IJETIE International Journal of Emerging Technology and Innovative Engineering
Volume I, Issue 3, March 2015
ISSN: 2394 - 6598
www.ijetie.org

Security and Privacy for data sharing in a cloud computing using Ring Signature

[1] M.MAHA KRISHNA JEYANTHI ,[2]P.MUNEESWARI,[3]M.NITHYA,[#4]E.REVATHI
[1] *P.S.R RENGASAMY COLLEGE OF ENGINEERING FOR WOMEN*
mahakrishnajeyanthi@gmail.com,muneeswarilakshmi10@gmail.com,nithyamurugan1994@gmail.com
[#4]*ASST.PROFESSOR OF CSE,*
P.S.R RENGASAMY COLLEGE OF ENGINEERING FOR WOMEN
e.revathisri@gmail.com

Abstract-Cloud computing is an internet based computing which enables sharing of resources .The integrity of cloud data is uncertainity enables due to hardware or software failures and human errors.Data owners and public verifier are allow to efficiently audit cloud data integrity without retrieving the entire data from the cloud server .These are all to be designed in many mechanism.Public auditing on shared data stored in the cloud is supported by novel privacy preserving mechanism.we are using ring signature to audit the correctness of shared data.

Index terms- cloud computing,privacy preserving, public auditing shared data.

I. INTRODUCTION

Cloud service is used for user efficient and scalable data storage services.It is a lower marginal cost then traditional approach[1].

Due to software or hardware failures and human errors data stored in the cloud easily be corrupted(or)lost[3],[4].Before any data utilization the integrity of cloud data should be verified.The entire data from the cloud for data correctness in traditional approach example:RSA,MD5 several mechanism have been designed to efficiently perform integrity checking to allow not only a data owner itself but also a public verifier[7]. A public verifier is without downloading the entire data from cloud is to perform integrity checking,which is refered to as public auditing. Data is divided into many small blocks .Each and every block is differently signed by one of the two user.once the user is modify the shared file,user must know his/her private key.Inorder to public verifier correctly audit the entire data using appropriate public key to preserve identity on shared data is failed during public auditing.several auditing task are performed after public verifier who first learn that Alice is a more important role in a group because shared file blocks are always signed by Alice.onotherhand this public verifier easily reduce the eighth block it contained the higher value of data because this block is continuously modify the two different user in this way to protect the confidential information for preserving identity privacy from public verifier[8].

In this paper to solve the privacy issue on shared data using novel privacy preserving mechanism.we utilize the ring signature is used for homomorphic authenticator so the public verifier is able to verify the integrity of shared data without retrieving the e ntire data from cloud[14]. Each block in the signer identity is kept private from pubic verifier .If further using batch auditing to support perform multiple auditing task simultaneously.Oruta is utilizing WWRL to preserve privacy of data from public verifier.

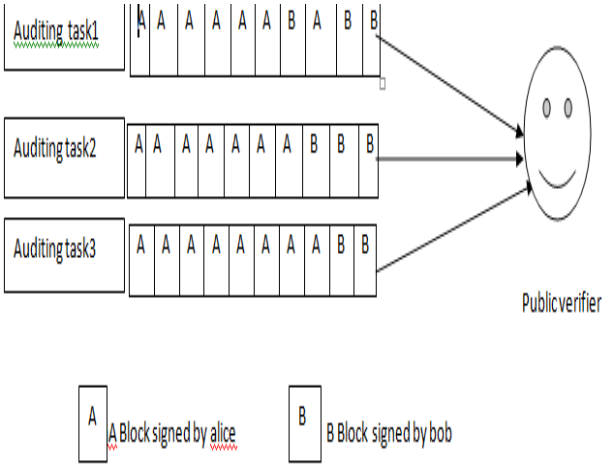

Fig 1.Alice and Bob share a data file in the cloud and a public verifier audits shared data integrity with existing mechanism.

II. SYSTEM MODEL

It involves cloud server group of users and the public verifier. Original users,number of group users are the two type of users in the group. First original user create a shared data in the cloud and the datas are shared into the group of users. Every user of the group is allowed to access and modify

IJETIE International Journal of Emerging Technology and Innovative Engineering
Volume I, Issue 3, March 2015
ISSN: 2394 - 6598
www.ijetie.org

the shared data[7].Third party auditor provide expect data auditing services.A public verifier to check the shared data integrity,public verifier sends an auditing challenges the cloud server. Cloud server response to the public verifier after receiving the auditing challenges.Finally public verifier verify the entire data.

