ISSN: 2350-0328

International Journal of Advanced Research in Science, Engineering and Technology

Vol. 3, Issue 2 , February 2016

Survey on Bounded and Reliable Data Transmission in Cloud using Auditor Component

Nivedita .M. Bulagoud, Mary Vidya John

PG student, Department of computer science, Vemana institution of technology, VTU Karnataka
Assistant professor Department of computer science Vemana institution of technology VTU Karnataka

ABSTRACT: Services from an outside supplier remote Cloud Service Provider (CSP) is a growing General line of orientation for numerous organizations mitigate the burden of local data storage and maintenance. While Cloud computing makes these advantages more sympathetic than ever, it also brings regular challenges and security threats towards user's outsourced data. It's of crucial importance to customers to have strong evidence that they actually get the service what they paid. Data owners need to be Having a strong belief or conviction that their data are in an accurate manner stored in the Cloud. So, one of the significant concerns with cloud data storage is that of data integrity verification at un desired servers. Moreover, they need to verify that all their data copies are not being interfere unwontedly with or partially deleted over time In order to solve the problem of data integrity checking, many schemes are proposed under different systems of rules and security models. In this paper we surveyed three core integrity proving schemes in detail along with different methods used for data integrity in these schemes.

KEYWORDS: Cloud service provider , Provable Data Possession, Proof of Retrievability. Auditor component.

I. INTRODUCTION

Cloud Computing has been fancied as the next generation architecture of the IT enterprise due to its long list of exceptional advantages: on-demand self-service, ubiquitous network access, location-independent resource pooling, speedy resource elasticity, and usage based pricing. Cloud provides major three types of services

- Infrastructure as a service (IaaS): The quality of being capable physically, intellectually or legally provided to the consumer is to provision processing, storage, networks and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can Allow participation in or the right to be part of, permit to exercise the rights, functions, and responsibilities of operating systems and applications
- Platform as service(PaaS): This is a platform that provide services like OS, middleware and runtime for a developer to create, develop, deploy and to manage the applications. This layer just above the IaaS.
  Ex: IBM BlueMix, MS Azure and Amazon Web Services(AWS) etc.
- Software as service(SaaS): This is a layer just above the PaaS that provides an application as a service to a developer where he or she can make use of that services into their application.
  Ex: Salesforge application and gmail.

In particular, the ever cheaper and more powerful processors, together with the "software as a service" (SaaS) computing architecture, are transforming data centres into pools of computing service on a huge scale.

Data outsource conveys with it many vantages. But consociated with it are the risks involved. however client cannot physically access the data from the cloud server instantaneously, without clients are either not used by client from a prolonged period of time. Hence, there is a requirement of investigation the data At regular time intervals for rectification purpose, known as data integrity. In this circumstance provided a survey on the different techniques of data integrity.

One of the biggest concerns with remote data storage is that of data integrity verification at un-trusted servers[16]. For instance, the storage service provider may decide to hide such data loss incidents as the Byzantine failure from the

ISSN: 2350-0328
International Journal of Advanced Research in Science, Engineering and Technology
Vol. 3, Issue 2 , February 2016

clients to maintain a reputation. What is more serious is that for saving money and storage space the service provider might deliberately discard rarely accessed data files which belong to an ordinary client. Considering the large size of the outsourced electronic data and the client's constrained resource capability, the core of the problem can be generalized as how can the client find an efficient way to perform periodical integrity verification without the local copy of data files.

In order to overcome above problem, many schemes have been proposed under different system and security models these are The basic schemes for data integrity in cloud are Provable Data Possession (PDP) [1]. Second one is Proof of Retrievability (PoR).One more is Bounded and Reliable Rata Transmission in Cloud Using Auditor Component [17]. These three schemes are the most participating area of research in the cloud data integrity field, de-duplication of data and as well as dynamic integrity.

II. RELATED WORK

Verifying the Data Integrity is a ambitious process as it involves optimization of several metrics. There should not be any performance degradation and there should not be any loss of Usability. Several Researches have been carried out in this Area especially to optimize the Verification Process and also improve Security.

