International Journal of Applied Engineering Research
ISSN 0973-4562 Volume 10, Number 3 (2015) pp. 5435-5442

http://www.ripublication.com

A Review of Public Auditing Schemes in the Cloud Computing

N.Jayaprakash[1], J.Ramesh Babu[2], T.Dhikhi[3]

[1]M.E,Department Of CSE, Saveetha University, Saveetha Nagar, Thandalam, Chennai-602105, India
[2]M.E, Department Of CSE, Saveetha University, Saveetha Nagar, Thandalam, Chennai-602105, India
[3]Assistant Professor, Department Of CSE, Saveetha University, Saveetha Nagar, Thandalam, Chennai-602105, India
javidprakash@gmail.com
Rameshbabu18.j@gmail.com
dhikhi@gmail.com

Abstract

Various Business sectors are diversely located in the globe. This factor enforces these organizations to keep their data in the cloud infrastructure which is one of the efficient ways to securely organize the data between different sectors of same organization as well as different organization. Depending upon the security of the data, it is provisioned in either of public, private or hybrid cloud. In order to ensure the integrity of the data hosted by the cloud, auditing scheme is imposed. In this paper, several auditing schemes have been analyzed and ways for ensuring integrity of data is imposed. To introduce a good TPA, new TPA scheme should not bring any data integrity problem and should not cost additional computation to the user.

Keywords: Cloud Computing, Auditing, TPA, Signature, Key Generation.

I. Introduction

Cloud Audit is a specification technique for the presentation of information about how a cloud computing service provider addresses its data in the cloud. The cloud audit important goal is to ensure the data readily available to its customer and the data provided should be safe to use. The cloud auditing enables a trusted interface between cloud customers and the cloud service provider. A cloud service provider will normally provide three types of audit and assurance to the cloud customer. First one is

well structured documentation about principles, measures, and policies. The second one provides the information about standard configuration of cloud customer computer system. The third one provides information about logging and maintenance procedures. The source from which information is provided for cloud auditing process is shown in fig1. Cloud supplier is one of the sources for information. Cloud supplier provides information about standard procedures and policies. Customer is another source of information, who provides information about own log files, own procedures and configuration of customer computers.

A third party is the one who verifies the information provided by cloud supplier and customer information's, then third party issues the audit reports and certificates. Alike certificates provided to the webpage by internet security providers, the third party certificate provisioned by TPA is taken into account by the user to easily ensure the integrity of the data hosted by the cloud service providers. Hence a trusted third party resource is needed to look over the integrity of the data as every owner cannot incorporate with assessing the integrity.

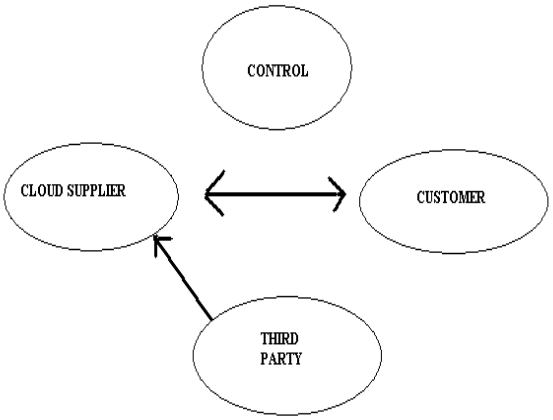

Fig 1: Information sources for cloud auditing

II. Third Party Auditing

Cloud Audit technique involves Audit, Evaluation, Affirmation and Guarantee. The nature or property of the data is unknown to the user, user unaware of originality of the content provided by the cloud service provider. The cloud service providers normally cannot integrate the data or service hosted in it. But sometimes cloud service providers (CSP) falsely ensure integrity of data, even though it is correct or not, in order to sustain in the competitive cloud service providers list. To support the service provided to users by CSP, normally a third party auditing scheme (TPA) provider will dynamically check the integrity of the data frequently.

At first instance of provisioning cloud platform, some key characteristics such as integrity, security, dependability of the data and service provided by the cloud service provider is unknown. There has been lot of dangerous attacks seen in the cloud environment. Some of the major attacks in cloud are listed in the table below.