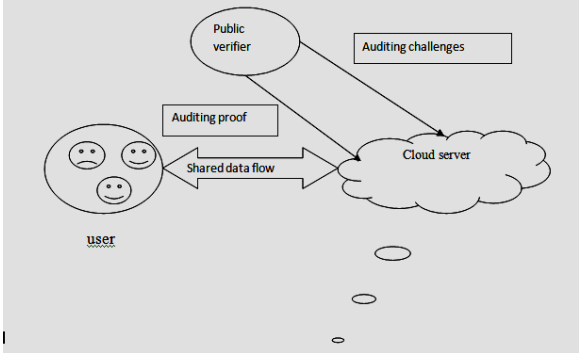

Fig 2.our system model includes cloud server,a group of users and a public verifier.

III. EXISTING SYSTEM

The first step is the provable data possession(PDP) mechanism to perform public auditing is to check the data storage correctness in an server without downloading the entire data. Moving a step forward Wang et all that is (WWRL)is designed to construct a public auditing mechanism for cloud data,so that in the time of pubic auditing the content of private data is belong to a personal user is not disclosed to a third party auditor.Data is divided into many small blocks each block is independently signed by owner.A public verifier could be a data user who would like to utilize the owner data via cloud or TPA who can provide expert integrity checking services.

DEMERITS

During the public auditing failing to preserve the identity privacy on shared data .They do not perform the multiple auditing task simultaneously.This mechanism is only suitable for auditing the integrity of personal data.

IV. PROPOSED SYSTEM

The proposed survey to solve the privacy issue on shared data.in this paper ,to produce a scheme called Oruta in cloud computing.oruta is a novel privacy preserving mechanism .we utilize the ring signature to construct a homomorphic authenticator in orutascheme by using this public verifier is able to verify the integrity or correctness of shared data without downloading the original data fully.To further extend our mechanism is support a multiple auditing task by using the concept of batch auditing.so the public verifier check the integrity of data in multiple auditing task simultaneously.

MERITS

The public verifier is able to correct to verifythe shared data integrity.During the process of public auditing a public verifier cannot differentiate the identity of signer on each block in shared data.

V. MODULES

The security and privacy for shared data in the cloud using ring signature are consists of following modules

1. Multi cloud storage
2. Ring Signature
3. Data Integrity
4. Third Party Auditor
5. Cloud user

5.1 Multi cloud storage

Each cloud admin consists of number of data blocks.The user in the cloud upload the data into multicloud.cloud computing is constructed based on open architecture and interfere[10] .A multi cloud allows client to easy acess their resources remotely through interfaces[8].

5.2 Ring Signature

Ring signature to construct a homomorphic authentication.so that public verifier is able to audit shared data without downloading the entire data,and yet it cannot differentiate who is the signer on each block.Ring signature is computed by one of the team member private key,but the verifier is cannot able to identify which one this.

5.3 Data Integrity

Data Integrity is an essential in database similar integrity of data storage in the cloud.The data integrity provides the validity of data assuring the consistency or regularity of the data. Data owner and public verifier to efficiently audit cloud data integrity without downloading the entire data from the cloud server.

5.4 Third Party Auditor

IJETIE International Journal of Emerging Technology and Innovative Engineering
Volume I, Issue 3, March 2015
ISSN: 2394 - 6598
www.ijetie.org

Third party auditor to verify the integrity of data that data are stored in cloud. Trusted third party view the user datas and upload into the distributed cloud[11]. If any modification by cloud owner message send to the third party auditor.Third party auditor check the correctness of data stored in the cloud.

5.5 Cloud User

A public verifier would be a data user who can like to utilize the owner data via Tpa or cloud who can provides the expert integrity checking services.[9]

VI. THREAT MODEL

6.1Integrity Threats

There are two kinds of threads that are releated to the integrity of shared data.First an opponent are try to corrupt the integrity of shared data.Second the hardware failures and human errors are the cloud service provider may unintentionally .

