IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 16, Issue 1, Ver. VII (Feb. 2014), PP 52-54
www.iosrjournals.org

Auditing Services in Cloud Computing For Achieving Data Access Control

N. Mahesh kumar
PG scholar Department of CSE Paavai engineering college Namakkal

Abstract: *Cloud computing has a great tendancy of providing robust computational power to the society at reduced cost. The wide adoption of this promising computation model is prevented by security which is the primary obstacle especially for customers when their confidential data are consumed and produced during the computation. The data stored in the cloud may be frequently updated by the users. It has been reported by many authors on auditing methods to efficiently audit the cloud data storage without challenging the local copy of data, and introduce no additional on-line load to the cloud user. This paper is a survey of different algorithms used in different auditing mechanisms that have been considered to support the storage correctness of data in cloud environment.*
General Terms: *TPA, HLA, PDP, FAME*

I. Introduction

Cloud computing is the practice of using a network of remote servers hosted on the internet to store, handle, and process data. The increasing network bandwidth and so far reliable flexible network connections make it even possible that users can subscribe high quality services from data and software that reside solely on remote data centers. Cloud Computing describes a new enhancement, consumption and delivery model for IT services based on internet, and it involves the provision of dynamically scalable and often virtualized resources as a service over the Internet.

The security for the outsourced data is provided by the Service Level Agreement (SLA). But, the data integrity and availability of the outsourced data is not guaranteed in the large scale data storage in cloud environment. Because the resources and the delivery models belonging to the cloud environment is maintained by the externally hosted Cloud Service Providers (CSP). This paper presents various algorithm used in different auditing mechanisms which is used to find the correctness of the data and maintains the integrity level of the data.

II. Third Party Auditing

A growing number of online service provider's offer to store customer's data. Customers cannot make informed decisions about the risk of losing data stored with any particular service contributor, reducing their motivation to rely on these services. The Third Party Auditing (TPA) process is important in creating an online service oriented system, which allows the customers to evaluate risks, and it increases the effectiveness of assurance based risk mitigation [7]. It has described the approaches and system hooks that support both internal and external auditing of online storage services which describes the motivations for service providers and auditors to adopt these approaches. It list challenges that need to be resolved for such auditing to become a reality.

The storage service accountability is provided through independent, third party auditing and arbitration [6]. The customer and service enter into an agreement or contract for storing the data and the service will provide some type of payment for data loss to return the data intact.

The service provider, whose target is to make a profit and maintain a reputation, has a reason to hide data loss. On the other hand, customers are very defective. Customers can openly or illegally claim loss to get paid. To avoid this independent, third party auditor will arbitrate and confirm whether stored and retrieved data is intact.

Homomorphic Linear Authentication technique in TPA:

The public key based homomorphic authenticator and uniquely integrated random masking technique achieve a privacy-preserving public auditing system for cloud data storage security have been utilized [1]. To support efficient handling of multiple auditing tasks, it has further explored the technique of bilinear aggregation signature to extend the main result into multi-user surroundings, where TPA can perform numerous auditing tasks simultaneously. General security and performance analysis shows it as a secure and efficient scheme.

The TPA involves the combination of KeyGen, SignGen, GenProof and VerifyProof algorithms [10]. These algorithms are classified into SetUp and Audit Phase for an efficient auditing process. The following figure describes the efficient working process of these two phases.

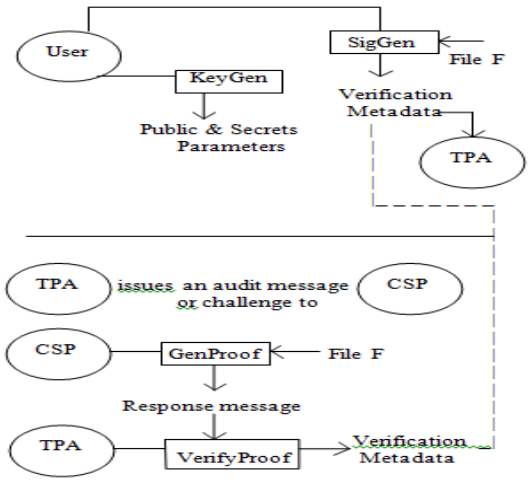

Figure.1 Setup and Audit Phase

III. Encryption Schemes

The sensitive user data is kept confidential against un-trusted servers in order to provide a secured access of services in public cloud [2]. The problem of simultaneously achieving fine-graininess, scalability, and data confidentiality of access control actually still remains unresolved.

By defining and enforcing access policies it addresses this challenging issue based on data attributes, and allow the data owner to delegate most of the computation tasks involved in fine grained data access control to untrusted cloud servers without disclosing the underlying data contents.

It is achieved by means of exploiting and uniquely combining techniques of attribute-based encryption (ABE), proxy re-encryption, and lazy re-encryption. It also has salient properties of user access privilege confidentiality and user secret key accountability. Extensive analysis shows that the scheme is highly efficient and provably secure under all the security models.

IV. Provable Data Possession Technique

In Provable Data Possession (PDP) model, the data are preprocessed by the clients and send to the server for storage. The server has to provide the acknowledgement for the client stored data.
The Dynamic PDP extends the PDP model to support updates provable to the stored data.

