I. INTRODUCTION

Cloud Computing is a new dimension scheme in the IT industry which offers an efficient, convenient, scalable business model for organizations to adopt various on demand services, applications from a shared pool of resources with no need of storing their data locally. The authentication of an authorised user and the data integrity of the outsourced data is a new challenging issue. In this paper we proposed a new authentication technique to access cloud which is GUI based graphical password & never introduced before. Also here an optimized public auditing protocol for verification of the outsourced data is introduced. The proposed technique provides extensive security and performance which makes it more secure and efficient.

II. OBJECTIVE

The main objective of our proposed work is to make such a system in which only authentic user access the cloud and whenever user wants to check the integrity he can ask to TPA and TPA will perform the integrity check on users data to check any unauthorised modifications. Security is the primary need of the cloud computing as the cloud stores lot of the client’s sensitive data which can easily be accessed by cloud service provider. The CSP can accidently either update, read or delete the clients data. Apart from data integrity the client’s authorisation is also an important issue to concern. Only authentic and legitimate user can access the account is done if we have some strong authentication schemes. To get intelligence, strong and secure login model, a strong and secure login process is required to access the cloud. A new Graphical Password scheme is proposed which can handle the probable security issues and new challenges in authentication.

III. PROBLEM IDENTIFICATION

The existing schemes for authentication and data integrity check over cloud suffers from many problems like-

A. Disadvantages of Existing Authentication System

The current password scheme is suffered from many attacks like Brute force attack, Timing attack,
Shoulder Surfing attack, Dictionary attack etc. In biometric recognition like face detection, iris recognition, thumb impression etc. Presence of required detecting hardware is not feasible all the time. Token based authentication such as bank cards, key cards also required some knowledge based methods to enhance the security, like in ATM cards, user need to remember the ATM pin for accessing the account. In Textual password scheme which is one of the widely used, the passwords which are hard to break or guess are also hard to remember. 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.

B. Disadvantages of Existing Integrity Verification System

The data stored at server can be compromised by some internal or external threats. The existing data integrity verification techniques are quite slow in encryption and in over all processing.

After outsourcing the data user deletes the local copy of his data and has no more access from the local machine. So, if any problem like modification of data, deletion of data, malicious attack, and server failure is occurred, user is not aware of it. One of the main problem is the user’s data is completely handled by the CSP and the CSP can mange in his own way. A need of Third Party Auditor is required for transparent verification of data which must be strong as well as fast.

IV. PROPOSED WORK PLAN

In this section we present our proposed authentication scheme and the public data auditing for the integrity verification. We start with our effective authentication scheme which will be preceded by the data integrity scheme.

The proposed scheme for authentication consists of two phases, we are defining below-

1. Registration phase- In this phase user has to enter a unique username and all his required details. The username can be alphanumeric. On the basis of username a image set is presented to the user. From those images he has to select an image and this selected image is further splits into sub-images of the main image. From those sub-images user has to select one of the image as his password.

The calculation behind the image set to be presented to the user on the basis of username is explained below-A username is entered for e.g. ABCD21 then the numbers assigned to ABCD & its reverse ZYXW is taken and calculated as sum of digits. The sum of A-01, B-02, C-03, D-04 is 10 and of Z-26, Y-25, X-24, W-23 is 98. On multiplying we get 980 and then the 21 in username is added i.e. 980+2+1=983. The first digit of 983 will be selected and a image set ranging from 1-9 is fetched.

2. Login Phase- After registration user can login into his account with the same username & graphical password which he has entered during registration. If the selected password image is not matched with the image given at the time of registration then the login process will be terminated. After the login process the user will be connected to the cloud and can upload, download his data and also can perform the integrity check over the data.

The proposed scheme for Data Integrity Verification is described below-

Data Integrity check- The file to be uploaded is first divided into n blocks and then encrypted and its hash value is generated. The file and its hash value is uploaded to cloud. Whenever user wants to check the integrity, he can ask to TPA for the verification. The TPA will challenge the cloud server for verification and in return server will send back the required file and its hash value to tpa which will be compared by the TPA.

V. OUR SYSTEM AND ASSUMPTIONS

A. The System Components

We consider cloud data storage service as three entities: the cloud user who has a lot of data to be outsourced on cloud storage, the cloud server (CS) which has a large storage space, computation resources and data storage services all are handled by cloud service provider (CSP), the third party auditor (TPA) who fulfils all the request of the user about his data integrity.

The user’s data is kept private from the TPA. We assume the threats for the authentic user to cloud are hackers who can easily attack and know the password. The textual password can be accessed by lot of methods like brute force attack, dictionary attack, timing attack, shoulder surfing attack.

We consider the threats for users data integrity can be external like bugs in network traffic & in software, system failure, hardware failure, hackers etc. and internal like cloud server is compromised or the corruption of data can be hidden by CS.

The user can trust the TPA as the outsourced data is audited by the TPA without knowing it. The TPA is a trusted Government Agency or any certified agency which is fair to both client and server and never be compromised.

Privacy Preserving for Secure Cloud Storage using Graphical Password

57
B. Threat Model
In the basic Authentication scheme i.e. Textual Password, Token based, Biometric etc. there are various problems with all the schemes. Apart from the authentication scheme the integrity of client’s data over the cloud might be at risk due to the following reasons. First, to gain profit and maintain the reputation, the Cloud Service Provider (CSP) can try to hide data loss caused by system failure, errors due to management, malware attacks etc.