S.NO	ATTACK	ATTACK DESCRIPTION
1	**Data Breaches**	**The cloud customer personal information is exposed to attacker. Encryption techniques can be used for avoiding data breaches.**
2	**Data loss**	Data may be lost from a disk drive before the backup of data is created by cloud customer. It happens when the cloud customer loses the key for the encrypted data.
3	**Account hijacking**	**Cloud customer control over their data is lost due to vulnerabilities like phishing, buffer overflow attacks, loss of credential data.**
4	**Insecure APIs**	Cloud has lot of contradictions in servicing the millions. All are connected to cloud using a third party API which is insecure.
5	**Denial of service**	**This type of attacks is carried out to interrupt the service to the end users. By frequent requesting the user IP denying other services to get in**
6	**Malicious insiders**	Any person exists within a cloud service providers or an ex-employee engages in wrong intention, effects would be hazardous. Hence cloud service providers should keep their keys on their own, not in the server.
7	**Misuse of cloud services**	**Inappropriate usage of cloud services by a hacker or any end user will results in degradation of performance and so on. Cloud service should be interactive while servicing.**
8	**Authentication attacks**	Authentication is still a loophole in virtual Services that faces the enormous attack over the year. Authenticating users includes different mechanisms but not enough secure to withstand. Organizations data stored on the cloud must be authenticated by on its own, not by cloud servers.
9	**Insufficient due diligence**	**Without understanding the main theme of the cloud, too many companies engage in this business affecting the aspects of cloud service.**

Table 1: List of attacks in Cloud

As the cost factors such as money, space, service became cheap in the cloud rather than implementing on own. The cloud service became boon to small companies compared to MNC sectors. The factors mentioned above became more prominent to be established by the cloud service providers. Due to rapid exploration of cloud service in IT sectors, third party auditing scheme is introduced by the third party organizations to ensure the service provided by the cloud service providers. At first instance of auditing, entire data is accessed by the third party sectors to analyze the integrity of the service provided by the cloud services.

Due to this kind of assessment, the privacy factor of the organization became vile.

The process of third party auditing is shown in fig2.

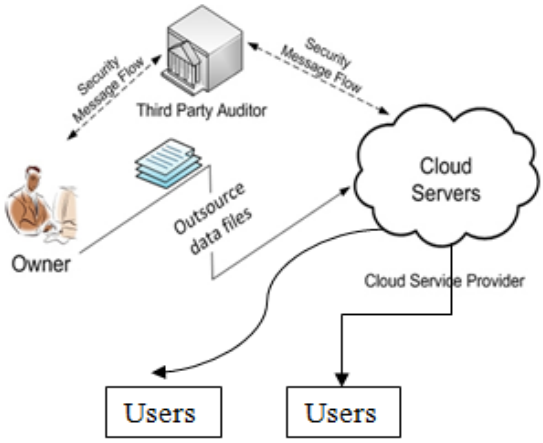

Fig 2: Third Party Auditing in Cloud

Henceforth a new scheme should be chosen to assure the privacy of the service. The information of the data owner used to analyze integrity should be minimized. Only required fields only should be shared with third party organizations.

III. Related Work

The assurance provided by the third party auditing is trusted by the end users of the cloud service. Hence so, the service (IAAS, PAAS, and SAAS) is audited by the TPA regularly. Every third party organizations have its own methodology to assure the cloud service. In order to secure the privacy of the data hosted by the data owner, each TPA moved to a new methodology to preserve the data integrity without retrieving entire data to analyze. Some of the techniques are discussed below.

Each methodology uses different factors to determine the originality of the data and service. Some of the methods are discussed below.

A. Certificateless Public Auditing for Data Integrity in the Cloud:

*B.wang, H.Li, B.Li and F.Li (2013)***[14]** developed a Certificateless public auditing mechanism in the cloud. Data owner gets his partial private key from KGC (key generation centre) and remaining partial key on its own based on CDH and HS CLS mechanism. Every data in the cloud is separated into blocks and signed with owner private key and hosted in the cloud. Every user including proprietor can raise Challenge Response scheme to ensure the integrity of the cloud. The data integrity is verified without retrieving entire data .Using public key of the owner, the data integrity is checked. This makes this mechanism secure and independent of traditional PKI (Public key infrastructure).