In a model is proposed called as Provable data possession which is a publicly verifiable mechanism which allows not only the Owner but anyone to Challenge the Server as it is Challenge-Response Algorithm and it utilises the similar Properties. There has been many improvisation provided based on this Mechanism and to support the evolving Multi-Cloud Environment[2]. But it provide a communication cost of order O(1).In a model is proposed called as Proofs of Retrievability which depends on pre-processing the Data by the client before sending the Data or Uploading it. Some Issues with Updating were overcome in Compact
version but it can only optimise to Communication Cost O(t) .

In a model is proposed called as Bounded and reliable data transmission in cloud using auditor component which uses Data Fragment Technique and Similarity of form Verifiable Tags to reduce Communication Cost as well as to improve Performance.

The following section gives the detailed explanation on Data Integrity Verification Schemes. The Mechanisms that are included are Provable data possession in Cloud and some of its Variants, Proofs of Retrievability and bounded and reliable data transmission in cloud using auditor component.

III.DATA INTEGRITY VERIFICATION SCHEMES

This Paper does not intend any new Schemes or any structure and organization of a computer's hardware or system software. It just surveys on Existing Schemes on Data Integrity in Cloud Environment. This Section provides the working of Several Integrity Verification Schemes proposed based on Researches carried out.

The Major three approaches of data Integrity that are included in this study are

1. Provable data possession (PDP).
2. Proofs of Retrievability (POR).
3. Bounded and reliable data transmission in cloud using auditor component.

A. PROVABLE DATA PROSSESSION(PDP):

To restore security assurances gnawed by cloud environments; researchers have intended two basic approaches to client verification of file accessibility and integrity. PDP scheme checks that a Separate cloud server retains a file, which consists of a collection of n blocks. The data owner processes the data file to render some metadata to store it locally. The cryptographic community has intended tools called proofs of retrievability (PORs) and proofs of data possession (PDPs).The file is then sent to the server, and the owner delete the local copy of the file. The owner affirms the possession of file in a challenge response protocol[1].

- **Sampling PDP and Efficient PDP:**

These PDP Schemes are based on Homomorphic Verifiable Tags (HVT) and Homomorphic Linear Authenticators (HLA) [4]. Sampling PDP and Efficient PDP Schemes carries out Verification based on the KEA1 assumption (Knowledge of Exponent Assumption) where if an un trusted Server stores the data transferred by a Client, Error is

ISSN: 2350-0328
International Journal of Advanced Research in Science, Engineering and Technology
Vol. 3, Issue 2 , February 2016

reported while Audition of data takes place. Data Possession is guaranteed only as a whole block which obtains more Cost. In this Method Tags are allocated to File Blocks as the Files are stored in blocks in Storage Server. The Cumulative Sum of all the Blocks is used as to verify the Integrity of the Data lay aside for future use.

