ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)
Vol. 4, Issue 2 (Apr. - Jun. 2016)
International Journal of Advanced Research in Computer Science & Technology (IJARCST 2016)

Methods for Secure Public Auditing in Cloud Storage

[I]Tejashwini K, [II]Sanjay Kumar C K
[I]PG Student, Dept. of IS&E, The National Institute of Engineering, Mysore, India
[II]Assistant Professor, Dept. of MCA, The National Institute of Engineering, Mysore, India

Abstract
Cloud storage, enabling users to store their data in a server and provide privacy to the user data. Nowadays cloud is becoming a major vehicle for storage of data, data owners outsource their data in cloud so major problem becomes is the data integrity and privacy of data in cloud. In this paper many methods and schemes are discussed to ensure data integrity and security in cloud that consists of methods like MAC based, HLA based, Proxy Re-signature and some cryptography based methods are used for securing data. TPA is used for public auditing for data integrity in cloud to ensure the privacy of owners' data in cloud.

Keywords
Public auditing, Third party auditor, proxy, cloud storage

I. Introduction

Cloud computing is the emerging technology where data is being centralized or outsourced to the cloud and it provides many advantages but it also brings security threats towards user's outsourced data. As users no longer audit the data and cannot stay in online. To reduce the online burden of the user and to audit the data in the cloud, introduces TPA to audit the user outsourced data when needed.

This paper discusses about methods used to public audit in the cloud storage. The overall summery of the schemes where most of the work done during the period of 2006-2008 we can see that the method, which are not privacy preserving and its communication and computation complexity are high. During 2009-2011, where uses secret keys that is used for auditing and securing data but once all possible secret keys are exhausted then its complex. In 2012-2014 work done are to reduce the online burden of users they need for auditing, Third party auditor is used for auditing but TPA gain knowledge about user data. And now 2015 where many methods are introduced to protect the data linkage to the TPA and makes auditing more secure.

The methods like a MAC based solution, uses secret key to check correctness of stored data on the cloud.

Homomarphic linear authentication based solution, authenticates a linear combination of the individual data blocks and supports efficient public auditing without retrieving data blocks. Public auditing for shared data when the user group is revoked. The idea of proxy Re-signature is used to avoid the downloading of entire data blocks.

And also non linear authentication uses RSA algorithm for encryption and decryption which follows the process of digital signatures for message authentication. And many methods and schemes are discussed for secure auditing of users' data in the cloud.

II. Literature Survey

The data owners outsource their data in cloud so major problem becomes the security of data in cloud.

To ensure data integrity and security in cloud many methods and schemes are introduced. Here the survey on preserving privacy and auditing of owners' data in cloud.

Considering the public auditing for data integrity in cloud Boyangwang [1], proposed public auditing for shared data. The user group where the data is shared between them, if a user misbehaves or damage any data in the cloud that user is removed and he no longer exists in that group. In this case the auditing of data integrity should be checked by TPA. Where TPA utilizes the idea of proxy Re-signature to avoid the downloading of entire data blocks to re-sign by the existing user, and the cloud gets all the user details and converts to existing user signature and re-sign the blocks, which were signed by the removed user with a re-signing key. But this scheme fails when the total number of re-signing keys is increased that the cloud needs to manage when cloud data is shared by a very large number of group users.

Public auditing for shared data is improved by Kai He [2], where the cloud convert signatures computed by different users into signatures computed by challenge user, who is one particular member in the cloud service users. This is achieved by utilizing proxy Re-signature, when generating signature proof. But the signatures stored in cloud server are not changed. To audit the stored data the challenged signatures are aggregated to form intermediate values on the cloud server, so that the auditor can check the integrity of data only with challenge user's public key.

P. Divya [3], proposed a scheme which supports dynamic groups efficiently, where user revocation made easy through novel revocation list without updating the secret keys of the remaining users. The size and computation overhead of encryption are constant and independent with the number of revoked users but the real identity of data owners can be revealed by the group manager when the user is removed from group or group manager itself can cause damage to the outsourced data.

