# A NOVEL GRAPHICAL PASSWORD APPROACH FOR ACCESSING CLOUD & DATA VERIFICATION

## Rupal Rawat[1], Sreeja Nair[2]

[1]M.Tech (CSE), Oriental college of science & Technology, Bhopal, Affiliated to RGPV, Bhopal, M.P, India
[2] Head of the Department (CSE) in Oriental College of science & Technology, Bhopal. Affiliated to RGPV Bhopal, M.P, India

## Abstract

*Cloud & its unique authentication schemes are questions to improve its strength & usability to provide a data security to user, it is an emerging, a fast reaching technique for user to access their data at anytime from anywhere and people count is increasing to use cloud access, password technique is always a issue in today's world where a secure scheme & research are going onto this , in order to improve better user experience . In this paper we are going to present a new technique for the password which is GUI based and never introduced before & it is assume to be proven best experimentally & to increase user experience. Also here we are using it onto the cloud & then on cloud we are enhancing the file checking scheme for the user point of view, that user can assure about its data onto the cloud.*

*Keywords: Graphical password, Security, Cloud Access, Secure cloud authentication, Secure Data verification.*

-----------------------------------------------------------------***-------------------------------------------------------------------

## 1. INTRODUCTION

In a Network, we have various issues to work with our services & data(maintenances) & today Cloud computing provides convenient on-demand network access to a shared pool of configurable computing resources. The resources can be rapidly deployed with great efficiency and minimal management overhead. Cloud is an insecure computing platform from the view point of the cloud users, the system must design mechanisms that not only protect sensitive information by enabling computations with encrypted data, but also protect users from malicious behaviours by enabling the validation of the computation result along with an effective authentication mechanism to the user, from the past timing we have a various scheme to authorize any interface- here also in order to access a cloud we use textual password which is not much secure in terms of authentication because textual password might be easy to guess & lot of brute force attack has been already done on textual based attack in current world so that still here we are finding an efficient way where we can get a reliable authentication to correct user, one of the  way which we got is object password or graphical password to authenticate interface which we have described in existing system.

We propose a technique for authenticating cloud which is advance authentication scheme in terms of graphical password at the same time we are going to propose this scheme for using in cloud & in cloud how we can verify the data integrity which we are storing. It is high-speed data verification scheme with minimal loss probability. The proposed approach is highly efficient in order to authenticate in proper manner in order to maintain login security & after authentication again to verify our data integrity correctly.

Organisations today are increasingly looking towards Cloud Computing as a new revolutionary technology promising to cut the cost of development and maintenance and still achieve highly reliable and elastic services. The Cloud technology is a growing trend and is still undergoing lots of experiments. Cloud promises huge cost benefits, agility and scalability to the business. All business data and software are stored on servers at a remote location referred to as Data centres. Data centre environment allows enterprises to run applications faster, with easier manageability and less maintenance effort, and more rapidly scale resources (e.g. servers, storage, and networking) to meet fluctuating business needs. A data centre in cloud environment holds information that end-users would more traditionally have stored on their computers. This raise concerns regarding user privacy protection because users must keep secure data. So, our proposed system fulfils the above requirement of user. With the help of this system user can access the cloud services with proper authentication and he can also check the integrity of his data stored at cloud.

## 2. RESEARCH FINDING

Here as we have described about our work – mainly our contribution will be for the cloud security solution in two ways-

1. First most to authenticate in order to connect user with the services of cloud account with the help of proposed authentication scheme.
2. Second once the user is connected securely again user should be get assure about the security of data which kept into the cloud, so here we are providing a data verification technique to check data integrity.

Firstly getting authentication via our effective password scheme & then verifying the data integrity with the procedure demonstrated in image.

## 2.1 Problem Identification

In current all the schemes user has to remember multiple images, which might be not easy to remember, there is a chance sometime that user can't recall all the images which user registered.

1. Current password scheme like textual password are sometime easy to remember & sometime they face the problem of brute force attack or robot attack.
2. Basic image password is hard to remember sometime as it has to be chosen by the user and a set of images need to remember.
3. Using over cloud is probably not been developed by any other CSP due to above reason.

## 2.2 Proposed Work Plan

The proposed scheme consists of three procedures, we are defining below-

1. We are going to demonstrate effective graphical password authentication scheme in order to authenticate the cloud.
2. Generating a automated system to generate a key in order to calculate file verification factor (Fcf).
3. File verification at receiver end or on request for data integrity verification.

Finally we are going to verify level of security in terms of – method name & procedure, ease of use, Advantages & Disadvantages.

