International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 02 Issue: 09 | Dec-2015 www.irjet.net p-ISSN: 2395-0072

Survey on Implementing Privacy Preserving Model for Shared Data in The Cloud

Geetanjali P. Rokade , Sambhaji Sarode.

MIT College Of Engineering ,

SPPU, Pune University, MS, India.

Abstract: ***Cloud Computing gives storage services where user can remotely stores and access data. Different types of applications would be developed using cloud services for different purposes such as data sharing in private or public domain, limiting the access rights to some groups or multiple users and as so on. It also reduces the load of maintenance and security of data on intranet network. Currently, the failure in hardware/software and human errors, the integrity, privacy and data access of cloud data is vulnerable, For these type of problems different mechanisms/solutions have been designed. However, maintaining integrity of shared data in cloud using public auditing is a critical task. Therefore user uses third party auditor to maintain and check integrity of data as and when required. Because of effective third party auditing verification process, the privacy maintained and not harmful to any party.So proposed system preserves privacy of shared data in cloud using public auditing. Ring signature could be used to compute and verify data which is required for auditing. With this mechanism the identity of signer on each block is kept private without disclosing data. It improves the data privacy by achieving traceability and the data freshness. Therefore proposed system will perform audit for some specific groups or multiple users efficiently.***

Keywords: - *Cloud Computing, Privacy Preserving, Data Storage, Public Auditing.*

1 Introduction

In today's life everything is depend on internet, and cloud computing is also internet based computing which made revolution. It is the biggest invention which uses advanced computational power and advance data sharing and data storing capabilities. Cloud computing could be a general term for the entire world that involves delivering hosted services over the net. These services generally divided into 3 categories: Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), and Software-as-a-Service(SaaS). The cloud service has distinct characteristics that differentiate it from ancient hosting. IaaS provides physical resources like central processing unit, network and storage etc. PaaS provides a platform for execution of application. SaaS provides completely different kind of application and net services to the users. Cloud is nothing but the large group of interconnected computers, on which we can store large number of data and run different application. Cloud provides shared pool of configurable computing resources and on demand network access. The main advantage of cloud is cost reduction; where as the prime disadvantage is nothing but the security. The cloud computing security has set of policies and technology to protect data, application and associated Infrastructure. Some security and privacy issues have to be considered. The only one thing was that the cloud computing lacks regarding the issue of data integrity, data accessed by unauthorized user and data privacy.[9]

Data integrity is nothing but the consistency of data, maintaining integrity of data in cloud is difficult task. And number of techniques has been proposed to protect integrity of data. Through this number of techniques the integrity can be checked and verify unauthorized change in original data without requesting original copy of data.[3]

The rest of the paper is divided into following sections.

Section 2 Existing system Techniques.Section 3 Literature survey.Section 4 Conclusion and Section 5 References for the survey.

2 EXISTING SYSTEM TECHNIQUES

2.1 MAC Based Solution [7]

This procedure utilized for information confirmation. In this instrument client transfer information hinders with MAC and Cloud supplier gives Secret key SK to TPA. Here TPA's errand is to recover information squares arbitrarily and MAC utilizes SK to check accuracy of information. Restrictions of this method are:

- Online weight to clients because of constrained use (i.e. Limited utilization) and statefull confirmation.
- Complexity in correspondence and calculation
- Maintaining and upgrading TPA states is troublesome.
- User need to download all the information to recomputed MAC and republish it on CS

2.2 HLA Based Solution

Without retrieving data block it provide efficient public auditing which aggregated and need constant bandwidth. By authenticating in linear mixture of individual block it is checks integrity of data block. But because of linear combination for authentication this technique is time consuming.[10]

2.3 Non linear Authentication

This technique to achieve cloud security Homomorphic non linear authenticator used with random masking technique. It uses RSA algorithm for cryptography which go after the process of digital signature for authentication of message.

2.4 Random masking technique

Jachak K. B. projected privacy conserving Third party auditing while not encryption. It uses a linear combination of sampled block within the server's response is masked with arbitrarily generated by a pseudo random function (PRF).[10]

2.5 Proxy re-signatures

Blaze proposed this technique in which semi-trusted proxy between two user to be used to translator signature. for example Alice and Bob, on the same block Alice signature is converted into Bob this is the concept of proxy.[11]

2.6 Homomorphic authentication

Homomorphic authentication has unforgebility (only a user with a secrete key will generate valid signature).The Homomorphic authentication additionally satisfy block less verification and non-malleability[8]. Blockless verifiability permits a verifier to audit the correctness of information keep within the cloud server with a special block [5], that cloud be a linear combination of all the blocks in information. If the integrity of the combined block is correct, then the verifier believes that the integrity of the complete information is correct. During this means, the verifier doesn't got to transfer all the blocks to examine the integrity of information. Non-malleability indicates that an individual cannot generate valid signatures no arbitrary blocks by linearly combining existing signatures.

