Privacy Preserving Batch Auditing for Multiuser and Multicloud

Miss. Harsha B.Patil[#1], Prof. Yogesh S. Patil[*2]

[#]*M.E. Student, Department of CSE, Shri Sant Gadge Baba College of Engineering & Technology, Bhusawal, North Maharashtra University, India*

[*]*Assistant Professor, Department of CSE, Shri Sant Gadge Baba College of Engineering & Technology, Bhusawal, North Maharashtra University, India*.

Abstract—**Cloud offers various services that not only stored but can also be shared among multiple users .But the major problem is about data integrity due to existence of hardware/software failure and human errors.To check the integrity of cloud data ,third party auditor(public verifier) is introduced to perform public auditing.A privacy preserving mechanism in which the identity of the user on each shared block is protected from public verifier, who is responsible to efficiently verify shared data integrity instead of retrieving the entire file. Ring signature is being exploited to audit the correctness of shared data by verifying the metadata available to the auditor.We introduce a new mechanism that perform batch auditing to handle multiple requests concurrently by improving the efficiency of the auditing using multi cloud.**

Keywords: public auditing,TPA, batch auditing,Cloud Computing, Privacy preserving, Security, Integrity

I. INTRODUCTION

With cloud computing and storage, cloud service providers offers various services e to access and to share resources to users . It is routine for users to cloud storage services to share data with others in a group, as data sharing is standard feature in most cloud storage .It offers services like Dropbox, iCloud and Google Drive. The integrity of data in cloud storage, is subject to incredulity and exploration, as data stored in the cloud can easily be lost or corrupted due to the hardware/software failures and human errors.

The traditional approach is to check data correctness is retrieve the entire data from the cloud and then verify data integrity by checking the correctness of signatures (e.g., RSA) or hash values (e.g., MD5)of the entire data. From that conventional approach able to successfully check the correctness of cloud data. However, the efficiency of using this traditional approach on cloud data is in doubtful because the size of cloud data is large. Downloading the entire cloud data to verify data integrity will cost or even waste users amounts of computation and communication resources, especially when data have been corrupted in the cloud.

Public auditing is to allow a public verifier as well as a data owner itself without downloading the entire data to efficiently perform integrity checking from the cloud.

The data is not physically present in user's storage we cannot use traditional cryptography methods to encrypt the data, downloading complete file only for verification is very difficult If the data is very large in size the task of auditing is very expensive. All these problems can be solved by enabling public auditing. In public auditing user can depends on the third party for the verification of downloaded data. Enabling public auditing leads to:

1. Third party Auditor checks the integrity of data periodically.
2. Save the cloud user's computational resources and reduces online burden.
3. It is easier and affordable for the user to check the data's integrity and correctness.
4. Using public auditing the user not suffer from the complexity in verifying data and hence it increases efficiency.

In public auditing mechanisms, data is divided into many small blocks, where the owner is independently sign each block; and during integrity checking, a random combination of all the blocks instead of the whole data is retrieved. A public verifier could be a data user, who would like to utilize the owner's data through cloud. A public verifier work as a third-party auditor (TPA) to provide expert integrity checking services. Existing public auditing mechanisms is used to verify shared data integrity .But there is a privacy issue introduced in shared data with using existing mechanisms is the preservation of identity privacy to public verifiers. It is difficulty to preserve identity privacy from public verifiers during public auditing, during protecting confidential information.

To solve this kind of privacy issue on shared data .ORUTA is proposed.Oruta is a privacy preserving public auditing mechanism that uses ring signature to construct homomorphic authenticators .In this mechanism public verifier is able to verify the integrity of shared data without retrieving the entire data during the identity of the signer on each block in shared data is kept private from the public verifier. Oruta also support for batch auditing.It perform multiple auditing tasks simultaneously and improve the efficiency of verification for multiple auditing tasks.Oruta stands for "One Ring to Rule Them All".We develop an efficient auditing mechanism, which support batch auditing for multiple data files in multi-cloud environment. We are using TPA to check the integrity of data.

A. Objectives

We have various measure on cloud computing security challenges from single to multi clouds. While making a cloud secure, following objectives are to be met:

- Any user in the group can store and share data files with others by the cloud.
- Data Integrity.
- To provide the system that supports data preserving as well as identity privacy preserving public auditing ofshared data in a clouds
- To provide a mechanisms that supports dynamic groups data sharing in the clouds
- To support batch auditing for user's multiple data.

