IJCSN International Journal of Computer Science and Network, Volume 5, Issue 3, June 2016
ISSN (Online) : 2277-5420 www.IJCSN.org
Impact Factor: 1.02

Review on Secure Proof of Retrievability

[1] Saurabhee Wandhekar, [2] Aradhana Deshmukh

[1] Dept. of computer Engineering,Savitribai phule pune university, SKNCOE.

[2] Prof. at Department of computer Engineering, SKNCOE

Abstract - Moving user data on cloud provides convenience and avoids the complexity and hardware management for the user. However, the cloud concept brings many challenges which influence the system on various factors such as usability, security, reliability, scalability and overall system performance. User who is storing the data on cloud server has to check the integrity of the data which becomes an overhead every time. This task is outsourced to another public auditor. These parties may not be trustworthy. To mitigate this possibility and to alleviate the integrity checking and computation overhead we proposed a system. Proposed system does the integrity checking and preserves the privacy of the data from the Third Party Auditor.

Keywords - *Cloud Storage, Integrity, Proof of Retrievability [POR], Public Auditing.*

1. Introduction

Cloud computing is a next generation architecture of IT enterprises possess advantages like on-demand self-service, reliable and flexible network with increasing bandwidth, rapid resource elasticity, and usage-based pricing. The cheaper and powerful processors with the software as a service (SaaS) computing architecture are transforming data centers into pools of computing service on a huge scale.Users can now use high quality services from data (storage) and software(Enterprise software)on remote data center.

Though moving user data on cloud provides convenience and avoids the complexity and hardware management for the user, the cloud concept brings many challenges which influence the system on various factors such as usability, security, reliability, scalability and overall system performance for e.g. to preserve the reputation, service providers may hide such data losses or discard rarely accessed data intentionally. There is need to verify that the data residing on cloud is safe and not tampered. All schemes can be divided in two categories. First are privateverification scheme in which verification can be done only by owner of the data. Another is Public verification schemes in which data integrity verification can be done by anyone on the behalf of the data owner. Problem of the Private verification schemes is that data owner gets excessively overloaded with this task. In the case of public verification schemes user is alleviated from this task. In private verification task there is chance to crash the user's computing devices due to complex verification calculations, so there is high chance that user's will accept the public verification. All current verification schemes do not consider that cloud provides dynamic operations on the data stored on the cloud. G. Ateniese et al. [1]onsiders this issue also and proposes efficient Public integrity verification scheme.

2. Background

Cloud Storage- It is most important feature in cloud computing. It is model of the storage in which data is stored in logical pools, physical storage is spread on multiple servers and all hardware part is provided by cloud owner party as a service. Service providers are responsible for on demand accessibility, integrity and security of the data. Most of the organizations choose cloud storage to focus on their business by outsourcing storage maintenance

Integrity- One of the important feature provided of cloud storage is Integrity by which CSP assures that data will not be changed or modified or deleted from their side or by any other third party. To use the data stored on the cloud it is very important to check the Integrity of the data.

Proof of retrievability – Downloading the data from cloud storage and check the Integrity is not practical solution for checking the Integrity of the data. For practical solution cloud sends some proof of retrievability to prove the integrity of the data.

Public Auditing- Checking the integrity is interactive process and needs user to be online during auditing

process. To mitigate the load of the auditing task is outsourced to another party is called as Public Auditing.

2.1 Related Work

Despite of many advantages of Cloud Computing, It also arises the some issues related to data integrity and computation cost. When user stores the data on server there is need for assurance of data security. G. Atenieseet al.[1] a model for provable data possession (PDP) is introduced. It allows the client who has stored data on untrusted server possesses original data without retrieving it. This model reduces I/O cost by sampling random sets of blocks from server which generates probabilistic proof of possession. Issue here is that the data owner has to compute a large number of tags for those data to be outsourced, which usually involves exponentiation and multiplication operations.In this POR scheme can only be can handle only a limited number of queries, which has to be fixed a priori.

A. Juelset al.[2] defines the proof of retrievability(PORs) enables a backup service to produce a proof that a user can retrieve desired data i.e. the backup or archives holds and transmit sufficient data to user reliably. POR designed to handle a large file. It is an important tool for online storage. To ensure privacy and integrity of retrieved file some cryptographic techniques are helpful. It's obvious that user wants to verify that the storage do not modify or delete files before retrieval. POR aims to achieve this without users having to download the file and guarantees file retrieval within time.