- **Scalable PDP:**
  Scalable PDP Scheme is based on the cryptographic Technique which uses symmetric key[5]. Verification Scheme is done based on the challenge issued by server for random blocks of Data and the Server in turn should carry out the check just on the specified data blocks only hence minimizing time and cost for large Data Blocks The Data Owner Pre-Computes several tokens for a set of blocks of data before handling the Data over to the Server.
- **Dynamic PDP:**
  Dynamic PDP Scheme is used to address the problem when a user tries to update a data block like modification of Data or any other operations carried out on the Data [6]. When the User inserts some difference in data then the previous approach causes some incommodiousness or inconvenience. Dynamic PDP uses Authenticated Dictionary and also utilizes a slight Variant where rank information is used for organizing the entries which is essential for authenticated transactions Another Extension of Dynamic PDP known as DPDP-II uses RSA tree for authentication hence increased chance of Detection of inconvenience but there is more time consumption for update Operation.
- **Distributed and Replicated PDP:**
  Distributed and Replicated PDP Scheme is used to attain data replication over more than one server and the spatial or geographic property of being scattered about over a range hence its said to be distribution. This is achieved by means of using one of the Cloud Service Providers as Organizer which co-ordinates the communication between servers. Hence it supports multi-cloud storage[8] The Organizer performs only load balancing and no group or disk operations which can prove to be expensive. Hence it is feasible to use such an option .Also Replication of Organizer is made possible and essential to avoid failures due to excess Loads. This PDP does not allow Servers to communicate with each other in the absence of an Organizer.
  The Computation done by Organizer is larger when compared to Server hence it might create some extra Cost when verification is done in a Multi-Cloud Environment.
- **Basic Multi Copy PDP:**
  Basic Multi Copy PDP Scheme has a different Concept of making copies of the Data and generating Different Keys for each copy of Data and the generated keys are kept as secret from the cloud Service Provider [7]. Hence it disables the possibility of any counterfeit or forgery that a cloud Service Provider can cause. In This Scheme the Client can verify the possibility of any Integrity Act in disregard of laws, rules, contracts, or promises by challenging each copy of the Data that was created using any existing PDP Schemes .Hence it can be used as an extension for any PDP Scheme
- **Pairing based Provable Multi Copy Data Possession (PB-PMDP):**
  Pairing based Provable Multi Copy Data Possession PDP Scheme uses Verification method that can be any one not only the Data Owner. Users can access the copies anytime, anywhere without any constraint [10]. But the Copies that are created should be made different from each other .It uses the diffusion property of the PDP Schemes in order to implement the above, thus disabling the Cloud Service Provider of Cheating the Data Owner which might end up showing that it stored multiple copies when only one copy exists.

B. PROOFS OF RETRIEVABILITY (POR) SCHEME:

A Proof of retrievability is similar scheme to that of Provable Data Possession. It provides the proof that a file is Intact and not modified by any attack [11].This helps more in defining the existence of data than that of Integrity (i.e.) Helps more in Checking the full everything that exists anywhere of Data .Hence it is gives the proof of Existence. They consume less bandwidth than the file itself and hence can be used in remote environment.

The main feature that occurs in this Scheme is that they can correct any Data corruptness's that is found by using Error Correction codes

- **Compact Proofs of Retrievability:**

Compact Proofs of Retrievability uses Homomorphic Property to reduce the size of appraiser value and hence reduces the computational cost. This Scheme makes use of blocks called as Sentinel Blocks which are randomly inserted to detect data corruption in the Data that was uploaded by Client. After that the Data Error codes can be used to recover

ISSN: 2350-0328
International Journal of Advanced Research in Science, Engineering and Technology
Vol. 3, Issue 2 , February 2016

the data from corruption. Encrypted File Verification is being carried out in this Scheme and queries are limited to certain phase.

- Two Types of CPOR are
- Compact Proofs of Retrievability-I
- Compact Proofs of Retrievability-II
  The Difference that differentiates the two schemes is that the construction to support Verification option, the former offers Public Verifiability where anyone not only the data owner can verify the integrity of the Uploaded Data and the latter provides private Verifiability which grants verifiability option only to the Data Owner.

C. BOUNDED AND RELIABLE DATA TRANSMISSION IN CLOUD USING AUDITOR COMPONENT:

The existing scheme can simultaneously provide provable security in the intensified in value of security model and enjoy desirable efficiency, that is, no scheme can resist reset attacks while supporting efficient public verifiability and dynamic data operations simultaneously bounded and reliable data transmission in cloud using auditor component [17] model is the first to support dynamic update operations and security against reset attack in a verification scheme. The robustness against reset attack ensures that a malicious storage server can never gain any advantage of passing the verification of an incorrectly stored file by resetting the client (or the audit server) in the upload phase. In this will see that most of existing Bounded and reliable data transmission in cloud using auditor component schemes cannot ensure this strong security for cloud storage.