G. Shreedevi [4], proposed multiple trusted TPA for data auditing in cloud. By using proxy Re-signature the first TPA to create initial verification key and creates revocation list, which contains the user information and another TPA to re-sign blocks on behalf of existing users so that existing user need not to re-sign and also need not download the entire data to re-sign the block of data. The multiple trusted TPA's are used for security reasons need to check that no information is revealed to the TPAs.

Prof. SawanBaghel [5], implements the efficient storage of data in cloud and also security considering various security issues in cloud. This scheme uses RSA algorithm for secure communication, where data is outsourced to cloud safely and MD5 algorithm for data integrity and Kerberos type of authentication system as third party auditor and checks the data integrity in the cloud. But this scheme is improved by AparajitaSai [6], which introduces TPA for auditing.

Partitioning of data is proposed by AparajitaSain [6], partitioning of data is the concept used in this scheme and slicing mechanism is used to divide data for storage. RSA based Storage Security

ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)

(RSASS) method is used for dynamic operations of shared data by enhancing existing RSA based signature by Prof. SawanBaghel [5]. Where TPA performs the partitioning of files and performs encryption and decryption of partition.

Further Rushikesh P. Dhanokar [7], proposes TPA to check the integrity of data in the cloud. Encryption of data is done using RSA algorithm using homomorphic linear authentication (HLA) and SHA-2 for data integrity. In this scheme auditor needs to maintain state of keys and all keyed hashes are used is affected by online burden on users.

In previous scheme Prof. SawanBaghel and Rushikesh P. Dhanokar [5,7], which are based on RSA which has some loopholes in encryption techniques this can be overcome using Mr.Santosh [8], advanced encryption standards (AES) encryption algorithm, which increases efficiency of TPA for batch auditing and are executed in batch wise fashion. It can be extended to public verification of data of multiple auditing tasks simultaneously.

For secured data storage G.Ranjith [9], where TPA provides the fault tolerance which is done using intelligence based security system auditing with CIA triad and AAA security management to protect data in cloud. This scheme needs to concentrate on data redundancy where more data replication is done in the cloud.

Data is recovered using backup and restore method by Prof. KalyaniWaghmare [10], where TPA is introduced to audit user's data in cloud but in this method TPA will give an idea about the damage file or corrupted file but will not say exactly which file and also inform CSP about this to improve their service. This scheme will not give exact information about the damage file.

Further to get auditing done perfectly introduced TPA by Ms. Suvidha R. Sardar [11], where data integrity is checked by TPA and informed to the user with full information where in this scheme users data is protected against external auditors is based on public key based on HAL and make randomness and uses BLS signature for authentication but this limits auditing using authenticators.

ShrutiBatham [12], can improve HAL algorithm of Ms. Suvidha R. Sardar [11], by improving aggregate keys generation based on fixed key size. In previous HAL based on homomorphic linear authentication which may reveal user data information to TPA and TPA has to maintain and update state between audits can be difficult and takes long time while decrypting with long length key. These can be overcome in this improved HAL algorithm.

Message recoverable signature by Mehmet SabirKiraz [13], the message itself is included in verification that was not there in the previous schemes. A valid signature is sufficient to recover the original message. Efficiency advantage compared to G.Ranjith [9], BLS short signature. This scheme is robust, in the sense that the message will be still recoverable unless the signatures are damaged.

Using multifunction Jianhong Zhang [14], introduces proxy signature to reduce the cloud user's computation burden. Lagrange-interpolation polynomial is used to preserve identity of data without increasing computation cost and communication overhead. Merkle hash tree and Index- Switch table to secure dynamic operation of shared data and private key to protect data.

M. Maha Krishna Jeyanthi [15], proposed to solve privacy issues on shared data in cloud. This scheme uses Ring Signature to construct a homomorphic authenticator.

The public verifier or TPA can verify the data correctness without downloading entire data and TPA cannot identity a signer on each block in shared data.

