Oruta: Privacy-Preserving Public Auditing for Shared Data in the Cloud

Sharddha Dangare[1], Swapnali Sakore[2], Rukmini Raut[3],
Vaishali Shinde[4]
*[1 2 3 4] (Department of Computer Engineering ,JSPM's RajarshiShahu College of Engineering
Pune, India)*

Abstract-When we are using cloud storage service, it is possible for data to be not only stored in the cloud, but also can shared across multiple users. It's a big challenge is to preserve identity privacy of public auditing for such shared data. It allows public auditing on shared data stored in the cloud by this first privacy preserving mechanism. For auditing the integrity of shared data it uses the ring signature to compute the verification information. The third party auditor is able to verify the integrity of shared data in the cloud. Hence, this is the mechanism who kept the identity of signer in shared data private from third party auditor. By using the auditing shared data it demonstrates effectiveness and efficiency

Keywords- Cloud computing, Public auditing, Privacy-preserving, Shared data, Third Party Auditor.

I. INTRODUCTION

In thismodel,privacy isaccomplished by allowingheartiest uploadtheirdata in multi clouds and data is split into multipleparts so it gives moreprotection. Currentworking scenarioinvolvespaperbasedworkforDataanalysisand verification.Data Storageis onewayto mitigate theprivacyconcern. Unauthorizeduserscanleakormisusethedata,thisproblemstillremains dueto thepaper based work.

Wepropose Oruta, aprivacy preserving public auditing mechanism. We useringsignatures toconstructhomomorphicauthenticators inOruta,sothatapublic verifierisabletoverify theintegrity ofshareddatawithout retrieving theentire data whiletheidentity ofthe signerinshareddata iskeptprivatefromthepublic verifier.Inaddition, this mechanism used tosupport batchauditing,whichcanperformmultipleauditing taskssimultaneously and improve the efficiencyof verification.

Forthefirsttimedatainserting in theEncryptionservice togenerateencryptionkey andthiskey isstoredonKeyStoragearea,and then encrypteddataisstoredonthe cloudstoragearea. Whentheuserrequeststhedata from decryption process,thekey and dataarecollectedattheDecryptionservicebuttheservicewillnotimmediately decrypt thedata,untilandunlessuser inserttheOTPsentonhismail.Whenuserwillenter correct OTP then thedata is decrypted byDecryption serviceand data is provided to the user.

Public auditing	Yes	Yes	Yes
Identity Privacy	No	Yes	Yes
Data Privacy	No	No	Yes

Table 1Comparison of System with Existing Mechanisms

II. RELATED WORK

In existing system the TPA is used to check the authentication of the user, it verifies the user whether it is valid or not. If the user is not authorized the TPA inform to the user that his data is used by some unauthorized person. But if the TPA isget hacked then the user will not get a notification mail from TPA. Authentication and verification is done by TPA and not byadmin. In existing cloud system, there are number of threats arisenand they are as follow:

1. Abuse and Nefarious use of cloud.
2. In secure Interfaces and API's.
3. Malicious Insiders.
4. Shared Technology Issues.
5. Data Loss and Outflow.
6. Account or Service Hijacking.

The boom in the cloud computing world has directed to a new period of on demand delivery of hosted service over a network. Cloud computing is a complex setup of software, hardware, processing and storage that is available as service. It has flexibility rendering user to customize the service appropriate to his needs. Inventions in virtualization and distributed systems have saved the path for interest in cloud

III. SYSTEM ARCHITECTURE

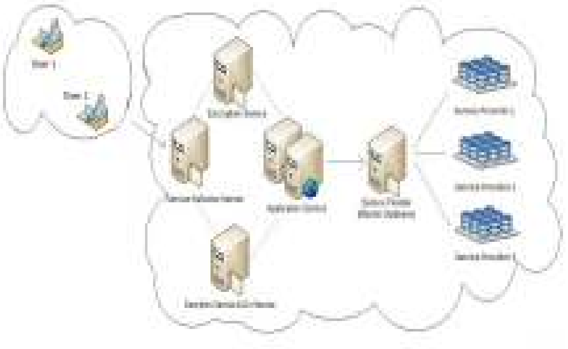

Fig1. system architecture

A cloud service provider offers the property of sharing and accessing the Resources at minor cost to users. In the cloud storage the Integrity of the data is focus on uncertainty and analysis, Due to failures of hardware and human errors data stored in untrusted cloud can easily vanished. Forchecking correctness of data, the traditionalapproach is to retrieve the entire data from cloud and for checking the correctness of signature to verify the data integrity in the cloud. In general the size of cloud data is huge, therefore the efficiency of using this traditional approach on cloud data is in uncertainty.