Scheme in [3] discussed the issues that how to frequently and securely with the efficiency verify that the client's data is safely and reliably stored on storage server. In [1], the dynamic data storage is not considered. In this paper [3] Ateniese et.al., proposed a dynamic storage of its prior PDP scheme. PDP is based on symmetric key cryptography and allows dynamic data to be outsourced i.e. it supports operation such as block modification, deletion and append. The system imposes a priori bound in the number of queries and do not support fully dynamic data. It uses a private verification scheme for POR so does not give a secure POR

H. Shacham et al.[4] proposed security model for Proof of retrievability. Checking scheme on the basis of following points-
i) It is possible to recover original data by using multiple challenges responses.
ii) Any algorithm cannot cheat the verifier with non – negligible probability. In PoR, client sends challenge after some time to ensure the integrity of the data stored on the cloud. Paper proposed the PoR scheme based on BLS signatures in which client's query and response from server is very short in length.

To ensure the user's data accuracy C. Wang et al. [5] proposed flexible distributed scheme with two important features. This scheme achieves identification misbehaving server(s) i.e. integration of surety of storage correctness and data error localization by utilizing homomorphic token with distributed verification of erasure coded data. However, they only considered partial support for dynamic data operation so does not give POR if data is modified.

Jin Li et al.[6] addressed the need of Third Part Auditor and designed the scheme for public integrity checking. Proposed system also considered the need of dynamic changes in the data stored on cloud by cloud users. Proposed scheme used Merkel hash tree for full dynamic data operations. Tag generation process executed at client's device. This system also does not provide a secure POR.

H. Xiong et al. [7] proposed end to end secure model by designing CloudSeal scheme which ensures confidentiality of content in the public cloud environments and provides facility of securely sharing and distributing content in public cloud. CloudSeal used efficient cipher content transformation in the delivery network and user key management. It achieves efficiency and avoids performance issues.

K. D. Bowers et al.[8] proposed a new variant on the Juels-Kaliski protocol and describe a prototype implementation for Proof of Retrievability. Proposed scheme is required less memory, tolerate higher error rate and secure against strong adversary model. System can encode file whose size is greater than main memory of the client's machine. It supports a fully Byzantine adversarial model, carrying only the restriction—fundamental to all PORs—that the adversary's error rate be bounded when the client seeks to extract FStoring a large file on a remote and unreliable server is of concern for data owner. To verify that the file has not been corrupted, a user could store a small private finger-print on his computer. User encodes and store a file in a way that it allows to verify that the file is has not been corrupted without reading entire file. This problem is called sub-linear authentication i.e. authenticating a message without reading all of its bits. An authenticator is a cryptographic object for encoding and storing clients file. Space, query and size of the secret are the main online complexity measures.

G. N. Rothblum et al. [9] showed that with lower space and query complexity any online memory checker can be used to construct an authenticator. This system is time consuming and takes a lot of time to give POR

Q. Zheng et al. [10] deals with dynamic data and ensures Proof of Retreivability and also considers another problem called fairness. Fairness property ensures that the dishonest owner cannot lawfully claim the honest cloud service provider. Service provider has to face difficulties if there is no proof about not manipulating the owner's data. Solution to this is to digitally sign the data by owner before outsourcing the data. Due to dynamic nature of data is not always possible. The problem is addressed with the introduction of new incremental signature scheme called Hash-Compressed and Signs (HCS). New authenticated data structure called Range-Based 2 3 tree (rb23Tree) is proposed for dynamic POR. The scheme is secure and efficiently worked on dynamic data.

Y. Zhu et al.[11] also proposed proof of retrievability for data stored on the cloud. Audit services are designed based on the fragment structure, random sampling and index-hash table. Proposed audit service supports dynamic update to the stored data. Additionally paper proposed efficient method based on periodic verification and probabilistic query for improving the performance of auditing. Security solutions such as Proof of Data Possession and Proof of Retrievability introduced to check the data modification or deletion at storage server side i.e. on cloud. Also the concept of Proof of Ownership (POW) evolved to relieve the cloud from storage of multiple copies of same data. This reduced the used server storage space and also the consumption of network bandwidth.

Q. Zheng et al.[12] it is showed that the two aspects (PDP and POW) can coexist within same framework. On this phenomenon they proposed Proof of Storage with Deduplication (POSD). In survey of "digital universe decade - are you ready?" International Data Corporation, 2010, it is stated that only 25% of data may unique. By storing a single copy of each data, much cloud space can be saved irrespective of number of clients outsourced it.

Y. Zhu et al. [13] addressed the provable data possession problem in distributed cloud storage to support the data migration and scalability of service. To solve this problem paper proposed remote integrity checking scheme which is designed with assumption of multiple cloud service providers to cooperate store and maintain the data submitted by clients.

B. Wang et al. [14] addressed the need of privacy preservation of the cloud data signer during public integrity verification and proposed the Privacy preserving mechanism which allows public integrity verification on shared data. Using this scheme identity of data signer at the time data upload is kept private from Third Party Auditor. Proposed scheme does not support dynamic data modification. Tag generation process is at client's side. To address the different security, efficiency and reliability issues in cloud computing different schemes and techniques are introduced.

