www.ijecs.in
International Journal Of Engineering And Computer Science ISSN: 2319-7242
Volume 4 Issue 11 Nov 2015, Page No. 14987-14992

Third Party Auditing of Data on Cloud With Fine Grained Updates

Ajinkya Sabale[1], Rohit Prajapati[2], Sameer Pathan[3], Sanket Prabhu[4] Prof .Sanjay Agrawal[5]

ajinkya.sabale@mmit.edu.in rohit.prajapati@mmit.edu.in sameer.pathan@mmit.edu.in
sanket.prabhu@mmit.edu.in sanjay.agrawal@mmit.edu.in
Marathwada Mitra Mandal's Institute of Technology
Approved by AICTE New Delhi, Recognized by DTE Maharashtra and Affiliated to University Of Pune

Abstract: ***Cloud computing opens a new stream in IT as it can provide various elastic and scalable IT services in a pay-as-you-go way, where its users can reduce the cost in their own IT infrastructure. In this way, users of cloud storage services do not physically maintain direct control over their data, which makes data security one of the major advantage of using cloud. Previous research work already allows data integrity to be verified without presence of the actual data file. When this verification is done by a trusted third party, the verification process is called as data auditing, and this third party is called an auditor. However, such schemes in existence suffer from several drawbacks .First ,the necessary authorization or authentication process is missing between the auditor and cloud service provider, means anyone can ask for challenge the cloud service provider about proof of integrity of certain file, in which the quality of the so-called `auditing-as-a-service' in risk; Second, although some of the previous work based on BLS signature which can support fully dynamic data updates over fixed-size data blocks, they only support updates with fix-sized blocks as basic unit, which called as coarse-grained updates. As a result, every small update will cause re-computation and updating of the authenticator for whole file block, which in turn causes higher storage and communication overheads. In this paper, we provide an analysis for all possible types of fine-grained data updates and propose a scheme that can provide full support to authorized auditing and fine-grained update requests. Based on our scheme, we also propose the technique that can reduce communication overheads for verifying small updates. Theoretical analysis and experimental results show that our scheme can 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 transaction.***

Keywords: Cloud computing, big data, authorized public auditing, fine-grained updates, TPA

1. Introduction

CLOUD computing is being intensively known as one of the most powerful innovation in information technology in recent age. By using reserve virtualization cloud delivers us computing capital and services in a pay-as-you-go mode, where cloud envision to turn into as suitable to use alike to way of life utilities such as electrical energy usage, irrigate, telephone u and water in the near prospect. Today world is moving on digitization and cloud computing is best technology to handle the big data sets. Various cloud computing services are categorize into Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS) and last one is Software-as-a-Service (SaaS).

Many global IT corporations now offer powerful public cloud services to users on a level from individual to venture all over the world various examples of this are Amazon AWS and IBM Smart Cloud [1]. As we know the current growth and propagation of cloud compute is fast rising, debate and hesitation on the practice of cloud still there. Data security and data solitude are some of the main concern in the acceptance of cloud compute. Users lose their direct control on data when they amass data on cloud as compare to conventional systems.

In our future work we will address the problem of honesty confirmation for big data storage on cloud. We call this problem as data audit when the confirmation is conducted by a trusted third party i.e. TPA called as an assessor. From cloud users perspective it is named as auditing-as-a-service. In a remote confirmation scheme, the cloud storage server (CSS) cannot provide a valid honesty proof of a given amount of data to a verifier unless all this data is intact. To ensure integrity of user data store on cloud service provider, this support is of no less consequence than any data guard instrument deployed by the cloud service supplier (CSP) [1], no matter how secure they seem to be, in that it will provide the verifier which is a piece of direct, trustworthy and real-timed cleverness of the honesty of the cloud user's data through a challenge request [2]. It is particularly not obligatory that data auditing should be conducted on.the three main contributions of our proposed work are described as follows:

1. Authorized third party auditing
2. Fine grained dynamic data updates
3. Auditability aware data scheduling

DOI: 10.18535/Ijecs/v4i11.21

2. Literature Survey

In past there have been lot of work has been done on cloud data security different techniques were used to provide security to cloud data but there are some disadvantages of such systems. Existing methods for protecting user data include data encryption prior to storage and user authentication procedures prior to storage or retrieval of data after that building secure channels for data transmission over the cloud. In this existing systems the algorithms used are cryptographic and Digital signature based [6].