Franklin Malugu [16], this scheme is the extension of Mehmet SabirKiraz [13], where the Ring signature is used to construct homomorphic authenticators so that TPA can verify data identity of shared data. This is extended to support batch auditing, which perform multiple auditing tasks simultaneously and leverage index hash tables to support both dynamic data and group.

A new homomorphic authenticable Ring signature (HARS) by KedarJayeshRasal [17], scheme. Which is extension of classic ring signature of M. Maha Krishna Jeyanthi [15], scheme. The traditional ring signature do not support block less verifiability, where whole data file has to downloaded to verify the correctness of shared data. To overcome this HARS is used, which supports block less verification for TPA.

B. BanuPriya [18], this paper discussed with various methods for public auditing mechanisms for data integrity in cloud. The auditing of data in cloud can be performed in various ways and in this paper discusses some of auditing mechanisms like Remote Data Checking (RDC) an avoidance tool and public key cryptosystem the MD5 message-digest algorithm are discussed.

Mr. J. Moses Pushparaj [19], proposed a privacy preserving public auditing for shared data in cloud using Hash Based Verification (HBV) and uses Ring signature to compute meta data verification on shared metadata. And this makes TPA cannot reveal the identity of signer on the block of shared data. This can be improved the data traceability of shared data using complex polynomial construction in Hash Based Verification method.

Mechanism for privacy preserving public auditing by PoojaKapadne [20], a trusted proxy is added between a group of users and the cloud in the system model. Each member's data is collected, signed and uploaded to the cloud by this trusted proxy. A public verifier can only verify and learn that it is the proxy signs the data, but cannot learn the identities of group members. But security of this method is threatened by the single point failure of the proxy.

Guangyang Yang [21], in order to deal with the distributed denial-of-service (DDOS) attack, proposes authorized auditing scheme with constrained auditing. A TPA's constrained auditing number is decided by the user.

Once the number of TPA's auditing reaches the constraint cloud server will not respond to the TPA's challenges, which can overcome with the threat of DDOS attack.

Multiple auditing mechanisms (MAM) are used by Elakkiya. B [22], where data dynamics is provided and user can perform insertion, deletion and modification on the block. Keys are generated by public key algorithm. A public verifier can audit the integrity of shared data without retrieving the entire data from the cloud. Scalability can be improved by reducing the number of re-singing keys as in Boyangwang [1], and public auditing for multiple auditing tasks.

Securely introduces an effective TPA by RemidicherlaRupa [23], an aggregate homomorphic linear authenticator with random masking technique. A protocol, the linear combination of sampled blocks in the server's response is masked with randomness generated by the server using Pseudo random function (PRF) and also uses the HAL Ms. Suvidha R. Sardar [11], which is based on the short signature scheme proposed by BLS.

Split cloud storage by DhanyaShenoy [24], is developed for integrity check via TPA, providing data privacy as well as public audit ability. The data is encrypted at the client then the signature is generated. The signature is stored at different clouds. Whenever audit takes place the data parts are merged and a new signature is generated then data integrity checking is done by TPA through equality checking of both signatures.

Chuanhe Huang [25], proposed a public auditing scheme for cloud storage system, in which deduplication of encryption data and data integrity checking can be achieved within the same framework. The cloud server can correctly check the ownership for new owners and the auditor can correctly check the integrity of deduplication data. This scheme supports deduplication of encryption data by using the method of proxy re-encryption and also achieves deduplication of data tags by aggregating the tags from different owners.