II. Existing System

Oruta is a privacy preserving public auditing mechanism for shared data in an untrusted cloud. In Oruta ring signatures is used to construct homomorphic authenticators , so that the third party auditor is able to verify the integrity of shared data for a group of users without retrieving the entire data and the identity of the signer on each block in shared data is kept private from the TPA. In addition, It also support for batch auditing, in that single auditing task audits multiple shared data simultaneously. Oruta uses random masking technique to support data privacy during public auditing, and index hash tables to support fully dynamic operations on shared data. A dynamic operation indicates an insert, delete or update operation on a single block in shared data.

Limitation Of Existing System

The Existing system(oruta)consist single cloud which contain multiple organization.When a client demand the Resources to the single cloud by providing multiple Request or queries like more than 10,000 to single cloud It become overloaded and Traffic conjuction is occurred ,Time Delay will happens, its fully based on CPU,BAND WIDTH,MEMORY). And No security.

III. Proposed System

The proposed diagram is shown below.

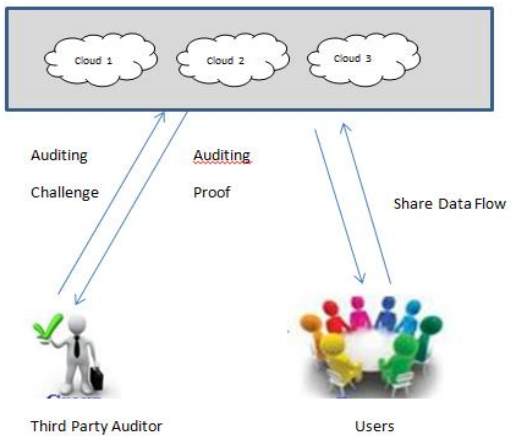

Fig. 1 System Architecture

The model involves three different entities cloud users, multicloud and third party auditor.

The cloud usershave a number of data files to be stored in multiple clouds. They have the authority to access and manipulate the stored data.

The multi-cloud consists of multiple Cloud Server Providers (CSPs). They provide data storage service and have enough storage space and significant computation re-sources. To reduce the communication burden of verification, one of CSPs is designated as an organizer for auditing purposethe organizer takes the responsibility todistribute the auditing challenge and aggregate the proof from multiple clouds.TheThird Party Auditor(TPA) has a more powerful computation and communication ability than regular cloud users

IV. Proposed System Flow

A.Components:

The system model consists of three different entities:

1) User Module: It consist of 2 modules registration module and login module.Using registration module user can do registeration.Login module is used to user can login into the system then he can upload ie store data on cloud and download data from cloud.

*2)Cloud Server Module:*The user can perform following operations on server like file uploading, file downloading on multiple cloud.. Cloud is the large repository of resources. Cloud is responsible for storing all user's data and granting access to the file.

*3) TPA Module:*The Trusted Party Auditor is a module which is used to the audit the data that are uploaded by the Data Owner in the Server. So that TPA will audit data to check the integrity of data.For this we design one attacker module ,the attacker does changes in cloud data.and when we check integrity of data then its shows the verification result.In that we also design 2 auditing phases individual and batch auditing module

B. Phases

System flow consist of two phases:

1)Setup Phase:

The first is the setup phase. Cloud user register itself to the cloud and generate parameter and upload file to the cloud server.

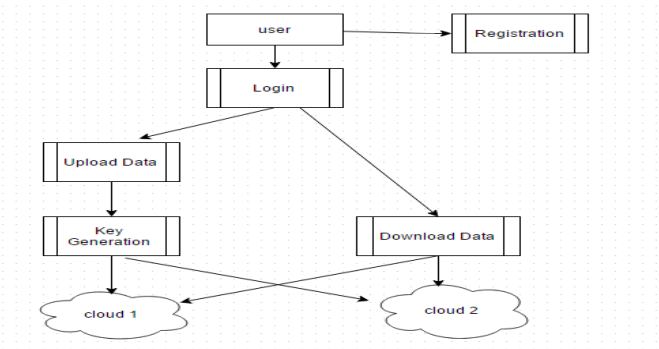

Fig.2 Setup Phase

2) Audit Phase:

Second is Audit phase. TPA send auditing challenge to cloud server. In response cloud generates a response message and send it to the TPA. Then TPA performs the auditing of the data stored on the cloud server.