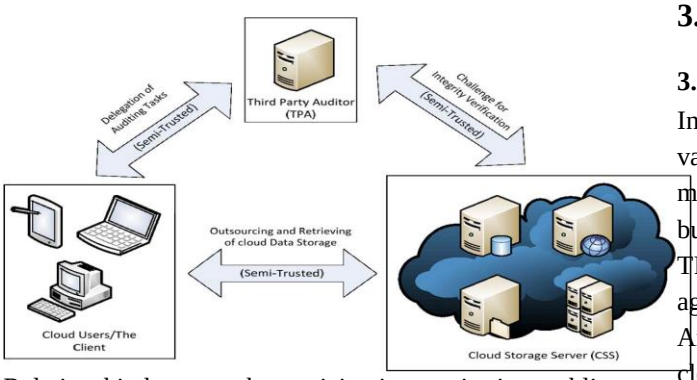


Fig. Relationship between the participating parties in a public auditing scheme.

First work is by Attendees et al who consider public audit ability in provable data control replica for ensuring possession of records on un trusted storages[4]. Attendees present a model in which RSA based homomorphism tag are used. With the help of this technique public audit ability concept is achieved. But the problem with this model is so as to it does not support dynamic data operation and too suffer security problems[8].
Another research by Wang careful dynamic data storage in a distributed scenario which is a better idea. he proposed challenge reply protocol can both determine the data rightness and locate possible errors but this model only measured partial support for dynamic data operation[9].
Kaliski obtainable a proof of retrievability representation. The main disadvantage of this model as it do not support public audit ability [5]. Extended research on this done by Shacham and Waters design an improved PoR system with full proofs of security in the security model [5]. In this model they use publicly verifiable homomorphism authenticators built from BLS signatures base on which the proofs can be aggregated into a small authenticator value by using this public irretrievability is achieved. The main concern comes in front with this is the author only consider static data files which are not preferable since our main concern is about big data files [3].
One research was there on MAC based scheme which has the inconvenience like the number of times a particular data file can be audit is limited by the number of secret keys that must be set a priori. So the difficulty arise here is once all likely secret keys are tired after that the user then have to get back data in full to recomputed and republish new MACs to TPA[10] .Here in this system TPA also has to keep and keep well-versed state flanked by audits that is to maintain track on the exposed MAC keys. It can only support static data and cannot professionally deal with dynamic data at all so this is a big issue to be solved when making an allowance for large data.
HLA based scheme- There is need of system which can prove integrity of data without retrieving data blocks there. So there is another method obtainable that is HLA scheme was used for this reason. The only difference between HLA and MAC is that HLA can be aggregate. The main issue with this system is that data can be retrieve only if linear combinations of same chunk are used [10].

3. Implementation Details

3.1 Problem Definition

In preceding research it is shown that cloud environment give various advantages by providing infrastructure as a service and maintenance as a service [1]. It relieves the load of user's task but security became a major concern in all time. User hires a TPA to check the integrity of data store in cloud server. But again the problem arises whether the TPA is authorized or not. Another concern is connected to the utilization of resources in cloud surroundings. There are number of resources as well as needs. There is no better way to serve the requests inside a particular time and with available reserve.
Previously scheduling algorithms were performed in grid but reduces the performance by requiring advance reservation of resources. In cloud environment due to scalability of capital, manually allocate resources to task is not likely.