6.2 Privacy threat

Each block the identity of the signer is shared data are confidential and private to the group.the process of auditing,a public verifier who is allow to check the correctness of shared data integrity.

6.3 Design Objectives

6.3.1 Public Auditing

A public verifier without downloading the entire data from the cloud is verify the integrity of data stored in the cloud.

6.3.2 Correctness

A public verifier is needed to check the data integrity.

6.3.3 Unforgeability

A valid verification metadata (signature) is generated by each user in the group.

6.3.4 Identity privacy

During the process of auditing, A public verifier cannot identify the signer identity on each block in shared data

VII. PRILIMINARIES

7.1 Ring Signature

The content of ring signature was first developed by Rivest et al[28]in 2001.a verifier is convinced that a one of the group member private key is computed by using the signature but the verifier cannot identify whose one of the private key[13].A ring signature and group of a users,a verifier not able to differentiate the signers identity with a probability greater than 1/a.this property used to preserve the identity of the signer from a verifier.

7.2 Homomorphic authenticators

Homomorphic authenticator[10] is a basic tool is used to construct a public auditing mechanism(if user with a private key can generate a valid signature.)

7.3 Algorithm

Three algorithms are keygen,ringsign and ring verify

In keygen,his/her publickey and privatekey is generated for each user in the group.

Ring sign,in the group the user is able to generate a signature on its block identifier and on a block with his/her and all the group members public key

In ring verify a verifier is to check whether a given block is signed by a group member.

7.4 Support Dynamic operation

Group consists of number of user.each user in the group to modify the data stored in the cloud.dynamic operations are supported by the oruta.insert,delete,update operations are included in a dynamic operation[11].

When a user modifies a data stored in the cloud.after the modifies data user needs to recompute the signature,the content of the blocks are not modified.

TABLE1
Comparing amongdifferent mechanism

	PDP	WWRL	ORUTA
PublicAuditing	✓	✓	✓
Data Privacy	x	✓	✓
Identity privacy	x	x	✓

7.5 Batch auditing

Public verifier needs to check the correctness of data stored in the cloud .batch

auditing is perform multiple auditing task simultaneously and efficiency is improved.

We further extend oruta to support batch auditing which means public verifier check the integrity of data of multiple auditing task simultaneously[14]. The TPA can combine their queries and save in computation time.the comparison function that compares the aggregate authentication has a property that allows checking multiple message in one equation.

VIII. PERFORMANCE

First we analyse the communication cost and computation cost of Oruta and then evaluate the performance[12].

8.1 Communication cost

The two aspects are introduced for Oruta in communication cost they are auditing proof and auditing challenges.In auditing challenge{j,y}€ the communication cost is c(|q|+|n|)bits where |q| is the length of element.

8.2 Computation cost

In an auditing task, the public verifier are generate a random value to construct an auditing challenges,that only introduce a small cost in computation.the after received the auditing challenges.to compute an auditing proof $\{\lambda,\mu,\emptyset,\{id_j\}j_{\epsilon}j$ .to check an auditing proof for an verification.

TABLE2
Performance of auditing

System Parameters	K=100,d=10	
Storage usage	2GB+200MB(data + signatures)	
Selected block c	460	300
Communication cost	14.55 KB	10.95 KB
Auditing Time	1.94s	1.32s

IX. RELATED WORK

Provable data possession(PDP) developed by Ateniese et al,allows a verifier to identify the correctness of shared data and data stored in server .By utilize the RSA based homomorphic authenticator the verifier is able to audit the data without downloading the entire data from cloud and it is refered to as public auditing.

The mechanism is only suitable for audit the integrity of personal data. The original and the accurate file is added with a randomly value check blocks called sentinels.BLS signature is built from first scheme and pseudo random function is based on second one.To support an dynamic data presented an Provable data Possession mechanism based on its symmetric key and this mechanism can help to update the data and to delete the data and one main reason is to the insert operation are not available in this mechanism. The public mechanism developed by Wang et alare able to preserve the user confidential data from a public verifier.In addition ,to operate multiple auditing tasks from multiple user efficiently , they extend their mechanism to batch auditing by using signature.