## 2.3 Our System and Assumptions

The secure integrity verification cloud computing storage model on giving a solution to authenticate it, considered in this work consists of three main components:

(i)   Creating & implementing a new Graphical authentication scheme to the cloud

(ii)  a CSP who manages cloud servers and provides paid storage space on its infrastructure to store the owner's files; and

(iii) Graphically giving access to authorized users — a set of owner's clients who have the right to access the remote data. Cloud computing data storage system model. The storage model used in this work can be adopted by many practical applications. For example, in e-health applications, a trusted government organization can be considered as the data owner, and the physicians as the authorized users who have the right to access the patients' medical history stored on cloud servers.

The integrity of customer's data in the cloud may be at risk due to the following reasons. First, the CSP – whose goal is likely to make a profit and maintain a reputation – has an incentive to hide data loss (caused by incidents like hardware failure, management errors, malicious attacks) or reclaim storage by discarding data that has not been or is rarely accessed. Second, a dishonest CSP may store fewer copies than what has been agreed upon in the service contact with the data owner. The authentication process is required to be considered at it best in order to get a proper authorization to proper user and give a best security level password scheme to compete its other competitor to provide best services.

## 3. LITERATURE REVIEW

Here we are mentioning the literature review the work which have already done in the field of image password- Shraddha M. Et al.[1] proposed a new system to authenticate a user for accessing the cloud services. In their proposed system for accessing cloud services user has to enter a alphabetical password of four letters, on the addition of digits assign to the letters the first digit is selected and the image subset is fetched from where user has to select two images as password. Two images are appended to the images select by user by the server. The combination of all the four images is the complete password for accessing the cloud services.

Fawaz A. Alsulaiman and Abdulmotaleb El Saddik [2] proposed a paper, in this paper a new approach to authenticate the user is described which is the 3D password scheme for securing the access only to the authentic user. In this paper, they present a 3D password authentication scheme in which while entering the password user interacts with a 3D virtual environment. The 3D password is a multifactor authentication scheme in which user interacts with a virtual 3D environment and interacts with number of objects present in that environment. User will select some of objects of his choice and the sequence of objects is the password for accessing the particular service.

Ms. Vidya Mhaske-Dhamdhere et al. [3] proposed a new technique for authentication. In their system user navigates through a virtual 3D environment and select some objects present in the environment which constitutes the password for authentication. This scheme is much more user friendly as user interacts with the environment which is similar to the real world system.

Rajkumar Chalse et al. [4] proposed a technique to check or verify the integrity of data stored at cloud. In their work they explained in cloud data storage system, users store their data in the cloud and no longer possess the data locally. To check the integrity of the data stored at cloud a tag is generated from the data and will be compared with the tag from the downloaded data. If the value of the tag is similar then the integrity of the data is maintained otherwise it is compromised. Thus, storage of files on the distributed cloud servers must be guarantee the correctness and availability of the data files and also there is no unauthorized data modification.

Issa M. Khalil et al. [5] provides comprehensive study of cloud computing security which includes the dependency level within classification and also provide a solution to solve the problem in form of preventive actions instead of

proactive actions. They have identified 46 issues related with cloud computing security. These issues have further been categorized into six classes that form a comprehensive classification.

Dinesha H A and Dr.V.K Agrawal [6]    proposed new multilevel password generation technique. According to this technique, a multi-dimensional password is used to access the cloud. So many parameters are considered to generate the multidimensional password such as: vendor details, consumer details, services, privileges etc. These various input dimension forms the password. They also describe Probability of Breaking Multi-dimensional Authentication.
Ms. Sneha Vasant Thakare et al. [7] proposed a technique for security of cloud system using graphical password. They explains that there are many security issues  for accessing services in cloud. To overcome from these issues the 3D security system is provided with powerful and more secure authentication techniques. This system can be used to categories the files or confidential data on cloud. Categorization depends on 3 important factors: Confidentiality, Integrity and Availability. There are three protection rings from the files to be uploaded has to pass. From these three rings the innermost is more powerful & secure.    Revised- CIA algorithm is used for file categorization. The file which is to be uploaded is divided in three rings. The uppermost ring uses 3D password, the middle one uses Graphical password and the innermost ring uses the PCCP (Persuasive clued click point).

Till now the work up to this level has been done, which has been assumed to be worked with cloud. Here in our proposed system we are going to extend the available password scheme and going to show the authentication of cloud via our proposed scheme & also further we are going to check the authentication & then integrity verification about the data which we are storing into the cloud.

## 4. OBJECTIVE

Our main objective is to make such a system which can make access to cloud system of only authentic user as well as user can perform integrity check on his data to check any unauthorised modifications.  Cloud services should ensure data integrity and provide trust worthy authentication to the user privacy. Although outsourcing data into the cloud is economically attractive for the cost and complexity of long-term large-scale data storage, it's lacking of offering strong assurance of data integrity. Cloud computing poses privacy concerns primarily, because the service provider at any point in time, may access the data that is on the cloud. The Cloud service provider could accidentally or deliberately alter or delete some information from the cloud server. Hence, the system must have some sort of mechanism to ensure the data integrity. The current authentication scheme for the cloud using is textual password & basic image password which we have demonstrated in existing work, so in order to get an Intelligence login model we require a secure login process in order to access our cloud properly & secure we are using an effective graphical login process which is derived on basis of assuming the probable security issue in

current graphical password authentication scheme.