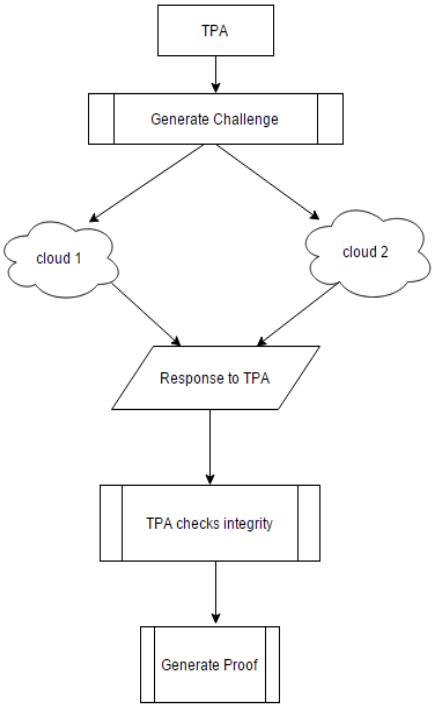

Fig. 3 Audit Phase

V. IMPLEMENTATION

A.Ring Signature

Ring signature concept first proposed by Rivest et al. in 2001.Verifier agreed about Ring signature which is computed using one of group member's private keys but verifier is not able to determine which one .This preserve identity of signer from verifier.

B. Homomorphic Authenticator

Homomorphic authenticator (Homomorphic verifiable tags)is a basic tool to construct public auditing mechanism. Homomorphic authenticator based on signature should satisfy the following properties:

*1)BlocklessVerifiability:*It allow verifier to audit integrity of data with special block which is linear combination of all the blocks in data.If integrity of combined block is correct then verifier believes that integrity of entire data is correct.

*2)Non-malleability:*An attackers cannot generate valid signatures on invalid blocks by linearly combining existing signature.

*C. Homomorphic Authenticator Ring Signature:*Traditional ring signature do not support blockless verification .Without BlocklessVerification,TPA has to download whole data file to verify correctness of shared data,which consumes excessive bandwidth and takes long verification times.Ring signature generated by HARS is able not only to preserve privacy but also support blocklessverification.

D.Oruta

It consist of 5 algorithms:

1) *KeyGen*:Each User will generate public and private key.
2) *SigGen*: User needs to compute the ring signatures on the blocks in shared data by using private key and group members' public keys.
3) *Modify*:User of group are able to perform upload and download opeartions.
4) *ProofGen*: Public verifier(TPA) and cloud server together interactively generates proof of possession for shared data
5) *ProofVerify* : The public verifier(TPA) audits the integrity of shared data by verifying the proof.

E.Implementation of Batch Auditing :

The implementation of batch auditing is as follows,Using public auditing in the cloud, the TPA may receive amount of auditing requests from different users in a very short time. Unfortunately, allowing the TPA to verify the integrity of shared data for these users in several separate auditing tasks would be very inefficient. Therefore, we further extend Oruta to support batch auditing, which can improve the efficiency of verification on multiple auditing tasks.

1)Batch Proof Generation:

Proof generation algorithm is operated by a public verifier and the cloud server together to interactively generate a proof of possession of shared data. The public verifier sends an audit challenge to the cloud server with initiate the proof generation algorithm to generate an auditing proof for each shared data. The cloud server runs the proof generation algorithm and sends the audit proof to the public verifier.

2) Batch Proof Verify :

In ProofVerify, the public verifier audits the integrity of shared data by verifying the proof .The public verifier audits the integrity of shared data by verifying the proof. With the auditing proof, an auditing challenge, public aggregate key and all group members public keys the public verifier checks the correctness of the proof.

VI. RESULT ANALYSIS

A. Performance Of Signature Generation

The generation time of a ringsignature on a block is determined by the number of users in the group and the number of elements in block. As shown in Fig. 3 and Fig.4, when k is fixed, the generation time of a ring signature is linearly increasing with the size of the group; when d is fixed, the generation time of a ring signature is linearly increasing with the number of files.