The methods schemes used for enabling privacy protecting public auditing and its advantages and disadvantages are listed below

Methods	Advantages	Disadvantages
User revocation	Avoid downloading of entire data blocks for auditing.	Fails when the total number of re-signing keys is increased.
User revocation using challenge user	Aggregate the signature under one challenge user.	Fails if the challenge user's data is crashed.
User revocation supports dynamic groups	Forms revocation list without updating the secret keys	Group manager can reveal the real identity of data owner
Using multiple trusted TPA	Multiple TPAs can handle both auditing and owner part of work.	Fails if the owner's data information is revealed to the TPAs
Using RSA and MD5 algorithms	Secure the data stored in cloud	Fails if authentication system is hacked
By partitioning of data	Reduces the storage maintenance by storing data in different servers	TPA handles partitioning of data which can gain knowledge of user data
Using homomorphic linear authentication (HLA) and SHA-2	Encryption of data is done in more secure way	Auditor needs to maintain state of keys and also affected by online burden on users
Using AES encryption algorithm	Increases efficiency of TPA for batch auditing	Difficult increases when large data is stored in cloud
AAA security management	Provides fault tolerance using intelligence based security	Needs to concentrate on data redundancy
Backup and restore method	TPA will give an idea about the damage file	Will not give exact information about the damage file
BLS short signature	Valid signature is sufficient to recover original message	Fails if signature itself gets damaged
Using ring signature	TPA cannot identify a signer on each block of data	Fails to recover the authenticators and do not support blockless verification
Homomorphic Authenticable Ring Signature (HARS)	Supports blockless verification for TPA	Fails if many servers or data is crashed
Hash based verification (HBV)	TPA cannot reveal the identity of signer on the data blocks	Can be improved in the data traceability
Adding proxy server	Each member's data is signed and uploaded to cloud by proxy	Security is threatened by single point failure of proxy
Multiple auditing mechanisms (MAM)	Data dynamics is provided	Scalability can be improved by reducing re-signing keys
Constrained auditing	Overcomes the threat of DDOS attack	TPA's auditing is constrained and cloud server will not respond
Split cloud storage	Signature is stored at different cloud	TPA needs to check equally both signature
Deduplication of encryption data	deduplication of data by aggregating the different owners	Fails if one user is removed from the group.

III. Conclusions

In this paper, we studied various methods and techniques used for a privacy preserving public auditing system for data storage security in Cloud Computing. As TPA will inform about data integrity and secure the user data in the cloud. All the methods used for secure public auditing are discussed.

References

[1] *Boyang Wang, Baochun Li and Hui Li, "Public auditing for shared data with efficient user Revocation in the cloud,"*

[2] *Kai He, Chuanhe Huang, Kan Yang and Jiaoli Shi, "Identity-preserving public auditing for shared cloud data," in the 23rd IEEE International Symposium on Quality of Service (IWQOS), 2015.*

[3] *P.Divya and B. Sivananthan, "A Privacy-preserving access control with robust data authenticity for cloud group," Journal of Scientific and Computational Intelligence, vol. 2, issue 1, Sep 2015.*

[4] *G. Shreedevi and K.G. Arunkumar, "Survey of public auditing of shared data with multiple third party auditor with efficient user revocation in the cloud," Journal of Computer Technology and Applications, vol.6 (2), Mar-Apr 2015.*

[5] *Prof. SawanBaghel and Prof. GauravSaboo, "Efficient Cryptographic algorithms for cloud storage security," Journal of Emerging Technologies in Engineering Research, vol.3, issue 2, Nov 2015.*

ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)

[6] *Aparajith Sain, ParnaDutta, NamrataDwivedi, PradnyaChikhale and VrundaBhusari, "Enhancing data storage security in cloud computing using PDDS technique," Journal of Advanced Research in Computer Engineering and Technology, vol. 4, issue 2, Feb 2015.*

[7] *Rushikesh P. Dhanokar and Prof. Gitanjali S. Mate, "Auditing of cloud data with privacy preserving using TPA," IOSR Journal of Computer Engineering, 2015.*

[8] *Mr. Santash P. Jadhav and Prof. B. R. Nandwalkar, "Efficient cloud computing with secure data storage using AES," Journal of Advanced Research in Computer and Communication Engineering, vol. 4, issue 6, June 2105.*