3 LITERATURE SURVEY

3.1 Privacy Preserving Public Auditing for Secure Cloud Storage [1]

In this paper Cong Wang , Qian Wang etl. proposed the Homomorphic linear authenticator with random masking for preserving the privacy of public auditing system for shared data in the cloud , which not only release burden of shared data but also avoid users fear of data leakage when sharing data on cloud. In public key homomorphic linear authenticator Third party auditor can performed the auditing task without demanding the local copy of original data so it reduce the computation and communication overhead rather that other auditing approaches. They proposed their experiment conducted on Amazon EC2 instance.

In this system arbitrariness generated by server is masked with the linear grouping of sampled blocks in the servers reply. With the help of random masking , third party auditor cannot build up exact group of linear equation and cannot resulting users data contents, there is no matter that how many sets of file blocks collected. For better efficiency third party auditor used multiple auditing in batch manner.

3.2 Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing[6]

In this paper Qian Wang, Cong Wang ,etl. proposedthe techniques which achieve both the public auditing and also dynamic data operations. To achieve effective data dynamic, use Merkle Hash Tree construction for block label authentication. And to handle effective auditing task bilinear aggregate signature would be used and extend over multiuser settings, where TPA can do multiple auditing tasks simultaneously.

System model has three different entities which are as follows: Client: can be individual user or organization how has large number of data files to store on cloud and relies for data maintenance and computation. Cloud Storage Server: cloud service provider can managed it,which maintain client data and has storage space and computation resources. Third Party Auditor : On the behalf of client request it can manage all cloud storage services.

Then some design goals can be as follows: Public auditablity, Dynamic data operation support and Blockless Verification. The system has Merkel Tree Hash which is well authentication structure, which securely and effectively prove that the set of element are undamaged and unaltered. Then to support effectively public auditing system resort on homomorphic authenticator, which is unforgeable metadata which generated from individual data blocks.

3.3 Towards Secure and Dependable Storage Services in Cloud Computing [2]

In this paper Cong Wang , Qian Wang , etl . proposed flexible distributed storage integrity auditing technique which make use of homomorphic token and distributed erasure-coded data , through this users can audit the cloud storage with very low communication and computation cost. This system not only gives the auditing result of cloud storage correctness guarantee but also achieves very fast identification of misbehaving server .It also performed efficient dynamic operations on outsourcing data, which include block modification, deletion and append, And highly efficient on Byzantine failure, malicious data modification attack and also on server colluding attacks.

The three main aspects are summarized in this paper as:

1. Compared to other system this system proposed the scheme to achieve the integration of storage appropriateness insurance and data error localization that is detection of misbehaving server(s).

2. Unlike other works for ensuring data integrity, the new technique supports secure and efficient dynamic operations on data blocks, like as update, delete and append.

3. The experiment result prove that the proposed system is highly efficient and security analysis shows that this scheme is flexible against Byzantine failure, malicious data modification attack and also on server colluding attacks.

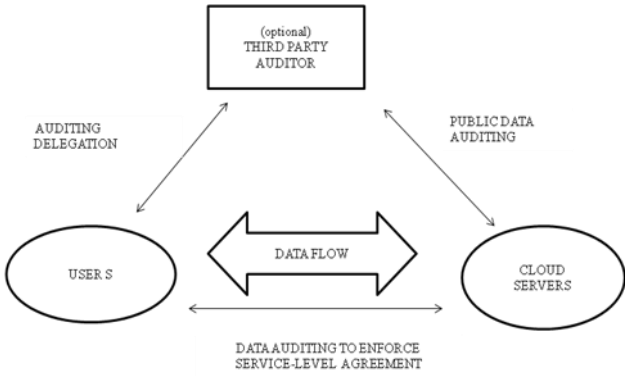

figure 1. system model public auditing of shared data

It include three different entities in their system model that can be as : User, Cloud Server and Third party auditor as shown in figure. Then they apply some dynamic data verification and operation to design following goals that are as : Storage correctness, Fast localization , Dynamic data support, Dependability and Lightweight. Then to maintain correctness of storage they used some algorithms as Token pre-computation then correctness proof and error localization, and error recovery. To achieve the data integrity and availability of dependable cloud storage services for users, they proposed effective and efficient and flexible distributed technique with effective dynamic data support, which include block data update, delete and append. They use erasure-correcting code technique in file sharing preparation to provide redundancy parity vectors and assurance the data dependability.

