloading and uploading facility.

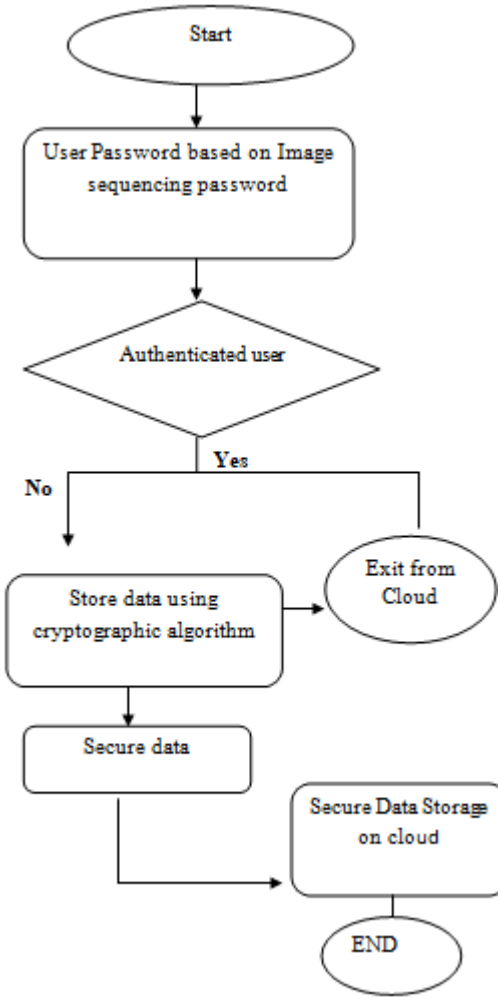


Figure 8: Flowchart of Proposed Technique

**Comparison with other methods**

- The Main problem is that if one user has more than one account, to memorize all those passwords, is just not possible.
- In several of the case it might happen that the person forgets the password when there is no everyday use of that account.
- If we provide the simple code word can also be a solution, but they are easily hacked. So there has to be a little technique for security. Password can be provided by multiple ways, but there are different drawbacks of that which can be strike by graphical password.[1][2]
- Most of up to date authentication scheme enclose username and password of minimum eight characters so it ensue to too large to remember.[3]
- Why we prefer the graphical secret word for cloud protection

Graphical password provides extra security than alphanumeric password. Most of the alphanumeric authentication chooses a plain

text or simple password to avoid the confusion. Whenever you like we confirm the alphanumeric password there is various hint option provided, with this hackers can simply gain entry to the system in less time. Mainly the system provides figure that is related to password i.e. graphical password. In this method images that you selected are used, user can have further number of images on every one page and among this entire password is chosen. Images are special for each case, so if hackers try to equivalent they each combination to locate the correct password it will take millions of year. In alphanumeric key eight typeset secret word is needed to expand entry of particular system, but in graphical key user have to select the images that in front of him/her and confirm the password. Whenever consumer pass during the authentication process it is very easy to remember images what they have chosen previously. Graphical password is enclose more memorable password than alphanumeric password which are able to reduce the burden on mind of user [4]

**REFERENCES**

[1] F. J. Krautheim, D. S. Phatak, and A. T. Sherman, "Introducing the Trusted Virtual Environment Module: A New Mechanism for Rooting Trust in Cloud Computing," TRUST **2010**, LNCS 6101,

2. H. Zhao amd X. Li, "S3PAS: A scalable shoulder-surfing resistant textual graphical password authentication scheme," Proceedings of the 21st IEEE International Conference on Advanced Information Networking and Applications Workshops, vol. **2**, Pp. **467-472**, May **2007**.

[3] KISA(Korea Internet Security Agency), "SecurePass", "http://news.donga.com/3/all/20100415/27578455/1", **2010**.4

[4] S. Wiedenbeck, J. Waters, L. Sobrado and J. Birget, "Design and evaluation of a shoulder-surfing resistant graphical password scheme", Proceedings of the Advanced Visual Interfaces, pp. **177-184**, **May 2006**.

[5] N. Santos, K. P. Gummandi, and R. Rodrigues, "Towards Trusted Cloud Computing," Workshop on Hot Topics in Cloud Computing, San Diego, CA,**2009.**

[6] Pass-Go, a New Graphical Password Scheme,HAITAOThesis submitted to the Faculty of Graduate and Postdoctoral Studies Electrical and Computer Engineering University of Ottawa© Hai Tao, Ottawa,Canada, June, **2006**

[7]Graphical Passwords,FABIAN MONROSE AND MICHAEL K. REITER, August 5, **2005**

[8] A Survey on Recognition-Based Graphical User Authentication Algorithms

[9] Authentication Using Graphical Passwords: Effects of Tolerance and Image Choice Susan Wiedenbeck Jim Waters College of IST Drexel University Philadelphia

[10] Design and Evaluation of a Shoulder-Surfing Resistant Graphical Password Scheme Susan Wiedenbeck and Jim Waters College of IST Drexel University Philadelphia, PA 19104 USA

[11] Graphical Passwords as Browser Extension: Implementation and Usability Study1,Kema Bicakci1, Mustafa Yuceel1, Burak Erdeniz2, Hakan Gurbaslar2, NartBedin Atalay3