B. PANDA: Public Auditing for Shared Data with Efficient User Revocation in the Cloud:

*B.Wang, B.Li and H.Li(2014)***[10]** proposed a model for efficient user revocation and public auditing mechanism. Every block of data in the cloud is

signed with a signature from the data owner as well as Data User. The entire signing mechanism and auditing mechanism is based on HAPS (Homomorphic Authenticable proxy resignature algorithm). This algorithm provides Blockless verifiability and Non-Malleability. The batch auditing and independent auditing mechanism is supported using Bilinear Maps algorithm by analyzing the signature of the block signed using the public key of the signed user. This ensures data integrity as well as privacy of the data by neglecting provision of entire data.

C. Privacy Preserving Public Auditing for Data Storage Security in Cloud Computing:

*C.Wang, Q.Wang, KuiRen(2010)***[11]** proposed a method for public auditing mechanism for ensuring cloud storage. Framework for Public auditing scheme comprises of four algorithms. Key generation scheme technique is implied on the cloud data and SignGen generation scheme is applied to create metadata which is used for verification process. Third party raises audit challenge to the cloud server. GenProof will generate a proof which is then verified by the third party using VerifyProof process. This algorithm can also be applied for batch auditing using bilinear aggregate signature scheme which supports the integration of multiple signatures by different signers on distinct data into a single signature and provides authenticity in secure way.

D. **Secure and Constant Cost Public Cloud Storage Auditing with DeDuplication**:

J.Yuan and shucengyu **[9]** provisioned a model for public auditing mechanism as well as deduplication of storage. This scheme involves Trust Authority who creates key for signing the data block which is based on CDH, SDH, T-SDH problems. The data owner signs the block and host in on the cloud. The auditing process is a challenge response method. TPA which needs in ensuring data integrity will then raise a challenge. The authentication tag is used by the TPA to ensure the data originality using public key of the user. Once the file is stored, If anyone tries to insert a copy of it, only new link is created which refers the same storage space. It avoid the duplication of file and saves storage space.

E. **Dynamic Audit Services for Integrity Verification of Outsourced Storages in Clouds**:

Y.Zhu, H.Wang, Z.Hu, Gail-Joon, H.Hu, S.Yau**[15]** proposed a method to audit the data in the cloud dynamically. The audit system infrastructure contains three models namely Tag Generation, Periodic Sampling Audit and Audit for Dynamic Operations. Every data is tagged with key and stored in the cloud. Every tagging provides a IHT (Index Hash Table) and PVP (Public Verification parameters) which is given as input for verification process by the TPA. Interactive proof protocol is used for periodic sampling of data. The key used to tagging can also be dynamically varied by authorized party which reflects respective IHT and PVP.

F. Enabling Public Audit ability and Data Dynamics for Storage Security in Cloud Computing:

Qian Wang, Cong Wang, Kui Ren , W Lou and Jin Li**[5]** proposed a method to verify the integrity of the data in the cloud. Homomorphic authenticator is used over the data stored in the cloud to create metadata, using this third party auditor can verify the Meta data information. Before verifying data, TPA checks the data signature to verify its owner. Proposed system is based on PKC-based Homomorphic authenticator. It uses key generation and signature generation and Merkle hash tree (MHT) concepts to maintain integrity of the data. This method is also based on challenge response method to verify the integrity of the data.

IV. Proposed Work

Third party auditing requires some of the user credentials to be supplied for analyzing the integrity of the data hosted in the cloud and also need to have access to the data store. But some of the information of the cloud user cannot be provided even to a trustworthy party. Because it will affects the privacy of the user. Considering cloud as a trusted place to host the data, organization can store their data without having local copy of the data in the organization. But cloud servers usually use same algorithm to protect the data from different entities (Ex. Government, schools, and private data). Hence there should be additional security to be taken care by the organization to maintain the integrity of the data.

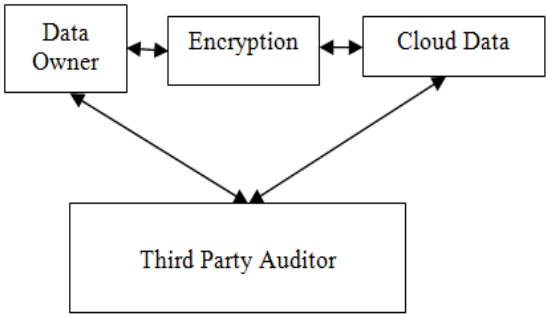

Fig 3: Third Party Auditing

The data hosted should be encrypted or hashed from the client side; the data can be used only if the user possesses a key. Using key management technique, keys can be effectively shared among users. As usual the data is dividing into blocks. Each block should be signed by its users.