3.4 An Efficient and Secure Dynamic Auditing Protocol for Data Storage in Cloud Computing[4]

In this paper, Kan Yang etl. Design an auditing structure for cloud storage systems and propose an efficient and privacy-preserving auditing protocol.PoR method which is use to generate an encoded result with the challenge stamp by using the Bilinearity property of the bilinear pairing, such that in this the auditor cannot decrypt it but can verify the exactness of the proof. Without using the mask technique, method does not require any trusted organizer during the batch auditing for multiple clouds. On the other side, this method, they let the server compute the result as an intermediate value of the verification, such that the auditor can directly use this value to verify the exactness of the proof.

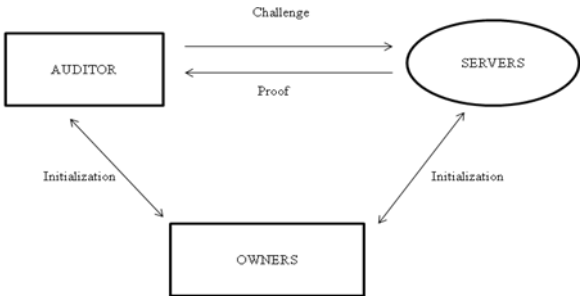

figure 2. system model of data storage auditing.

3.5 Oruta : Privacy Preserving Public Auditing for shared Data in the cloud[8]

In this Bonyang Wang etl. proposed that the a novel Privacy Preserving Technique which support the shared data public auditing in the cloud. System uses Homomorphic Authenticator technique with ring signature to compute and verify the correctness of the data. Signature on each data block is kept private from the verifier, how verify the data integrity without retrieving the entire data files. This mechanism is useful to perform simultaneous multiple auditing task instead of verify one by one.

System has some design objective as: Public auditing, Correctness, Unforgeability and Identity privacy. The homomorphic authenticator ring signature technique contains three algorithm in their construction as: KeyGen, RingSign and RingVerify ,whereas the public auditing technique contains the five algorithms as: KeyGen, SigGen, Modify and ProofGen and ProofVerify. In RingSign, User in a group can generate a signature on each block and block identifier has his/her secrete key and other group member's public key. In RingVerify , verifier check each block signed of group member.

To further improve the efficiency of multiple auditing task this mechanism support batch auditing. But this system has the problem of traceability and data freshness while preserving the identity privacy and even the re-computation introduce by the dynamic group.

3.6 Panda: Public Auditing for Shared Data with Efficient User Revocation in the Cloud[6]

In this paper Boyang Wang etl. Proposed, public auditing mechanism in which the previously signed block of revoked user must be re-sign by current user. In this proxy-resignature is used for re-sign blocks at the time of user revocation on the behalf of existing user so there is no need of download and re-sign block of data to existing user. Proxy re-signature provides a semi-trusted proxy between two user to be used as translator of signature.

In this Homomorphic Authenticable proxy re-signature is use to construct public auditing technique. As it preserve the identity privacy and also support blockless verifiability. There are five algorithms: KeyGen, ReKey, Sign, ReSign and Verify were used in construction and also bilinear map based properties, to correct verification in verify. To improve the effectiveness of user revocation, cloud performs as a proxy and change signature for user. [11]

This system have generally two levels of signature in different forms and they need to verify separately, so achieveingblockless verifiability of two level signature and verify them together in public auditing technique is one issue in this system.