The CSP can discard the data stored at cloud that has not been/is rarely used and can reclaim for the storage. Second, the CSP has an agreement with the data owner to maintain the number of copies of the data. The CSP may store fewer copies than the copies mentioned in the agreement.

Proposed Algorithm for data verification:
The proposed scheme consists of following algorithms:

1. KeyGen - This algorithm is run by the data owner. It takes an implicit security parameter and returns a secret key (sk) and a pair of secret-public tag key (skt, pkt).
2. TagGen (M, skt) - This algorithm is run by the data owner. It takes the secret tag key skt and the encrypted M data blocks as input and gives hash values T of each data blocks as output.
3. Challenge (Minfo) - This algorithm takes some Message information (e.g. File-id, file size, time stamp etc.) as input and output a challenge Ch.
4. Proof (M, T, Ch) - This algorithm is run by the CSP. It takes Message M, tags T and Challenge Ch from TPA as input ad give proof P as output.
5. Verify (P, pkt) - This algorithm is run by the TPA. It takes as input the public tag key pkt, and the proof P returned from the CSP. The output is 1 if the integrity of all file copies is correctly verified or 0 otherwise.

VI. OVERVIEW OF OUR SOLUTION

C. Procedure for Authentication and Data Verification
Suppose a user wants to upload his data on the cloud. First of all he has to register himself with the proposed authentication technique using graphical password. After registration, he can login to his account with the same graphical password and the username. Now suppose the user wants to upload a file M over the cloud, to do this the user just run the proposed algorithm KeyGen as discussed above. The file is first divided into m blocks (m1, m2….mn) and encryption is performed on each of the data blocks using AES algorithm. After encryption another algorithm TagGen is called to get the hash /tag s of each of the data blocks with the help of secret hash key. Each block with its hash value is uploaded to cloud.

Whenever user wants to check the integrity of his outsourced data he passes the Message information, tag values and a public tag key o the TPA. The TPA passes a challenge in the form of Minfo to the CSP and in return the CSP runs the Prove algorithm on the basis of Minfo and gives the File data blocks and their corresponding tag values. The TPA now will generate the tag with the help of public tag key and compare the tags. The verify algorithm is used by TPA which gives 1 for correct data and 0 for corrupted.

B. Advantages of Proposed Model
Using Graphical password approach for cloud access is a new concept which is not been proposed yet. To select an image as password which will further splits into sub-images increases its complexity. It cannot be easily recognized by any of the attack as the number of images and their sub-images makes a large number of possible combinations. Apart from authentication for data integrity verification there is a strong encryption and hash generation algorithm. In this scheme user have knowledge about the size of its data file being uploaded. It is fast and as much secure as the existing one.

VII. SECURITY ANALYSIS
The security can be analyzed in two aspects- Confidentiality and Integrity. Confidentiality is maintained as the data is first encrypted and then outsourced over the cloud. The AES algorithm is used for encryption and decryption of the data. It will ensure that the file is not intercepted by any third person. Integrity is maintained as the hash values of each data block is calculated and then the data block is stored with the data tags on the cloud. Following are the possible attacks on the proposed model. We assume that the TPA is honest and performs the verification procedure honestly. TPA receives the data from cloud server and do his job but the server can be dishonest and may perform the following attacks-
1. Replace attack. The challenged pair of data block and tag can be replaced by some another existing or corrupted pair by CSP.
2. Forge attack. If the same secret tag key is used for different data files or messages then the CSP can forge the data tag and cheat the TPA.
3. Replay attack. The server may show some another proof generated by previous one or from some other information without gaining access to the actual data.

VIII. COMPARATIVE STUDY

Table-1: Comparative study of existing scheme and proposed scheme.

<table>
<thead>
<tr>
<th>System</th>
<th>Existing System</th>
<th>Proposed System</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time Complexity</td>
<td>Less</td>
<td>More</td>
</tr>
<tr>
<td>Performance</td>
<td>Low</td>
<td>High</td>
</tr>
<tr>
<td>Flexibility</td>
<td>Less</td>
<td>Good</td>
</tr>
<tr>
<td>Algorithm used</td>
<td>RSA and MD5</td>
<td>AES and SHA1</td>
</tr>
<tr>
<td>Password Method</td>
<td>Textual</td>
<td>Graphical</td>
</tr>
</tbody>
</table>

IX. SCREENSHOTS

CONCLUSION AND FUTURE ENANCEMENT

In recent years, cloud computing is become more popular for its scalability, reliability and flexibility. One of the problem with the cloud system is security of data stored at cloud. A novel graphical password scheme is proposed for login into the cloud and an optimized method for verifying the correctness of data is also merged. The Graphical password gives choice to the user of selecting images of his own choice. For data integrity verification in our scheme, interaction between authorized user and CSP is considered. Our design principle is mainly based on the strong Encryption algorithm and secure hash algorithm. Moreover the proposed scheme supports public verifiability and allows unlimited number of auditing. On studying the security analysis and performance in detail of the proposed scheme, we show that our scheme is highly efficient and flexible. In future work, to improve the system performance, we will concentrate on the batch auditing system in which the auditor will consider the auditing requests from multiple data owners simultaneously.

REFERENCES

[2] Cong Wang, Member, IEEE, Sherman S.M. Chow, Qian Wang, Member, IEEE, Kui Ren, Senior Member, IEEE, and


Privacy Preserving for Secure Cloud Storage using Graphical Password