Message Authentication Code:

The availability of remote storage providers in the security community in cloud environment allows a client to verify integrity and availability of the data outsourced to an untrusted remote storage server at a relatively low cost [3]. Most recent solutions to this problem is allowing the client to read and update (insert, modify, or delete) store data blocks while trying to lower the overhead associated with verifying data integrity.

It has a support for operations on ranges of blocks, and revision control. It guarantees to achieve stem from a original data structure, term balanced update tree, and removing the need to verify update operations. It rely on a Message Authentication Code (MAC) scheme, defined by three algorithms such as key generation algorithm Gen, tag generation algorithm Mac, and verification algorithm Verify.

Cooperative PDP:

Provable data possession (PDP) is a technique for ensuring the integrity of data in storage outsourcing. In [4], the construction of an efficient PDP scheme for distributed cloud storage to support the scalability of service and data migration is addressed. A cooperative PDP (CPDP) scheme based on homomorphic verifiable response and hash index hierarchy is presented.

The security based on multi-proven zero-knowledge proof system, which satisfy completeness, knowledge soundness, and zero-knowledge properties has been proved. In addition, performance optimization mechanisms in particular present an efficient method for selecting optimal parameter values to minimize the computation costs of clients and storage service providers. It has introduced a lower computation and communication overheads in comparison with non-cooperative approaches.

The following table describes the Block operations in the PDP schemes.

Scheme	Block operations			
	Append	**Modify**	**Insert**	**Delete**
PDP	Yes	No	No	No
Dynamic PDP	Yes	Yes	Yes	Yes
Scalable PDP	Yes	Yes	No	Yes

Table.1 Block operations in PDP scheme

V. Other Schemes

a) Firewall Anomaly Management Environment:

An innovative policy anomaly management framework for firewalls is represented, adopting a rule-based segmentation technique to identify policy anomalies and to derive effective anomaly resolutions [5]. A grid-based representation technique, providing a spontaneous cognitive sense about policy anomaly is articulated. A proof-of-concept implementation of a visualization-based firewall policy analysis tool called Firewall Anomaly Management Environment (FAME) is discovered to resolve anomalies in firewall policies.

b) Boneh-Lynn Shacham(BLS):

BLS algorithm can support fully dynamic data updates over fixed-size data blocks, it only support updates with fixed-sized blocks as basic unit, which was called coarse-grained updates [6]. As a result, every small update will cause re-computation and updating of the authenticator for an entire file block, which in turn causes higher storage and communication overheads.

A formal analysis for possible types of fine-grained data updates is provided and can fully support authorized auditing and fine-grained update requests. Theoretical analysis and experimental results describes an offer not only enhanced security and flexibility, but also significantly lower overhead for big data applications with a large number of frequent small updates, such as applications in social media and business transactions.

VI. Conclusion

Cloud Computing is a major technology that provides services over the internet in an efficient way. There are various challenges which need to be addressed for making cloud computing work well in reality. The challenges like security issues and storage issues are important for the service providers to improve the services. This paper presents the different algorithms in auditing services to achieve data access control in cloud and to provide privacy for outsourced data in the cloud environment. It also provides the brief description of the auditing process in cloud for future development.

References

[1] C. Wang, Q. Wang, K. Ren, and W. Lou, in "Privacy Preserving Public Auditing for Storage Security in Cloud Computing" in Proc. IEEE INFOCOM '10, Mar. 2010.

[2] "Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing" Shucheng Yu, Cong Wang, Kui Ren, and Wenjing Lou Dept. of ECE, Worcester Polytechnic Institute.

[3] "Dynamic Provable Data Possession" C. Chris Erway Alptekin K upc¸, Charalampos Papamanthou Roberto Tamassia from Brown University, Providence in November 29, 2009

[4] "Cooperative Provable Data Possession for Integrity Verification in Multicloud Storage" Yan Zhu, Member, IEEE, Hongxin Hu, Member, IEEE, Gail-Joon Ahn, Senior Member, IEEE, and Mengyang Yu in "IEEE Transactions on parallel and distributed systems, vol. 23, no. 12, December 2012"

[5] "Detecting and Resolving Firewall Policy Anomalies" Hongxin Hu, Student Member, IEEE, Gail-Joon Ahn, Senior Member, IEEE, and Ketan Kulkarni.

[6] Privacy-Preserving Audit and Extraction of Digital Contents" Mehul A. Shah Ram Swaminathan Mary Baker HP Labs, Nov 2007.

[7] "Auditing to Keep Online Storage Services Honest" Mehul A. Shah, Mary Baker, Jeffrey C. Mogul, Ram Swaminathan Jun 2007

[8] "The Security of an Efficient Dynamic Auditing Protocol in Cloud Storage" Jianbing Ni, Yong Yu, Yi Mu, Senior Member, IEEE, Qi Xia , in "IEEE Transactions on parallel and distributed systems".

[9] "Secure Overlay Cloud Storage with Access Control and Assured Deletion" Yang Tang, Patrick P.C. Lee, Member, IEEE, John C.S. Lui, Fellow, IEEE, and Radia Perlman, Fellow, IEEE presented in "IEEE Transactions on dependable and secure computing, vol. 9, no. 6, November/December 2012"

[10] K.B.Jachak, S.K.Korde, P.P.Ghorpade and G.J.Gagare in "Homomorphic Authentication with random masking Technique" Bioinfo publications.