## 5. METHODOLOGY USED (FLOW CHART OF PROPOSED SYSTEM)

1  Enhanced  Graphical  password  authentication module generation.
2  Challenge Token Creation.
3  Correctness Verification.

Flow chart of the proposed system is covered in three steps. They are-
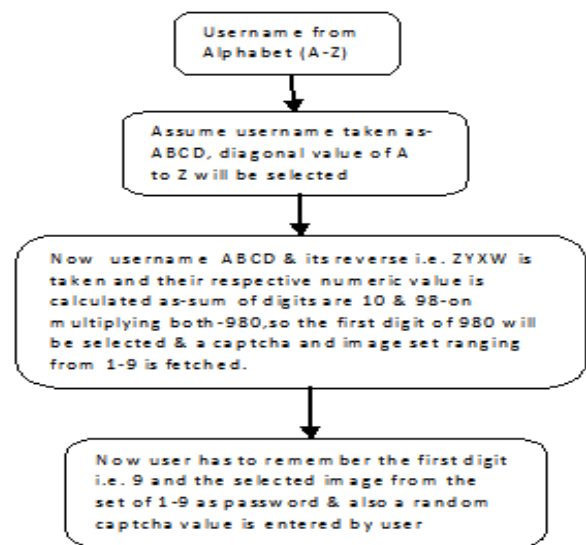
### 5.1 Registration Process



