International Journal of Engineering Research and General Science Volume 4, Issue 3, May-June, 2016
ISSN 2091-2730

Cloud With Third Party Auditor

[1]Mr. Surwase Vaishnav Popatrao , [2]Prof. M.B Ansari

[1]ME Student , Department of Computer Science & Engineering , BAMU University, SYCET, Aurangabad.

[2] Head Of Department , Department of Computer Science & Engineering , BAMU University, SYCET, Aurangabad

Abstract– Today individual and organization data is created in a rapid rate. The demand is very high to maintain the growing of data. Datasets are generated by various organization, government or business industry to centralize the information and it is managed by an external storage provider called Cloud Storage Service. The CSS provide the facility of distributed data center and data on demand service for data virtualization.
Here TPA (Third party Auditor) controlled communication between cloud storage service and the cloud user. TPA is an external agent, it also manipulate the user data stored on cloud. So this paper focuses of checking the authenticity to TPA

Index Terms– For this process we use Cloud computing, big data, authorized auditing and fine-grained data updates.

I. INTRODUCTION

Today world is moving on digitization and cloud computing is best concept to handled big datasets. Here we are focused on nature, origin and security related issues of big datasets. From various domains data are originated are follows education, industry etc.

The Public audit ability is used to ensure data integrity. Public audit ability allows an external party, in addition to the user to verify the correctness of remotely stored data. As third party auditor is used for verifying integrity of data.

The data generated features of different sources are different and definitions are also different like velocity, value, volume etc. new infrastructure and tools are used to support the big data.

For managing the features of big data cloud use better infrastructure, storage, network, high computing performance. New data infrastructure trusted on centric security modules and proposed purpose for processing and storage of data.

A cloud dynamically provision and through dialogue between service provider and consumer of the service level agreement or more integrated computing resources that are presented as consisting of a collection of interconnected and virtualized computers parallelism type of distributed system.

Our research cloud users and cloud service provider is certified to authenticate the TPA. Another purpose is to allow the CSS-grained dynamic data updates and its benefits, efficiency calculations will be analyzed in our paper.

II. LITERATURE SURVEY

On basis of its features cloud computing is hype on its demand to store the big data. Features are scalability, elasticity and efficiency are supporting dynamic data. As according to current need with service interruption and management effort cloud users are able to conveniently scale up/down on their virtual allocation of resources. Data security and privacy is the most existing problem on cloud computing.

Main area of today's research is integrity verification for outsourced data storage. Jules et al. [1] is applied to static data storage is based on a model proposed POR. Atomiesetal. Theyhomogenous verifiable tags (HVT) callto confirm previously calculated through a combination of file tag ratio of out sourced confirm the integrity of the file based on the PDP proposed a similar model. . Basis of BLS signature scheme proposed another model. BLS signature is shorter then RAS signature as compare both of them. Elway, et al. proposed the first PDP scheme based on skip list that support full dynamic data updates.

Privacy& security issues of cloud storage:

Secure cloud and privacy is of most important thing for cloud, Privacy issues include protection of identity information, transaction histories and sensitive data, authentication, Idea of cloud computing is store user data on shared Infrastructure. So, there is risk of unauthorized access.

III. IMPLEMENTATION DETAILS

Different techniques were used to provide security to cloud data but there are some disadvantages of these system. Generally Common methods is used to protecting user data include encryption prior to storage, user authentication procedures prior to storage or retrieval, and building secure channels for data transmission.
These protection methods normally require cryptography algorithms and digital signature techniques.

Public audit ability in is used for Ensuring possession of files on untrusted storages. In this model RSA based holomorphic tags are used for the security. To achieve the public audit ability.

Cloud data storage consists of 3 entities –

1] User – who has large amount of data which is to be Stored on cloud.
2] Cloud Server – which has computing resources to
Manage cloud data.
3] Third party auditor – to challenge cloud server to
Check correctness of data on behalf of user.

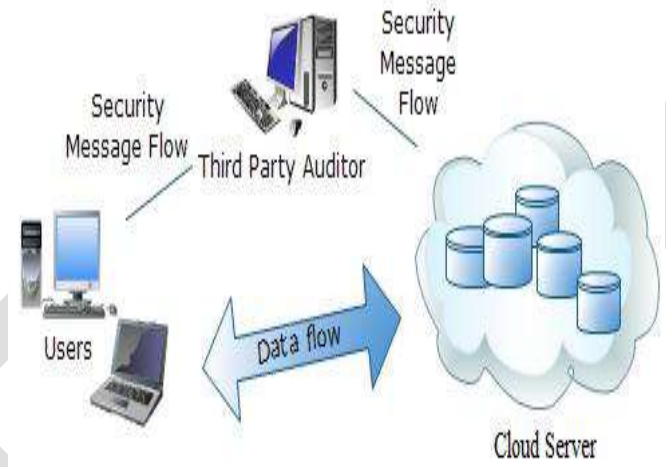

Fig -Architecture of cloud

Public Auditing of Dynamic Big Data Scheme:

When third party auditor is used for verification purpose privacy should be preserved. In public auditing scheme, third party auditor does not have any knowledge about data. Public auditing scheme has following advantages –
1] Public Auditability – Public auditability allows TPA to check integrity of data without retrieving it.
2] Storage Correctness – User's data should be stored
Correctly on cloud.
3] Privacy Preserving – This ensures that TPA cannot
Derive any data content.
4] Lightweight – To allow TPA to perform auditing
With minimum overhead.
5] Batch auditing – To allow TPA to challenge server
for checking integrity of data for multiple clients at the
Same time.

Fine-grained Update Verification: - This process occurs between client and CSS. The client send fine-grained update request to CSS via Perform Update and client runs verify Update algorithm to check whether CSS has performed the update correctly on the data block as well as in corresponding authenticator.

Fine-Grained Data Updates

The second major concern of our research work is to be able to do fine-grained updates in contrast to coarse-grained updates. Fine-grained update in dynamic data is the provision of doing small changes in the corresponding data block instead of accessing and changing the whole block. This method can reduce the communication overhead as occurring in previous methods.

IV.RESULTS

A. Software and hardware requirements

Hardware Configuration
- Processor - Pentium 2.6 ghz
- RAM - 512 mb ram
- Monitor - 15" color
- Hard Disk - 20 GB
- Key Board - Standard Windows Keyboard

Software Configuration

- Operating System - Windows XP/7
- Programming Language - Java
- Database - MySQL
- Tool - NetBeans

V. CONCLUSION AND FUTURE WORK

Today the example of big computing paradigm in cloud computing to store the big datasets. Important aspect for cloud user is cloud data security. For security and integrity of data cloud user ensure only the trusted third party. How to ensure trusting a third party we present an overview in this paper. TPA cannot derive user's data during the process of public data auditing because it focused on privacy-preserving for datasets.The proposed system is that it will prevent malicious TPA cannot be forged, which uses a better signature scheme. For increases the efficiency of update process it provides a feature of fine-grained dynamic data update.we uses third party auditor which achieves public auditability, stateless verification and also data dynamics. Third party auditor verifies integrity of user data as well as privacy is preserved.

In future we have to more improve the security issues of data storage on cloud storage service. On cloud computing this topic is not negotiable to improve. For implementing that process we increases the layers of authentications to TPA.

Proposed System:
Disadvantage of HLA is linear combination of block can reveal user data information. To achieve privacy Preserving public auditing HLA with random masking is used. TPA cannot retrieve information if random Masking is used. Public key based HLA is used to achieve public auditability.
Data content, no matter how many linear combinations of the same set of file blocks can be collected .Due to TPA the relationship between the cloud user and cloud service provider is transparent.

We also provide the server-side protection methods for efficient data security with effective data confidentiality and availability .Along with other metrics such as storage and computation, a highly efficient security-aware scheduling scheme will play an essential role under most cloud computing.

REFERENCES:

1. A. Juels and B.S. Kaliski Jr., ''PORs: Proofs of Retrievability for Large Files,'' in Proc. 14th ACM Conf. on Comput. and Commun. Security (CCS), 2007, pp. 584-597.
2. H. Shacham and B. Waters, ''Compact Proofs of Retrievability,'' in Proc. 14th Int'l Conf. on Theory and Appl. of Cryptol. and Inf. Security (ASIACRYPT), 2008, pp. 90-107.
3. Q. Wang, C.Wang, K. Ren,W. Lou, and J. Li, ''Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing,'' IEEE Trans. Parallel Distrib. Syst., vol. 22, no. 5,pp. 847-859, May 2011.
4. G.Ateniese, R.B. Johns,R. Curtmola, J.Herring, L. Kissner,Z. Peterson, and D. Song, ''Provable Data Possession at Untrusted Stores,'' in Proc. 14th ACM Conf. on Comput. and Commun. Security (CCS), 2007, pp. 598-609.

5. C. Wang, Q. Wang, K. Ren, and W. Lou, ‘‘Privacy Preserving Public Auditing for Data Storage Security in Cloud Computing,’’ in Proc. 30st IEEE Conf. on Comput. and Commun. (INFOCOM), 2010, pp. 1-9.

6. Cong Wang, Sherman S.-M. Chow, Qian Wang, Kui Ren, and Wenjing Lou, “Privacy-Preserving Public Auditing for Secure Cloud Storage,” IEEE Transactions On Cloud Computing, Year 2013.

7. C. Wang, K. Ren, W. Lou, and J. Li,“Toward publicly auditable secure cloud data storage services,” IEEE Network , vol. 24, no. 4, pp. 19–24, 2010