Wang et al describes as the homomorphic tokens to show codes based on data distributed on different server.this mechanism is not able to support dynamic data ,to identify misbehaved server also. Compare to previous work this mechanism is to avoid the high decoding computation for data user and is to save computation resources for the online data owner in that time repair.

X. CONCLUSION

In this paper ,we propose oruta , a privacy preserving public auditing mechanism for shared data in the cloud.to construct an homomorphic authenticator by utilizing ring signature.so that a public verifier is to auditing the shared data integrity without retrieving the entire data ,and it cannot differentiate who is signer on each block.we extend our mechanism to support batch auditing of verifying multiple auditing task.

XI. FUTURE WORK

our future work there are two interesting problem will continue to study for future work. One is traceability,which mean group manager ability our future work is how to prove data freshness while still preserving identity privacy.

REFERENCE

[1] B. Wang, B. Li, and H. Li, “Oruta: Privacy-Preserving PublicAuditing for Shared Data in the Cloud,” Proc. IEEE Fifth Int’l Conf.Cloud Computing, pp. 295-302, 2012.

[2] 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, “A View of Cloud Computing,” Comm. ACM,vol. 53, no. 4, pp. 50-58, Apr. 2010.

[3] K. Ren, C. Wang, and Q. Wang, "Security Challenges for the PublicCloud," IEEE Internet Computing, vol. 16, no. 1, pp. 69-73, 2012.
[4] D. Song, E. Shi, I. Fischer, and U. Shankar, "Cloud Data Protectionfor the Masses," Computer, vol. 45, no. 1, pp. 39-45, 2012.
[5] C. Wang, Q. Wang, K. Ren, and W. Lou, "Privacy-PreservingPublic Auditing for Data Storage Security in Cloud Computing,"Proc. IEEE INFOCOM, pp. 525-533, 2010.
[6] B. Wang, M. Li, S.S. Chow, and H. Li, "Computing EncryptedCloud Data Efficiently under Multiple Keys," Proc. IEEE Conf.Comm. and Network Security (CNS '13), pp. 90-99, 2013.
[7] R. Rivest, A. Shamir, and L. Adleman, "A Method for ObtainingDigital Signatures and Public Key Cryptosystems," Comm. ACM,vol. 21, no. 2, pp. 120-126, 1978.
[8]The MD5 Message-Digest Algorithm (RFC1321).https://tools.ietf.org/html/rfc1321,\2014
[9] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner,Z. Peterson, and D. Song, "Provable Data Possession atUntrusted Stores," Proc. 14th ACM Conf. Computer and Comm.Security (CCS '07), pp. 598-610, 2007.
[10] H. Shacham and B. Waters, "Compact Proofs of Retrievability,"Proc. 14th Int'l Conf. Theory and Application of Cryptology and InformationSecurity: Advances in Cryptology (ASIACRYPT '08), pp. 90- 170 2008.
[11]C.Erway,A.Kupcu,C.Papamanthou,andR.Tamassia "Dynamic provable data possession","proc.16th ACM Conf.computer and communication security(css'09)pp.213-22,2009.
[12]Q.Wang,C.Wang,J.Li,K.Ren,andW.Lou"enabling public verifiability and Data dynamic for storage security in the cloud,"proc.14thEuropean Conf.Research in Computer Security(ESORICS'09),pp.355-370,2009
[13]c.Wang,Q.Wang,K.Ren,andW.Lou,"Ensuring data storage security in cloud computing,"proc.17th Int'l Workshop Quality of service(IWQos'09)pp.1-9,2009.
[14]B.Chen,R.Curtmola,G.Ateniese,andR.Burns,"Remote data checking for network coding based distributed data storage systems,"Proc.ACM Workshop cloud computing security workshop(CCSW'10)pp.31-42,2010.
[15]Y.Zhu,H.Wang,Z.Hu,G-J.Ahn,H.Hu and S.S Yau "Dynamic Audit Services for Integrity verification of outsourced storage in the cloud," Proc.ACMsymp.Appliedcomputing(SAC'11),pp.1550-1557 2011.
[16]N.Cao,S.Yu,Z.Yang,W.Lou and Y.T,Hou,"LT Codes –Based secure and reliable cloud storage services,"Proc IEEE INFOCOM,2012.