[9] *G. Ranjith, J. Vijaya Chandra, P. Sagarika and B. Prathusha, "Intelligence based Authentication- Authorization and Auditing for secured data storage," Journal of Advanced in Engineering and Technology, vol. 8, issue 4, Aug 2015.*

[10] *PriyaRupeja and Prof. KalyaniWaghmare. "Privacy preserving public auditing and recovery using backup and restore method for secure cloud storage," Journal of Engineering and Computer Science, vol. 4, issue 1, Jan 2015.*

[11] *Ms. Suvidha R. Sardar and Dr. A. D. Gawande, "Implementation of privacy- preservation in public cloud storage: a Review," Journal of Advanced Research in Computer Science and Software Engineering, vol. 5, issue 4, April 2015.*

[12] *ShrutiBatham, UmeshLilhore and SiniShibu, "Improve HLA based encryption process using fixed size aggregate key generation," Journal of Modern Trends in Engineering and Research, vol. 2, issue 1, Jan 2015.*

[13] *Mehmet SabirKiraz, Isa Sertkaya and OsmanbeyUzunkol, "An Efficient ID-based message recoverable privacy preserving auditing scheme," in the 13th Annual IEEE Conference on privacy security and trust, 2015.*

[14] *Jianhong Zhang and Xubing Zhao, "Privacy- preserving public auditing scheme for shared data with supporting multi function," Journal of communications, vol. 10, no. 7, July 2015.*

[15] *M. Maha Krishna Jeyanthi, P. Muneeswari, M. Nithya and E. Revathi, "Security and privacy for data sharing in a cloud computing using Ring signature," Journal of Emerging Technology and Innovative Engineering, vol. 1, issue 3, March 2015.*

[16] *Franklin Malugu and K. Suresh Babu, "Public audit of cloud shared data by using efficient privacy preserving scheme," Journal of Scientific Engineering and Research, vol. 3, issue 4, April 2015.*

[17] *KedarJayeshRasal, Dr. S.V. Gumaste and Sandip A. Kahate, "Survey on privacy preserving public auditing techniques for shared data in the cloud," Journal of Engineering Science and Innovative Technology, vol. 4, issue 3, May 2015.*

[18] *B. BanuPriya, V. Sobhana and Prof. MishmalaSushith, "Concise survey on privacy preserving techniques in cloud," Advanced ResearchJournal in Science Engineering and Technology, vol. 2, issue 2, Feb 2015.*

[19] *Mr. J. Moses Pushparaj and Ms. K. Rekha, "Enhanced Privacy preserving metadata verification by accomplishing traceability for shared data in cloud," IJAICT, vol. 2, issue 2, June 2015.*

[20] *PoojaKapadne and Deepak Sharma, "Mechanism for privacy preserving public auditing for shared data in cloud," Journal of Engineering Science and Innovative Technology, vol. 4, issue 5, Sep 2015.*

[21] *Guangyang Yang, Hui Xia, WentingShen, XiuXiu Jiang and Jia Yu, "Public data auditing with constrained auditing number for cloud storage," Journal of security and its applications, vol. 9, issue 9, 2015.*

[22] *ElakkiyaB,Savitha S, VaniParvathi G, Saranya A and Sindhu S, "Public auditing and data dynamics for cloud storage," Journal of Computer Science and Engineering Communications, vol. 3, issue 3, 2015.*

[23] *RemidicherlaRupa, "Auditing outsourced data on cloud using HLA with random masking technique," Journal of Engineering Development and Research, vol. 3, issue 3, 2015.*

[24] *DhanyaShenoy and N. P.Chawande, "Privacy preserving secure auditing scheme with split cloud storage," Journal of Engineering Trends and Technology, vol. 23, no. 4, May 2015.*

[25] *Kai He, Chuanhe Huang, Haozhou, Jiaolishi, Xiaomao Wang and Feng Dan, "Public auditing for encryption data with client-side deduplication in cloud storage," Wuhan University Journal of Natural sciences, vol. 20, issue 4, August 2015.*