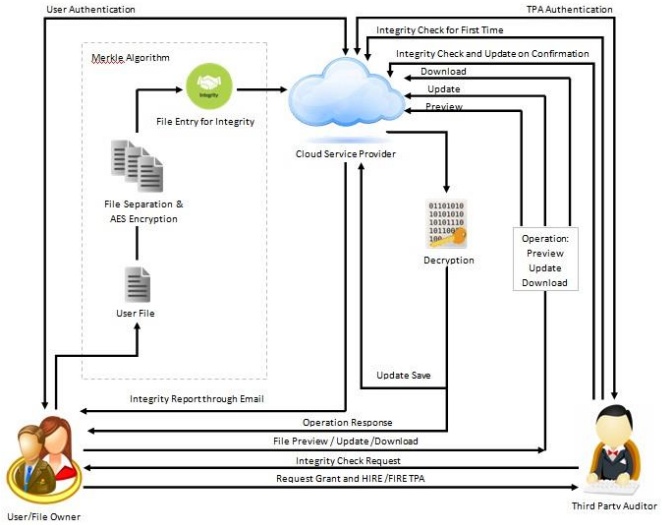
3.2 Proposed System

Variety of main steps of our proposed scheme is described as follows:

1. The client will engender keying materials via KeyGen and FileProc after that he upload the data to CSS. Different from preceding schemes here in our scheme the client will store a RMHT as metadata.
2. After that the client will authorize the TPA by sharing a value sigAUTH.
3. Verifiable Data Updating: the CSS performs the client'sfine-grained update requests via PerformUpdate on user's information.
4. Client runs Verify Update to check whether CSS has performed the update on both the data blocks and their analogous authenticators (used for auditing) honestly.
5. Confront, Proof Generation and Verification: describe how the integrity of the data stored on CSS is verified by TPA via GenChallenge, GenProof and Verify.
6. Auditability aware data scheduling: In this scheme we are clustering various tasks submitted in an request both from the user and auditor on the basis of their main concern.

DOI: 10.18535/Ijecs/v4i11.21

3.3 System Architecture



.

Fig. 2. System architecture Diagram

Work Flow of System is as follows,

The new user first registers with application. After his/ her registration the user can access the account if and only if the user is authenticated by the Cloud Service Provider. The System has three dedicated logins for Data Owner, Third party Auditors and Cloud Service Provider. Cloud Service Provider Manages the users of applications. Users are like DO and TPA. This both users are authenticated by the CSP. If User is not authenticated by the CSP then user is not able to visit the account dashboard. After Successful login of the DO, DO can perform Several operations like, File upload, file Preview , File part Update, File Delete, Accept request proposal of the TPA, Grant access to file to the TPA, Hire TPA , Fire TPA. Views Notification form TPA about file updates. Here The User will upload the file, that file will be divided in to three parts, and three parts will get encrypted. Each time to Preview, Updating this respected parts are getting decrypted and previewed. Each time on any operation on file these multiple parts of file will get operated. The TPA can check the integrity of the file system only if that TPA is hired by the User. The TPA can Check the integrity of the file and sent the notification to the user account and email to the email Id provided by user at the time of Registration. The integrity check is performing by without revealing the contents' or file to the TPA. While updating the file the TPA cannot access the file integrity check. If the integrity of the file will be checked at the of file updating by DO that time the TPA will not be able to check the integrity of file, ass he will get any different result. This is done by the Priority Scheduling. The TPA will see the waiting screen for the same. To check the integrity of file we have created the SHA1 algorithm with our code. The SHA1 will give the 62 bit hash key which will be used for the cross verification of file safety. The encryption can be performed by the developing the AES algorithm to encrypt and decrypt the files and file parts of the File.