In this system an efficient verification scheme for ensuring remote data integrity in cloud storage. The proposed scheme is proved secure against reset attacks in the strengthened security model while supporting efficient public verifiability and dynamic data operations simultaneously proposed a dynamic version of the prior PDP scheme. The system imposes a priori bound on the number of queries and do not support fully dynamic data operations. In [15], Wang et al. considered dynamic data storage in distributed scenario, and the proposed challenge-response protocol can both determine the data correctness and locate possible errors. Similar to [12], they only considered partial support for dynamic data operation. In [14], they also considered how to save storage space by introducing deduplication in cloud storage. Recently, Zhu et al. [13] introduced the provable data possession problem in a cooperative cloud service providers and designed a new remote integrity checking system. In this scheme following are the model different models.

- **Client module:** an entity that has large data files to be stored in the cloud and trusts on the cloud for data upkeeps and computation, can be either individual consumers or organizations.
- **Cloud Storage Server (CSS) module:** an entity, which is managed by Cloud Service Provider (CSP), has significant storage space and computation resource to maintain client's data. The CSS is required to provide integrity proof to the clients or cloud audit server during the integrity checking phase.
- **Auditor component :** a TPA, which has expertise and capabilities that clients do not have, is trusted to assess and expose risk of cloud storage services on behalf of the clients upon request. In this system, the cloud audit server also generates all the tags of the files for the users before uploading to the cloud storage server.
- The basic goal of bounded and reliable data transmission in cloud using auditor component model is to achieve proof of retrievability. Informally, this property ensures that if an adversary can generate valid integrity proofs of any file F for a non-negligible fraction of challenges in this can construct a PPT machine to extract F with overwhelming probability.
- It is formally defined by the following game betien a challenger C and an adversary A, where C plays the role of the audit server (the client) and A plays the role of the storage server:
- **Setup Phase**: The challenger C runs the Setup algorithm to generate its key pair (pk, sk), and forwards pk to the adversary A.

Upload Phase: C initiates an empty table called Rlist. A can adaptively query an upload oracle with reset capability as follows: – Upload: When a query on a file F and a state index i comes, C checks if there is an entry (i, ri) in the R-list. If the ansir is yes, C overwrites ri onto its random tape; otherwise, C inserts (i, ri) into R-list where ri is the content on its random tape. Then C runs $(F*, t) \leftarrow$ Upload (sk, F; ri), and returns the stored file $F*$ and the file tag t. Here Upload(• ; ri) denotes an execution of the upload algorithm using randomness ri.

ISSN: 2350-0328

International Journal of Advanced Research in Science, Engineering and Technology

Vol. 3, Issue 2 , February 2016

- **Challenge Phase:** A can adaptively make the following two kinds of oracle queries: – Integrity Verify: When a query on a file tag t comes, C runs the integrity verification protocol Integrity Verify{A C(pk, t)} with A. – Update: When a query on a file tag ˆt and a data operation request "update" comes, C runs the update protocol Update{A C(sk, ˆt, update)} with A.

V. CONCLUSION

Cloud computing has emerged as a technology that has defined the way of computing and the types of services offered across the internet. There are several major concerns that occur in cloud Environment especially Data Integrity, This Paper carried a study on various data integrity Techniques in Cloud Environment, and it also introduced dynamic integrity in bounded and reliable data transmission of cloud using auditor component. This auditor component provides data integrity dynamically, reset attack and trust worthy services. Also Several Variants of these Techniques have been studied Hence this Paper Surveyed existing Techniques to initiate Future Research in this Area of Data Integrity to enhance Cloud Security.

