Data Verification and secure auditing scheme in Cloud

***Abstract*—Cloud Computing provides services to users to store enormous amount of data without any limitations. The data is verified using Digital Signatures. In this work, auditor plays an important role in preserving privacy, integration and data verification.**

This paper presents the secure auditing scheme where only authorized users are able to access the files. The comparison of SHA-1 and ORUTA scheme with respect to storage of the file uploaded in the cloud is depicted. Our experimental evaluations show that SHA-1 is more secure, occupies less space and has more accuracy than RSA.

Keywords—Auditing, Cloud Computing, Security

I. INTRODUCTION

Cloud Computing is the practice of using an Internet-hosted remote server network to store, handle, and process information instead of a local server or personal computer. Pretty much every individual who is utilizing the cutting-edge innovation in the present world are utilizing distributed computing procedures inside or remotely. This is assessed as the progress in innovation ability towards distributed computing. Major cryptographic strategies are proposed for performing security a lot more grounded way. Individuals from different areas of expertise are therefore dependent on cloud, especially for company in organizations. Client data in cloud servers are held as classified as mystery that ensures client security and cloud information.

II. EXISTING SYSTEM

In this RSA algorithm is used to generate the keys and it cannot give maximum security to the data. In existing systems cloud server performs integrity checking along with the task of handling the data storage which increases the burden of cloud server. It is necessary to develop an efficient and secure auditing scheme which can perform public auditing effectively by maintaining both integrity and confidentiality of data.

In the existing system we use RSA algorithm to generate the keys and it cannot give security to data comparatively. In existing system there is cloud user, third party auditor and cloud owner. One of the problem aroused is how to preserve identity and privacy from the third party.

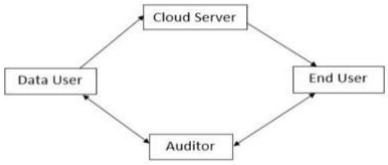
Hence, we use an external party which is the auditor for maintaining the correctness of the stored data. Auditor plays an important role he is the one who has all the authorities. Here privacy preserving problem by using auditor

III. PROPOSED SYSTEM

In the proposed system we used AES and SHA-1 algorithm so that we can achieve maximum security.

We mainly used 4 modules namely; Cloud server, Data User, End User and Auditor.

1. Cloud Server: All the stored data here and cloud server is used as storage, depends upon the cloud server capacity we choose the number of blocks of data to be divided.
2. Data User: The user who upload the file to cloud server to maintain their data confidential. User must request for public key and secret key with the Auditor. Once the auditor authorized the person then only user can upload the file to the cloud server. User has an authority to upload the file, edit the file and delete the file.
3. End User: The end user can download the file. Before it should get the files it should take authorization from the auditor by obtaining private key for accessing the data.
4. Auditor: The Auditor has main role in this concept and he is the one who authorizes the end user and data user.



Flow diagram of the proposed system

To overcome the privacy issues such as data security and identity privacy of users in public auditing mechanism an ORUTA (One Ring to Rule Them All) scheme is used. ORUTA scheme is a new privacy preserving technique which utilizes ring signature. By using ring signature, the identity of each user is kept under secret or hidden from public verifiers. Main purpose of ring signature is to hide an actual key generator on each block. Another advantage of using ring signature is that it should be computationally difficult to determine which of the group members keys are used to produce the signature. The ring signature scheme convinces a verifier that a document has been signed by one of n independent signers.

The construction of ORUTA includes five algorithms:

KeyGen, SigGen, Modify, ProofGen and ProofVerify.

1) KeyGen: In KeyGen a valid user in the group can generate valid keys to compute ring signature. Key is generated based on the users attributes.

2) SigGen: In SigGen, the users form the ring structure using the keys that is based on the priorities set by the data owner.

3) Modify: In modify, a user can compute new ring signature on the new block. ORUTA scheme supports dynamic operations such as insertion, deletion or update operation on a block.

4) ProofGen: The ProofGen is done by third party auditor and the cloud server together to generate a proof of possession of distributed data.

5) ProofVerify: In ProofVerify, the external auditor will examine the accuracy of data by analyzing the proof.

The system design works as follows:
1) The shared data and verification information such as keys are accumulated in the cloud server. A third party auditor(TPA) is there to provide verification services to cloud users, whether the user is authenticated to view or access the confidential data in cloud.