TPA can audit the blocks by requesting the cloud for keys which in turn request the associated owner of the information. Data owner provides access to the TPA by providing a temporary user ID. So that TPA can audit the data hosted. Only data owner reside the information of the keys.

V. Conclusion And Future Enhancement

To host the data in the cloud, integrity should be maintained by the cloud service providers. To provide this feature, data must be safeguard against all type of attacks. Hence a secured technique should be deployed by the service providers to remain in the competitive technical market. Metadata should be shared in an efficient way and user information should be protected. Encrypting the data does add some computation overhead over the system. But it provides integrity to the data.

Only some of the user identity details should be shared among the third party systems. Separate assessment should be enforced to do this to preserve user privacy. In future, a separate methodology should be adapted to securely exchange user information via cloud.

VI. References

[1] Cloud storage services “http://www.tomsguide.com/us/ cloud-storage-service-computing, review-1539-9.html”

[2] Oruta: Privacy-preserving public auditing for shared data in the cloud by Boyang Wang ; State Key Lab. of Integrated Service Networks, Xidian Univ., Xi'an, China ; Baochun Li ; Hui Li. In Cloud Computing, IEEE Transactions on Jan.-March 2014”

[3] B. Wang, B. Li, and H. Li, “Public Auditing for Shared Data with Efficient User Revocation in the Cloud,” in the Proceedings of IEEE INFOCOM 2013, 2013, pp. 2904–2912.

[4] C.Wang, Q. Wang, K. Ren, and W. Lou, “Ensuring Data Storage Security in Cloud Computing,” in the Proceedings of ACM/IEEE IWQoS 2009, 2009, pp.

[5] Q. Wang, C. Wang, J. Li, K. Ren,W. Lou, “Enabling Public Verifiability and Data Dynamic for Storage Security in Cloud Computing,” in the Proceedings of ESORICS 2009. Springer-Verlag, 2009, pp. 355–370

[6] A New Approach to Pseudorandom Number Generation Ankur, Divyanjali; Advanced Computing & Communication Technologies (ACCT), 2014 Fourth International Conference on DOI: 10.1109/ACCT.2014.26 Publication Year: 2014 , Page(s): 290 - 295

[7] Rackspace Devstack cloud construction methods “http://github.com/ openstack-dev/devstack” for OpenStack installation.

[8] Understanding OpenStack installation procedures “http://mirantis. com/Cloud/Understanding%20OpenStack%20Authentication%20%20Keyston e%20PKI%20%20Pure%20Play%20OpenStack.htm” for easy working with open stack.

[9] Secure and Constant Cost Public Cloud Storage Auditing with DeDuplication, Jiawei Yuan, Shucheng Yu ”http://ieeexplore.ieee.org/ xpls/abs_all.jsp? arnumber=6682702 &tag=1” [10] PANDA: Public Auditing for Shared Data with Efficient User Revocation in the Cloud: B.Wang, B.Li and H.Li(2014) “http:ieeexplore.ieee.org”.

[10] Privacy Preserving Public Auditing for Data Storage Security in Cloud Computing: C.Wang, Q.Wang, KuiRen (2010) "http:ieeexplore. ieee.org".

[11] Public Data Integrity Verification for Secure Cloud Storage, Hongwei Liu, Peng Zhang, Jun Li "http://ojs.academy publisher.com/index.php/ jnw/article/view/jnw0802373380".

[12] Secure Audit Service by Using TPA for Data Integrity in Cloud System, Shingare Vidya Marshal "http:// www.ijitee.org/attachments/ File/v3i4/D1180093413.pdf"

[13] Certificateless Public Auditing for Data Integrity in the Cloud, Boyang Wang, Baochun Li, Hui Li and Fenghua Li "http://iqua.ece.toronto.edu/~bli/papers/ boy ang -cns13.pdf"

[14] Dynamic Audit Services for Integrity Verification of Outsourced Storages in Clouds, Y.Zhu, H.Wang, Z.Hu, Gail-Joon, H.Hu and S.Yau "http://people.cs.clemson .edu/ ~hongxih/ papers/ acmsac2011.pdf"