REFERENCES

1. G. Ateniese, R. C. Burns, R. Curtmola, J. Herring, L. Kissner,Z. N. J. Peterson, and D. X. Song, "Provable data possession at untrusted stores," in ACM Conference on Computer and Communications Security, P. Ning, S. D. C. di Vimercati, and P. F.Syverson, Eds. ACM, 2007, pp. 598–609.
2. A. Juels and B. S. K. Jr., "Pors: proofs of retrievability for large files," in ACMConference on Computer and Communications Security, P. Ning, S. D. C. di Vimercati, and P. F. Syverson, Eds.ACM, 2007, pp. 584–597.
3. Kan Yang and Xiaohua Jia.,"TSAS: Third-Party Storage Auditing Service" in Security for Cloud Storage Systems,SpringerBriefs in Computer Science 2014, pp 7-37
4. G. Ateniese, R. Burns, R. Curtmola, J.Herring, L. Kissner, Z. Peterson, and D.Song, "Provable data possession at untrusted stores," in CCS '07: Proceedings of the 14th ACM Conference on Computer and Communications Security, New York, NY,USA, 2007, pp. 598–609.
5. G. Ateniese, R. Di Pietro, L. V. Mancini, and G. Tsudik, "Scalable and efficient provable data possession,"in Secure Comm '08: Proceedings of the 4th International Conference on Security and Privacy in Communication Netowrks, New York, NY, USA, 2008, pp. 110.
6. Q. Wang, C. Wang, J. Li, K. Ren, and W.Lou, "Enabling public verifiability and data dynamics for storage security in cloud computing," in ESORICS'09: Proceedings of the 14th European Conference on Research in Computer Security, Berlin, Heidelberg, 2009, pp. 355–370.
7. Ayad F.Barsoum and M.Anwar Hasan Provable Possession and Replication of Data over Cloud Servers.
8. Mohammad Etemad and Alptekin Koc University,Istanbul,Turkey."Transparent,Distributed, and Replicated Dynamic Provable Data Possession".
9. Zhu,Y.,Hu, H.,Ahn, G.,Yu, M.: Cooperative provable data possession for integrity verification in multi-cloud storage. IEEE Trans. Parallel Distrib. Syst. 23(12) 2231–2244 (2012).
10. Ayad F. Barsoum, M. Anwar Hasan. "Integrity Verification of Multiple Data Copies over Untrusted Cloud Servers".
11. A. Juels and B. S. K. Jr., "Pors: proofs of retrievability for large files," in ACMConference on Computer and Communications Security, P. Ning, S. D. C. di Vimercati, and P. F. Syverson, Eds.ACM, 2007, pp. 584– 597. G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, "Provable data possession at untrusted stores," in *CCS '07: Proceedings of the 14th ACM conference on Computer and communications security*. New York, NY, USA: ACM, 2007, pp. 598–609.
12. A. Juels and B. S. K. Jr., "Pors: proofs of retrievability for large files," in *CCS '07: Proceedings of the 14th ACM conference on Computer and communications security*. New York, NY, USA: ACM, 2007, pp. 584–597.
13. Y. Zhu, H. Hu, G.-J. Ahn, and M. Yu, "Cooperative provable data possession for integrity verification in multicloud storage," *IEEE Trans. Parallel Distrib. Syst.*, vol. 23, no. 12, pp. 2231–2244, 2012.
14. H. Xiong, X. Zhang, D. Yao, X. Wu, and Y. Wen, "Towards endto- end secure content storage and delivery with public cloud," in *CODASPY*, 2012, pp. 257–266.
15. Q. Zheng and S. Xu, "Secure and efficient proof of storage with deduplication," in *CODASPY*, 2012, pp. 1–12.
16. C. Wang, Q. Wang, and K. Ren, "Ensuring data storage security in cloud computing," in *Proceedings of IWQoS 2009*, Charleston, South Carolina, USA, 2009.
17. J. Li, X. Tan, X. Chen, D. Wong, and F. Xhafa, OPoR: Enabling proof of retrievability in cloud computing with resource-constrained devices," ac- cepted and to be publish in IEEE Transactions on Cloud Computing, Oct. 2015.

AUTHOR'S BIOGRAPHY

NIVEDITA M BULAGOUD, received the B.E degree in COMPUTER SCIENCE and pursuing M.Tech degrees in computer science from vemana Institute of Technology in 2014 - 2016, respectively. Under the guidance **MARY VIDYA JOHN** am doing my research work "Bounded and reliable data transmission in cloud using auditor component"

ISSN: 2350-0328

International Journal of Advanced Research in Science, Engineering and Technology

Vol. 3, Issue 2 , February 2016

MARY VIDYA JOHN, received the B.E. degree in computer science and M.Tech, working as assistance professor in VEMANA IT BANGALORE.