2) TPA will verify the security of resources on behalf of cloud users.

3) When a user wishes to access the resources accumulated in cloud. User first sends an auditing request to third party auditor.

4) On receiving the audit request, TPA creates an auditing message and send it to the cloud.

5) After getting the audit message, the cloud server will verify the request and generate an auditing proof and send back to TPA.

6) The third party auditor will analyze the proof sent by the cloud server and generates an audit report to the requested user.

7) The audit report indicates whether the requested user is authenticated to use the confidential data in cloud. During auditing phase, the third party auditor learns users confidential information and identity of users.
2) TPA will verify the security of resources on behalf of cloud users.

3) When a user wishes to access the resources accumulated in cloud. User first sends an auditing request to third party auditor.

4) On receiving the audit request, TPA creates an auditing message and send it to the cloud.

5) After getting the audit message, the cloud server will verify the request and generate an auditing proof and send back to TPA.

6) The third party auditor will analyze the proof sent by the cloud server and generates an audit report to the requested user.

7) The audit report indicates whether the requested user is authenticated to use the confidential data in cloud. During auditing phase, the third party auditor learns users confidential information and identity of users. Cloud server which acts as a storage has connection between both the data user and the end user, all the data which has to be taken and which is to be stored it must be stored directly in the cloud server. Here the data user and end user have a separate profile to manage their activities. Data user and end user should authorized by auditor before using the cloud server to store and download the file respectively.

IV. ALGOITHMS USED

1. ORUTA algorithm:-

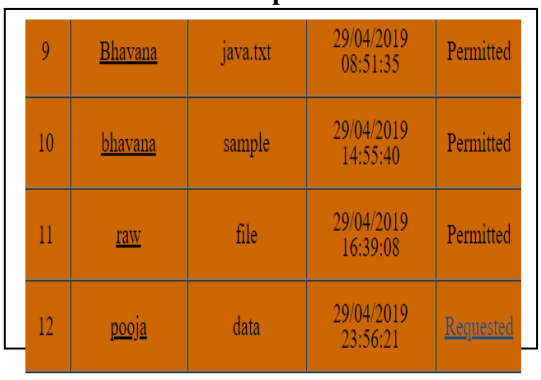
This algorithm is used to encrypt and decrypt the data, here it generates OTP's by using this otp we can convert the data into encrypted form and also by generating another otp we can again decrypt the same data. When compared to other algorithms it is more secure because we cannot able to notice encrypted and decrypted data.

2. SHA-I algorithm:-

By using SHA-1, we generate the digital signatures and we divide the data into blocks and then uploaded to the cloud server. We can divide the data into maximum number of blocks depends upon the cloud server capacity, in our proposed system it divides into 4 blocks and it converts into encrypted data. By this it maintains high security, data integrity.

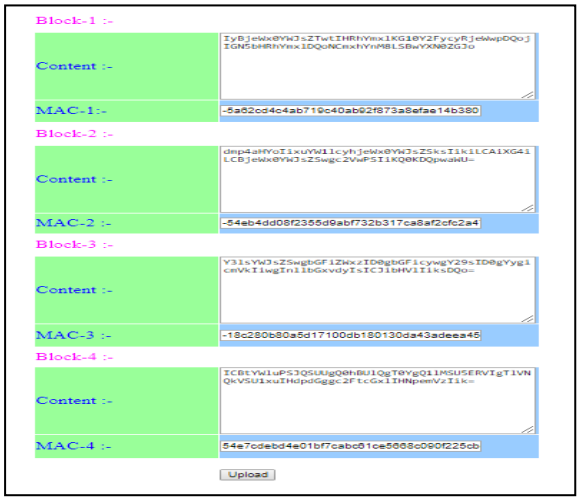
V. RESULTS

Data user asking permission from auditor to upload a file



9	Bhavana	java.txt	29/04/2019 08:51:35	Permitted
10	bhavana	sample	29/04/2019 14:55:40	Permitted
11	raw	file	29/04/2019 16:39:08	Permitted
12	pooja	data	29/04/2019 23:56:21	Requested