Various phases of our proposed work are as follows.

a. Key Generation Algorithm:

1. Start
2. Read Data owner id (udoid)
3. If(doid==udoid) (Execute step 4 to 10)
4. Read secret key (ssk)
5. Choose random number α from Zp(α <- Zp)
6. Choose random group generator (g) from Zp
7. Calculate v=gα
8. Display secrete key pair spk=(v, ssk)
   And Public key pair spk=(v,spk)
9. Update α value on alpha xml in sky drive.
10. Stop
11. Else
12. Stop.

b. Signature Generation Algorithm:

1. Start
2. Read data owner id (udoid)
3. If (doid ≠ udoid)
4. Stop
5. Else
6. Read file path (Fp)
7. Read No. of levels (n) for the construction of MHT
8. Calculate the block size of MHT =size of file/n.
9. Divide the file into NOB Bloks
10. For i=0;
11. For (i<=0) && (i>=NOB)
12. Calculate Hc[i] = enceyptsha1[block[i]]
13. Display hc[i]
14. Choose random number u from set of group generators 'G'
15. if (i<=0 &&i>=NOB)
16. Calculate Sig[i] = (hc[i]*)α
17. Display sig [i]
18. Construct MHT and generate Root node(R)
19. Generate signature for root node rootsign = (H(R))α
21. Upload file to web server
22. Update hash values & signature on TPA xml on Sky Drive.

c. Data Integrity Verification by TPA Algorithm:

1. Start
2. Read data owner id(udoid)
3. If (doid ≠ udoid)
4. Stop
5. Read file name from AWS
6. Retrieve No. of blokes from TPA xml
7. Select the blocks number the user want to verify.
8. Get the auxiliary information for block chal from TPA xml
9. Based on Auxiliary information generate new root for MHT
10. If (new root ≠ root) file modified
11. Else File not modified
12. Stop.

d. Resource Scheduling Algorithm:

In Our Project we use the Scheduling Algorithm for scope Enhancement. The allocation of resources to various tasks is known as job/ resource scheduling.

Auditability aware priority Based Scheduling algorithm:

In cloud environment, there are lots of resources like network, hardware, software, operating system and also number of user. User can be the cloud client or TPA. For different purpose

they send diverse requests to cloud server. There should be proper scheduling between the tasks and resource to improve the utilization and efficiency of resources. In this priority based algorithm, every job or task is assigned with a priority [7]. The higher priority job would get executed first and then the task with priority less than the previous one will get execute and so on. Some individuality of priority based scheduling are:

1. Starvation can happen to low priority process
2. The waiting time slowly but surely increases for the equal
   priority processes
3. Higher priority progression have slighter waiting time and response moment

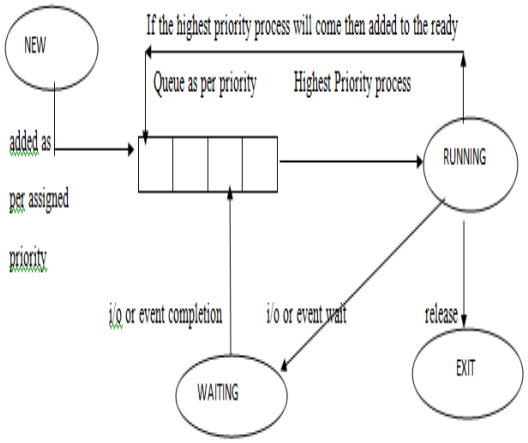


Fig. 3 Priority scheduling

Algorithm for scheduling:

1. for i = 0 to i <main queue-size
2. if priority (task i+1) > priority (task i)
3. then
4. add task i+1 in front of task i in the queue
5. end if
6. end for

4. Results

Numerous of project works developed previously which can merely store data and share data between large numbers of user in a group. In our proposed work we have presented an third party auditing scheme to construct a secure data organization mechanism with high privacy protection method plus also working on audit ability conscious data preparation system which is base on priority.

In this scheme the main qualities are: (1) data security (2) privacy protection (3) audit details to the data owner (4) Auditability aware data preparation

Here we are going to assess the presentation of our future scheme in conditions of the computation overhead introduced by each process.