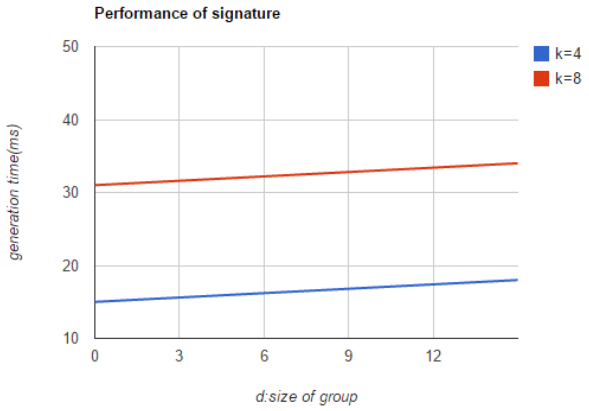

Fig.4 Impact of d on signature generation time

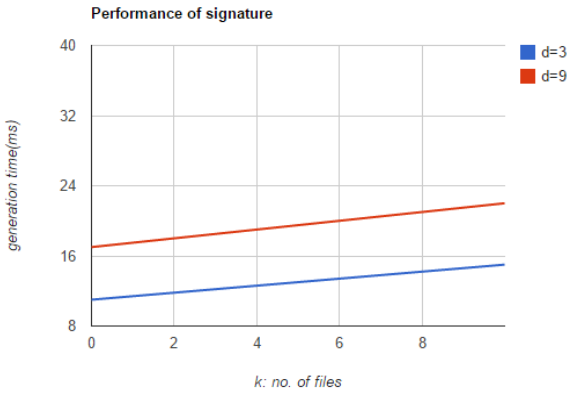

Fig.5 Impact of k on signature generation time

B.Comparision of Separate Auditing and Batch Auditing

Graph shows thecomparison between separate auditing and batch auditing

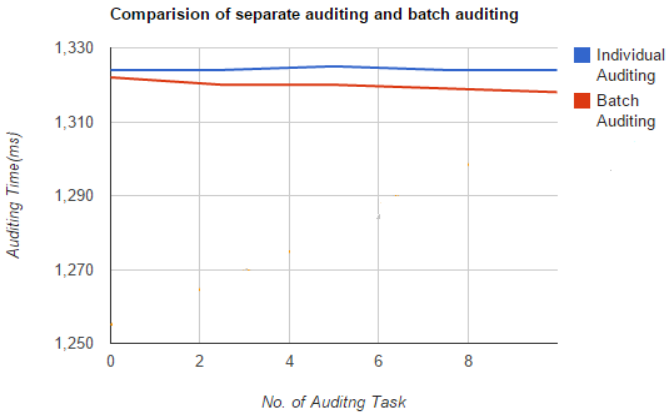

Fig.6 *Comparision of Separate Auditing and Batch Auditing*

VII .RELATED WORKS

Table 1 shows the Different mechanism with their advantages and disadvantages:

TABLE 1:Different Mechanism

	Title	Year	Author	Method	Advantages	Disadvantages
1	Public Auditing for data storage security	2010	C. Wang, Q. Wang, K. Ren, and W. Lou	Dimentionality of data space	ensures correctness and unforgeability	the identity privacy is not achieved
2	Towards Secure and Dependable Storage Services in Cloud Computing	2012	Cong Wang, Qian Wang, KuiRen, Ning Cao and Wenjing Lou	Distributed storage integrity auditing mechanism	Dynamic data verification	Data Integrity is not achieved
3	LT Codes-based Secure and Reliable Cloud Storage Service	2012	Ning Cao, Shucheng Yu, Zhenyu Yang, Wenjing Lou, Y. Thomas Hou	LT codes-based cloud storage service	• Efficient and fast data retrieval • Less storage cost	•Need to retrieve entire data to check data integrity •TPA is not trustable
4	Privacy-Preserving Public Auditing for Secure Cloud Storage	2013	Cong Wang, Sherman S.M. Chow, Qian Wang, KuiRen and Wenjing Lou	Privacy-preserving public Auditing mechanism	• Assures zero knowledge leakage •Better privacy preservation	Group access of data cannot be secured
5	Mona: Secure Multi-Owner Data Sharing for Dynamic Groups in the Cloud	2013	Xuefeng Liu, Yuqing Zhang, Boyang Wang, and Jingbo Yan	Secure multi owner data sharing scheme	•Better security over group of users •User revocation is handled effectively	Remote data integrity is not considered
6	Dynamic Audit Services for Outsourced Storages in Clouds	2013	Yan Zhu, Gail-JoonAhn, Hongxin Hu, Stephen S. Yau, Ho G. An, and ChangJun Hu	Dynamic audit services	•Less communication overhead • Less memory storage	Highly causes from security attacks
7	Knox:Privacy-Preserving Auditing for Shared Data with Large Groups in the Cloud	2012	Boyang Wang, Baochun Li and Hui Li	Group signature	Reveals the identity of signer	Used for large groups
8	Oruta: Privacy-Preserving Public Auditing for Shared Data in the Cloud	2014	Boyang Wang, Baochun Li and Hui Li	ORUTA	User identity information are hided from TPA	Data freshness is not concentrated

VIII. CONCLUSION

Cloud computing is emerging technology .which provide various services through internet. User can remotely storedtheir data on the cloud.Third party auditor checks the integrity of data without retrieving entire dataOruta is privacy preserving mechanism for shared data in cloud.Weuses ring signatures to construct homomorphic authenticators which achieve identity privacy.We extend our mechanism using multicloud and batch auditing process User is able to share data with others in the group without revealing identity privacy to the multiple cloud.Using batch auditing ,multiple auditing tasks are performed to improve efficiency of verification.