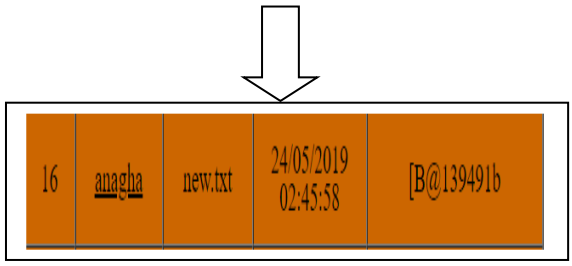
CSP permits data owner to upload a file



owner uploads a file using secret key which will be in encrypted form

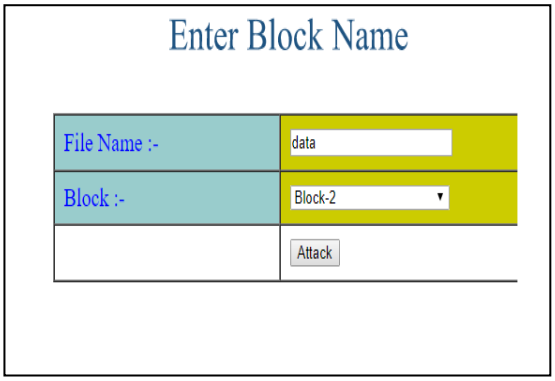
Sl.No.	File Name	File Size	Status/Response
1	new.txt	1579	Requested

End user requesting TPA to generate decrypt key



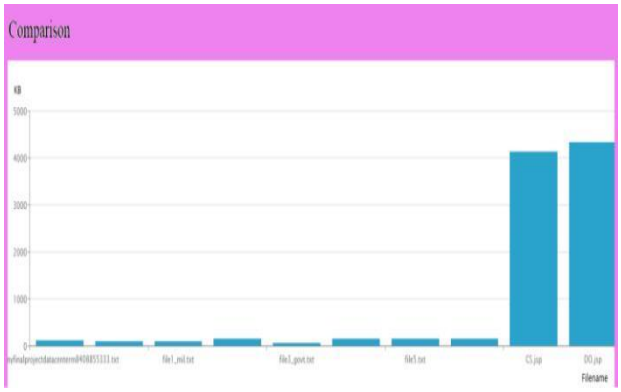
16	anagha	new.txt	24/05/2019 02:45:58	[B@139491b

TPA generates a decryption key



Attacker trying to guess a file name and open it
Data owner verifying the file

On file recovery



Here we are comparing the two algorithm performance and Storage Capacity. The algorithm what is used in the proposed system is taking more space then SHA-1. It also guarantees the security. System storage and data integrity achieved.

VI. Conclusion

The Secure Auditing Scheme is presented here which implements the *AES* and *SHA-1* algorithm. It verifies the data by using digital signatures. By comparing with *ORUTA* scheme, we conclude that our proposed scheme justifies the store data integrity and security in the cloud computing environment.

REFERENCES

[1] K. Ruth Ramya, T. Sasidhar, D. Naga Malleshwari & M.T.V.S. Rahul, "A review on security aspects of data storage in cloud computing", International Jounal of Applied Engineering Research, Vol 10, No 5, 2015. pp. 13383-13394.

[2] Hassan Rasheed, "Data and Infrastructure security auditing in cloud computing environments", International Journal of Information Management, 2014.pp. 364-368.

[3] C. Wang, Q. Wang, K. Ren and W. Lou, "Privacypreserving public auditing for data storage security in cloud computing", IEEE INFOCOM 2010, IEEE, 2010.

[4] Sonali. D. Thosar and Nalini.A. Mhetre, "Integrity checking privacy preserving approach to cloud using third party auditor", In proceedings of2015 International conference on pervasive computing (ICPC), IEEE 2015.

[5] Amazon Web Services. https://aws.amazon.com/.

[6] D. Burihabwa, R. Pontes, P. Felber, F. Maia, H. Mercier, R. Oliveira, J. Paulo, and V. Schiavoni. On the cost of safe storage for public clouds: an experimental evaluation. In Proceedings of the 35th IEEE Symposium on Reliable Distributed Systems, pages 157–166, 2016.

[7] J. Y. Chung, C. Joe-Wong, S. Ha, J. W.-K. Hong, and M. Chiang. CYRUS: Towards client-defined cloud storage. In Proceedings of the 10th ACM European Conference on Computer Systems, EuroSys'15, 2015.

[8] Cloud Security Alliance. The notorious nine: Cloud computing top threats in 2013, Feb. 2013.