IV. PROPOSED SYSTEM

In our mechanism data is allocated into a small blocks and owner signed the block independently. During integritychecking the whole data is not retrieved instead of random combination of the entire block done. Currentpublic auditingmechanismscanactuallybeextendedtovalidate shareddata integrity. Toprotectthe personalinformation,itisnecessaryandacutetop reserveidentity privacyfrompublicverifiersduringpublic auditing. To overcome this problem, Oruta is proposed. Toconstruct homomorphicauthenticators inOruta, we developringsignatures. Therefore, withoutretrievingtheentiredata,public verifierisabletovalidatethe integrityofshareddata. Whilethesigner identity oneachblockin shareddataisreservedprivatefromthepublicverifier.

Tosupportbatchauditing,whichcanperformmultiple auditing taskssimultaneously; we extended this mechanism and develop the effectiveness of verification for multipleauditing tasks.

Modules:

1. Owner Registration
2. Third Party Auditor
3. User
4. Data Sharing

1. Owner Registration:

In this module an owner has to upload its files in a cloud server, he/she should register first. Then only he/she can be able to do it. For that he needs to fill the details in the registration form. These details are maintained in a database.

2. Owner Login:

In this module, any registered owner have to login, they should login by giving their email id and password.

3. User Registration:

In this module if a user wants to access the data which is stored in a cloud, he/she should register their details first. These details are maintained in a Database.

4. User Login:

If the user is an authorized user, he/she can download the file by using file id which has been stored by data owner when it was uploading.

V. ADVANTAGE

1. The client stores their data in the server without keeping a local copy.
2. It is of critical importance that the client should be able to verify the integrity of the data stored in the remote Un-trusted server.
3. It provide expert integrity checking service
4. Improve the efficiency of verification for multiple auditing tasks.
5. Keep data confidential against the auditor.
6. Allow dynamic updates of data in cloud

VI.DISADVANTAGE

1.As it is web based it is dependent on network traffic.

2.Data owners may share the data under the policy over attributes from multiple authorities: difficulty to encrypt data.

VII.CONCLUSION

To ensure cloud data storage security, it is critical to enable a TPA to evaluate the service quality from an objective and independent perspective. Public audit ability also allows clients to delegate the integrity verification tasks to TPA while they themselves can unreliable or not be able to commit necessary computation resources performing continuous verifications. Another major concern is how to construct verification protocols that can accommodate dynamic data files. In this paper we explored the problem of providing simultaneous public auditability and data dynamics for remote data integrity check in cloud computing.

REFERENCES

[1]M.Armbrust,A.Fox,R.Griffith,A.D.Joseph,R.H.Katz,A. Konwinski,G.Lee,D. A. Patterson,A.Rabkin,I.Stoica,andM.Zaharia,―AViewof CloudComputing,‖ Communicationsofthe ACM, vol. 53, no. 4, pp. 50–58, Apirl 2010.

[2]G.Ateniese,R.Burns,R.Curtmola,J.Herring,L.Kissner,Z.Peterson,andD.Song, ―ProvableDataPossessionatUntrustedStores,inProc.ACMConferenceonComputer and Communications Security(CCS), 2007, pp. 598–610.

[3]C.Wang,Q.Wang,K.Ren,andW.Lou,―Privacy-Preserving Public Auditing for Data Storage Security inCloudComputing,inProc.IEEEInternationalConferenceon Computer Communications (INFOCOM), 2010, pp. 525–533.

[4] R. L. Rivest, A. Shamir, and Y. Tauman, ―How to Leak a Secret, in Proc. InternationalConferenceontheTheory andApplicationofCryptology andInformation Security(ASIACRYPT).Springer Verlag, 2001, pp. 552–565.

[5]D. Boneh, C. Gentry,B.Lynn,and H.Shacham, ―Aggregateand VerifiablyEncrypted SignaturesfromBilinearMaps, inProc.InternationalConferenceontheTheoryand ApplicationsofCryptographicTechniques(EUROCRYPT).Springer-Verlag,2003,pp.416–432.

[6]H.Shachamand,B.Waters,―Compact Proofs of Retrievability in Proc.International Conference on theTheory and Application of Cryptology and Information Security (ASIACRYPT). Springer Verlag, 2008, pp. 90–107.

[7]Y.Zhu,H.Wang,Z.Hu,G.-J.Ahn,H.Hu,andS.S.Yau,―Dynamic Audit Services for Integrity Verification of Outsourced Storage inClouds ,in Proc.ACMSymposium on Applied Computing(SAC), 2011, pp. 1550–1557.

[8] R. Gellman, "Privacy in the clouds: Risks to privacy and confidentiality from cloud computing", Prepared for the World Privacy Forum, online at http://www.worldprivacyforum.org/pdf/WPF Cloud Privacy Report.pdf, Feb 2009.

[9] W. Itani, A. Kayssi, A. Chehab, "Privacy as a Service: Privacy-Aware Data Storage and Processing in Cloud Computing architectures," Eighth IEEE International Conference on Dependable, Autonomic and SecureComputing, Dec 2009.

[10] Cloud Security Alliance, "Security guidance for critical areas of focus in cloud computing," 2009, online at http://www.cloudsecurityalliance.org.