Computation difficulty: We analyze the computation complexity for the next operations like system setup, new user grant, new file formation , file deletion and user revocation and file access.

a. Software and hardware requirements

Hardware Configuration

- Processor - PentiumIV 2.6 ghz
- RAM - 512 mbdd 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

5. Conclusion and Future Work

Nowadays the instance of large compute example in cloud compute is to amass the big datasets. Significant aspect for blur user is blur data security and solitude. For security and integrity of data cloud user ensure only the trust 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. This paper proposes an algorithm based on priority which will schedule the tasks coming to CSS.
In future we have to improve more on security issues of data storage on cloud storage service. On cloud computing this topic is not negotiable to improve. For implementing that process we increase the layers of authentications to TPA.

6. Acknowledgement

I would like to express my thanks to my guide Prof. Sanjay Agrawal for his highly appreciable support and encouragement also to my HOD Prof. P.M.Daflapurkar. Their guidance is a force behind the completion of this paper. I am grateful for all the suggestions and hints provided by him. My acknowledgment of gratitude to all who supported to make it possible.

References

[1] Chang Liu, Jinjun Chen, Senior Member, IEEE, Laurence T. Yang, Member, IEEE, Xuyun Zhang,Chi Yang, Rajiv Ranjan, and

Ramamohanarao Kotagiri , "Authorized Public Auditing of Dynamic Big Data Storage on Cloud with Efficient Verifiable Fine-Grained Updates." VOL. 25, NO. 9, SEPTEMBER 2014

[2] A. Juels and B.S. Kaliski Jr., ''PORs: Proofs of Retrievability for Large Files,'' in Proc. 14th ACM Conf. on Comput. andCommun. Security (CCS), 2007, pp. 584-597.

[3] 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.

[4] 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.

[5] 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. andCommun. Security (CCS), 2007, pp. 598-609.

[6] 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. andCommun. (INFOCOM), 2010, pp. 1-9.

[7] Cong Wang, Sherman S.-M. Chow, Qian Wang, KuiRen, and Wenjing Lou, "Privacy-Preserving Public Auditing for Secure Cloud Storage," IEEE Transactions On Cloud Computing, Year 2013.

[8] C. Wang,"Toward publicly auditable secure cloud data storage services," IEEE Network , vol. 24, no. 4, pp. 19–24, 2010.

[9] G. Ateniese, R. Burns, R. Curtmola, Peterson, and D. Song, "Provable Data Possession at Untrusted Stores," Proc. 14th ACM Conf. Computer and Comm. Security (CCS '07), pp. 598-609, 2007.

[10] Zissis, D. and D. Lekkas, 2011., Addressing Cloud Computing Security Issues,"" Future Gen. Comput. Syst., 28(3): 583-592.

[11] R. Curtmola, O. Khan, R.C. Burns, and G. Ateniese, ''MR-PDP: Multiple-Replica Provable Data Possession,'' in Proc. 28th IEEE Conf. on Distrib. Comput. Syst. (ICDCS), 2008, pp. 411-420.

[12] 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.

[13] G. Ateniese, S. Kamara, and J. Katz, ''Proofs of Storage From Homomorphic Identification Protocols,'' in Proc. 15th Int'l Conf. on Theory and Appl. of Cryptol. and Inf. Security (ASIACRYPT)

DOI: 10.18535/Ijecs/v4i11.21

Author Profile

Mr.Ajinkya Sabale studying in Final year of Computer enginnering at Marathwada Mitra Mandal's Institute of Technology, Lohgaon Pune.

Mr.Rohit Prajapati studying in Final year of Computer enginnering at Marathwada Mitra Mandal's Institute of Technology, Lohgaon Pune.

Mr.Sameer Pathan studying in Final year of Computer enginnering at Marathwada Mitra Mandal's Institute of Technology, Lohgaon Pune.

Mr.Sanket Prabhu studying in Final year of Computer enginnering at Marathwada Mitra Mandal's Institute of Technology, Lohgaon Pune.

Mr.Sanjay Agrawal Assistant Professor at Department of Computer enginnering at Marathwada Mitra Mandal's Institute of Technology, Lohgaon Pune.