REFERENCES

[1] B. Wang, B. Li, and H. Li, "Oruta: Privacy-Preserving Public Auditing for Shared Data in the Cloud," Proc. IEEE Fifth Int'l Conf. Cloud Computing, pp. 295-302, 2014.

[2] A. Juels and B.S. Kaliski, "PORs: Proofs of Retrievability for Large Files," Proc. 14th ACM Conf. Computer and Comm. Security (CCS'07), pp. 584-597, 2007.

[3] H. Shacham and B. Waters, "Compact Proofs of Retrievability," Proc. 14th Int'l Conf. Theory and Application of Cryptology and Information Security: Advances in Cryptology (ASIACRYPT '08), pp. 90107, 2008.

[4] G. Ateniese, R.D. Pietro, L.V. Mancini, and G. Tsudik, "Scalable and Efficient Provable Data Possession," Proc. Fourth Int'l Conf. Security and Privacy in Comm. Networks (SecureComm'08), 2008.

[5] D. Boneh, B. Lynn, and H. Shacham, "Short Signatures from the Weil Pairing," Proc. Seventh Int'l Conf. Theory and Application of Cryptology and Information Security: Advances in Cryptology (ASIACRYPT'01), pp. 514-532, 2001.

[6] C. Erway, A. Kupcu, C. Papamanthou, and R. Tamassia, "Dynamic Provable Data Possession," Proc. 16th ACM Conf. Computer and Comm. Security (CCS'09), pp. 213-222, 2009.

[7] C. Wang, Q. Wang, K. Ren, and W. Lou, "Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing," Proc. IEEE INFOCOM, pp. 525-533, 2010.

[8] D. Boneh, C. Gentry, B. Lynn, and H. Shacham, "Aggregate and Verifiably Encrypted Signatures from Bilinear Maps," Proc. 22nd Int'l Conf. Theory and Applications of Cryptographic Techniques: Advances in Cryptology (EUROCRYPT'03), pp. 416-432, 2003.

[9] C. Wang, Q. Wang, K. Ren, and W. Lou, "Ensuring Data Storage Security in Cloud Computing," Proc. 17th Int'l Workshop Quality of Service (IWQoS'09), pp. 1-9, 2009.

[10] B. Chen, R. Curtmola, G. Ateniese, and R. Burns, "Remote Data Checking for Network Coding-Based Distributed Storage Systems," Proc. ACM Workshop Cloud Computing Security Workshop (CCSW'10), pp. 31-42, 2010.

[11] N. Cao, S. Yu, Z. Yang, W. Lou, and Y.T. Hou, "LT Codes-Based Secure and Reliable Cloud Storage Service," Proc. IEEE INFOCOM, 2012.

[12] S. Halevi, D. Harnik, B. Pinkas, and A. Shulman-Peleg, "Proofs of Ownership in Remote Storage Systems," in Proc. ACM Conference on Computer and Communications Security (CCS), 2011, pp. 491–500.

[13] Q. Zheng and S. Xu, "Secure and Efficient Proof of Storage with Deduplication," in Proc. ACM Conference on Data and Application Security and Privacy (CODASPY), 2012.

[14] M. Franz, P. Williams, B. Carbunar, S. Katzenbeisser, and R. Sion, "Oblivious Outsourced Storage with Delegation," in Proc. Financial Cryptography and Data Security Conference (FC), 2011, pp. 127– 140.

[15] S. D. C. di Vimercati, S. Foresti, S. Paraboschi, G. Pelosi, and P. Samarati, "Efficient and Private Access to Outsourced Data,"WANG et al.: ORUTA: PRIVACY-PRESERVING PUBLIC AUDITING FOR SHARED DATA IN THE CLOUD 15 in Proc. IEEE International Conference on Distributed Computing Systems (ICDCS), 2011, pp. 710–719.

[16] B. Wang, B. Li, and H. Li, "Knox: Privacy-Preserving Auditing for Shared Data with Large Groups in the Cloud," Proc. 10th Int'l Conf. Applied Cryptography and Network Security (ACNS'12), pp. 507-525, June 2012.

[17] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, "Provable Data Possession at Untrusted Stores," Proc. 14th ACM Conf. Computer and Comm. Security (CCS '07), pp. 598-610, 2007.

[18] Y. Dodis, S.P. Vadhan, and D. Wichs, "Proofs of Retrievability via Hardness Amplification," Proc. Theory of Cryptography Conf. Theory of Cryptography (TCC), pp. 109-127, 2009.