**Fig-1:** Registration process to access the cloud
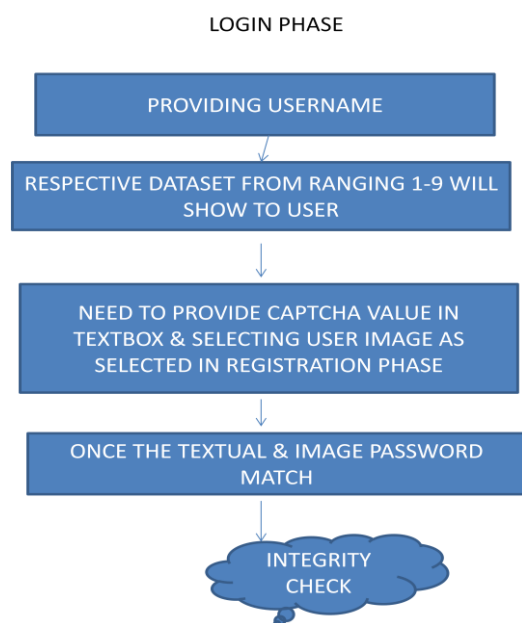
### 5.2 Login Process



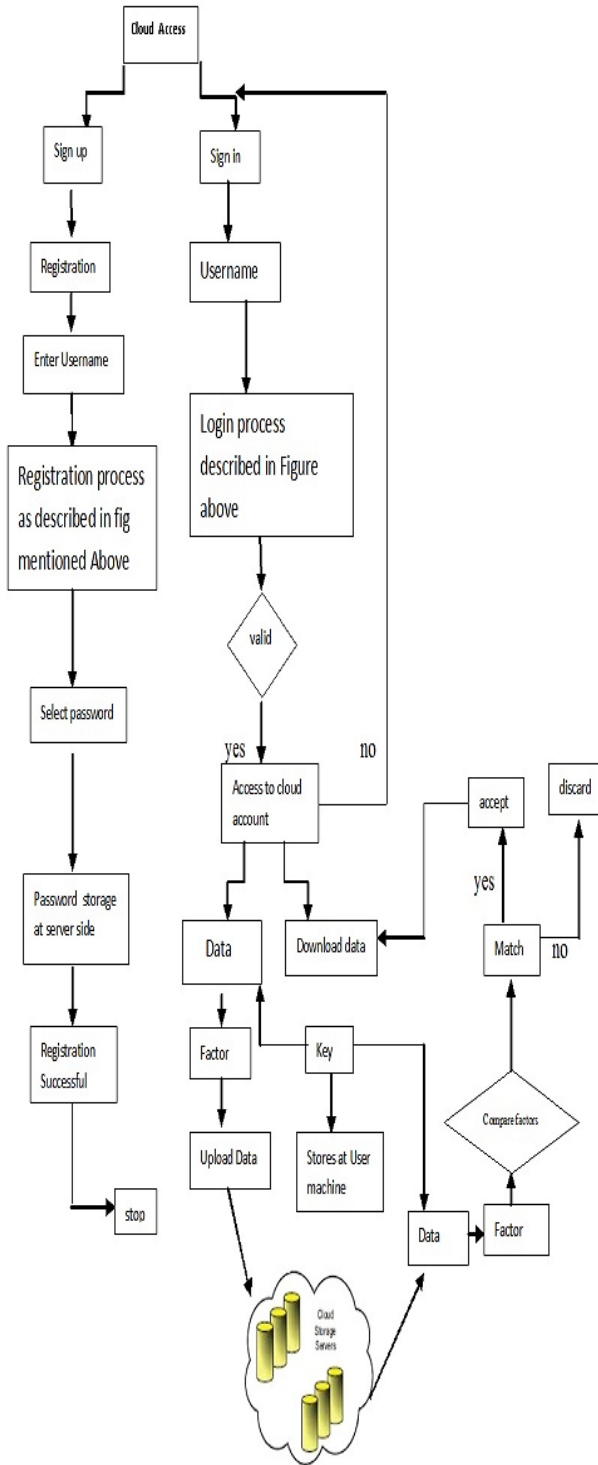**Fig-2:** Login process to the cloud

## 5.3 Complete Scenario



**Fig-3:** Complete process for login & integrity check over cloud

## 6. CONCLUSIONS AND FUTURE WORK

Cloud Computing is gaining remarkable popularity in the recent years for its benefits in terms of flexibility, scalability, reliability and cost effectiveness. Despite all the promises however, Cloud Computing has one problem: Security, we studied the problems of data security in cloud data storage, which is essentially a distributed storage system. An effective and flexible distributed scheme is proposed to ensure the login into the cloud server & then checking correctness of user's data in the cloud servers. By detailed security and performance analysis, we show that our scheme is highly efficient in recovering the singleton losses almost immediately and recovers from busty data losses. The future work for our research will be in the field of Intrusion detection technique.

## REFERENCES

[1]    Shraddha M. Gurav,Leena S. Gawade, Prathamey K. Rane,  Nilesh R. Khochare, "Graphical password authentication" – cloud securing scheme-2014 International Conference on Electronic Systems, Signal Processing and Computing Technologies, IEEE 2014.

[2]    Fawaz A. Alsulaiman and Abdulmotaleb El Saddik, *Senior Member, IEEE,* "Three-Dimensional Password for More Secure Authentication" IEEE TRANSACTIONS ON INSTRUMENTATION AND MEASUREMENT February 6, 2011.

[3]    Ms. Vidya Mhaske-Dhamdhere , Prof. G. A. Patil, "Three Dimensional Object Used for Data Security", in International Conference on Computational Intelligence and Communication Networks, IEEE 2010.

[4]    Rajkumar Chalse, Ashwin Selokar , Arun Katara, "A New Technique of Data Integrity for Analysis of the Cloud Computing Security" in 5th International Conference on Computational Intelligence and Communication Networks IEEE 2013.

[5]    Issa M. Khalil, Abdallah Khreishah, Salah Bouktif, Azeem Ahmad , "Security Concerns in Cloud Computing", in 10th International Conference on Information Technology: New Generations, IEEE 2013.

[6]    Dinesha H A Agrawal ,V K CORI, "MULTI-DIMENSIONAL PASSWORD GENERATION TECHNIQUE FOR ACCESSING CLOUD SERVICES" in International Journal on Cloud Computing: Services and Architecture (IJCCSA),Vol.2, No.3, June 2012.

[7]    Ms. Sneha Vasant Thakare, Ms. Deipali V. Gore," 3D Security Cloud Computing using Graphical Password" in International Journal of Advanced Research in Computer and Communication Engineering Vol. 2, Issue 1, January 2013.

[8]    Ainul Azila Che Fauzi, A. Noraziah, Tutut Herawan, and Noriyani Mohd. Zin, "On Cloud Computing Security Issues", in J.-S. Pan, S.-M. Chen, N.T. Nguyen (Eds.): ACIIDS 2012, Part II, LNAI 7197, pp. 560–569, 2012. © Springer-Verlag Berlin Heidelberg 2012.

[9]    Cong Wang, Qian Wang, Kui Ren, Wenjing Lou, "Towards Secure and Dependable      Storage Services in Cloud Computing," IEEE transactions on Services Computing, 06 May 2011.  Rampal Singh, IJECS Volume 2 Issue 3 March 2013 Page No. 825-830 Page 830.

[10]    Amazon.com, "Amazon web services (aws)," Online at http:// aws.amazon.com/, 2009.

**BIOGRAPHIES**

Rupal Rawat, M.Tech (CSE) Oriental college of science & Technology, Bhopal. Affiliated to RGPV, Bhopal, M.P. India

Sreeja Nair, Working as Head of Department CSE, Oriental College of Science &Technology, Bhopal Affiliated to RGPV, Bhopal, M.P ,India