Table 1. Literature survey

SR. NO.	TITLE	METHODS	PROS	CONS
1	Privacy Preserving Public Auditing for Secure Cloud Storage. Cong Wang, Member, IEEE, Sherman S.M. Chow, Qian Wang, Member, IEEE . 2013[1]	Homomorphic Linear Authenticator and Random Masking	This method allow Secure public data auditing.	System is secure but some user files are not encrypted on some open source cloud data storage. Privacy of data cannot preserve.
2	Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing. Cong Wang, Student Member, IEEE, Qian Wang, Student Member, IEEE, IEEE Transaction On Parallel and Distributed system May 2011. [6]	Message Authenticated code	It provide secure auditing of shared data	High communication and computation complexity.
3	Towards Secure and Dependable Storage Services in Cloud Computing . Cong Wang , Qian Wang , Student Member IEEE [2]	Homomorphic Token and Distributed Erasure-Coded Data	Audit cloud data with lightweight communication and computation cost	System is secure but some user files are not encrypted on some open source cloud data storage.
4	An Efficient and Secure Dynamic Auditing Protocol for Data Storage in Cloud Computing Kan Yang , XiaohuaJia ,IEEE Transaction On Parallel and Distributed system september 2013.[4]	Proof of Retriviability with bilinearity property of bilinear paring	Low communication and computation cost	This scheme does not support the efficient privacy preserving public auditing of shared data
5	Oruta : Privacy Preserving Public Auditing for shared Data in the cloud. B. Wang, Student Menber, IEEE , Baochun Li, Senior Member, IEEE, IEEE Transaction On Cloud Computing Vol.2, No.1, January-March 2014.[8]	Homomorphic Authenticator with ring signature	To perform simultaneous multiple auditing task instead of verify one by one.	Traceability and data freshness while preserving the identity privacy and even the re-computation introduce by the dynamic group
6	Panda : Public Auditing for Shared Data with Efficient User Revocation in the Cloud. B. Wang, Student Member , IEEE, B.Li, Senior Member, IEEE. IEEE Transaction On Services Computing, Vol.8, No.1, January/February 2015 [5]	Homomorphic Authenticable proxy re-signature	Preserve the identity privacy And also audit data efficiently.	Achieving blockless verifiability of two level signature and verify them together in public auditing technique

4 CONCLUSION

In this survey paper we have try to explore different techniques related to preserving the privacy for shared data in the cloud up till now. We have discussed about different methods used for the public auditing and also advantages and disadvantages of this technique.

5 REFERENCES

[1] Cong Wang, Sherman S.M. Chow, Qian Wang, Kui Ren, and Wenjing Lou," Privacy-Preserving Public Auditing for Secure Cloud Storage", IEEE Transactions On Computers, Vol. 62, No. 2, February 2013

[2] Cong Wang, Student Member, IEEE, Qian Wang, Student Member, IEEE, Kui Ren, Member, IEEE, "Towards Secure and Dependable Storage Services in Cloud Computing"

[3] Cong Wang, Qian Wang, and Kui Ren Department of ECE Illinois Institute of Technology Email: {cwang, qwang, kren}@ece.iit.edu "Ensuring Data Storage Security in Cloud Computing".

[4] Kan Yang "An Efficient and Secure Dynamic Auditing Protocol for Data Storage in Cloud Computing", IEEE Transactions OnParalleland Distributed Systems, VOL. 24, NO. 9, SEPTEMBER 2013

[5] B. Wang, Student Member , IEEE, B. Li, Senior Member, IEEE and Hui Li, Member, "Panda: Public Auditing for Shared Data with Efficient User Revocation in the Cloud ", IEEE Transaction On Services Computing, Vol.8, No.1, January/February 2015

[6] Qian Wang, IEEE, Cong Wang, Kui Ren, Wenjing Lou, and Jin Li, " Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing", IEEE Transactions On Parallel And Distributed Systems, VOL. 22, NO. 5, MAY 2011.

[7] S. Ashli, B. Gowrie, S. Acanthi, "Privacy-Preserving Public Auditing In Cloud Using HMAC Algorithm", in International Journal of Recent Technology and Engineering (IJRTE) ISSN: 2277-3878, Volume-2, Issue-1, March 2013.

[8] B. Wang, Student Member, IEEE , B. Li, Senior Member, IEEE, and Hui Li, Member , IEEE "Oruta: Privacy Preserving Public Auditing " IEEE Transaction On Cloud Computing Vol.2, No.1, January-March 2014.

[9] X. Liu, Y. Zhang, B. Wang, and J. Yan, "Mona: Secure Multi- Owner Data Sharing for Dynamic Groups in the Cloud," IEEE Trans. Parallel and Distributed Systems, vol. 24, no. 6, pp. 1182-1191, June 2013.

[10] Jachak K. B. and GagareG.J."Homomorphic Authentication with Random Masking Technique Ensuring Privacy and Security in Cloud Computing" , Bioinformatics Security Information ,vol.2,no.2,pp.49-52,ISSN.2249-9423,12 April2012

[11] B. Wang, B. Li and H. Li, " Public Auditing for Shared Data with Efficient User Revocation in the Cloud ", Proc.IEEE INFOCOM, pp.2904-2912, 2013.