Q. Wang et al.[15] proposes very efficient remote data verification scheme (audit server) supports public verifiability and dynamic data support for PoR service simultaneously. The scheme also reduced the user's burden of computing tags of outsourced data and defines the new security model for cloud storage which is able to resist the reset attacks invoked by the cloud server storage in upload phase.

Before [15] there was no any prior work which provides public verification, dynamic data support and outsourced tag generation. In the existing system of [15] tag generation is done at third party, data is which is to be uploaded on the cloud is visible to third party i.e. auditor. As this data is visible to the auditor there is privacy leak for the data. If user doesn't want to disclose its data to any third party then existing system does not provide any privacy preservation mechanism during tag generation.

3. Proposed Work

3.1 Limitation of Existing System

i. Existing system was designed with the assumption that third public auditor is trusted party. In the existing system all thedata of the files is visible to the public auditor which leaks the privacy of the data.
ii. Blocks of the plain text files are stored on the cloud storage and here also data of the clients can be misused by the cloud storage server

3.2 Scheme of Proposed System

In our system we are going to establish Secure Integrity system for public verification scheme. The objective of proposed system is to provide Security for public verification scheme. The proposed system architecture is shown in Figure 1.In this cloud user encrypt the file before uploading to the cloud auditor. At the cloud auditor tagsand signatures are calculated and these tags and signatures along with the file are sent to the cloud storage server. When user wants to see the integrity of uploaded file he/she will send integrity checking query. At the cloud storage server Integrity verification is done using tags and signatures of uploaded file. If the file is in integrated format then it sends proof of integrity to cloud user. Then user can download the file. When it starts downloading the file is decrypted automatically. In this proposed system

tags and signatures are generated at cloud audit server so it will reduce client's computational load.

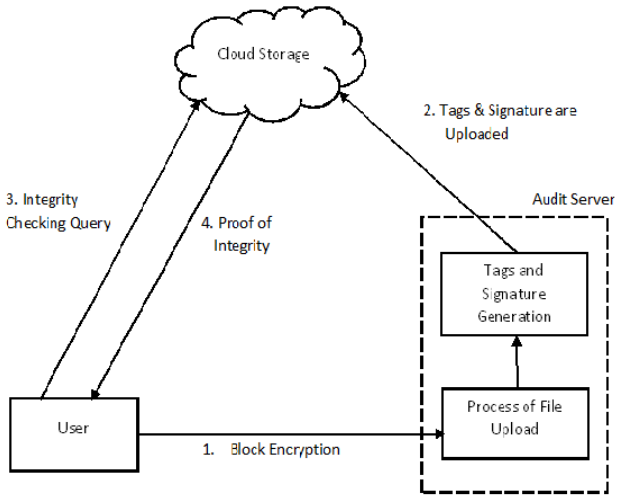

Figure1: System scheme

4. Conclusion

This paper describes importance of the cloud for storage, challenges in using cloud as storage and prior works to solve those challenges. Paper addressed the lack of privacy preservation in existing system and proposed a system which provides Public Integrity verification, Privacy from public auditor and cloud storage server, Dynamic Data modification.

References

[1] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, "Provable data possession at untrusted stores," in Proc. 14th ACM Conf. Comput. Commun. Security, 2007, pp. 598–609. 1

[2] A. Juels and B. S. Kaliski Jr, "Pors: Proofs of retrievability for large files," in Proc. 14th ACM Conf. Comput. Commun. Security, 2007, pp. 584–597. 2

[3] L. V. M. Giuseppe Ateniese, R. D. Pietro, and G. Tsudik, "Scalable and efficient provable data possession," in Proc. Int. Conf. Security Privacy Commun. Netw., 2008, pp. 46–66. 11

[4] H. Shacham and B. Waters, "Compact proofs of retrievability" in Proc. 14th Int. Conf Theory Appl Cryptol. Inf. Security, 2008,

[5] C. Wang, Q. Wang, and K. Ren, "Ensuring data storage security in cloud computing," in Proc. 17th Int. Workshop Quality Serv., 2009, pp. 1–9. 22

[6] Jin Li, Xiao Tan, Xiaofeng Chen, Duncan S. Wong, and Fatos Xhafa, "OPoR: Enabling Proof of Retrievability in Cloud Computing with Resource-Constrained Devices," IEEE 2015.

[7] H. Xiong, X. Zhang, D. Yao, X. Wu, and Y. Wen,"Towards end-to-end secure content storage and delivery with public cloud," in Proc. ACM Conf. Data Appl. Security Privacy, 2012, pp. 257–266.

[8] K. D. Bowers, A. Juels, and A. Oprea, "Proofs of retrievability: Theory and implementation," in Proc. ACM Workshop Cloud Comput. Security, 2009, pp. 43–54

[9] M. Naor and G. N. Rothblum, "The complexity of online memory checking," J. ACM, vol. 56, no. 1, pp. 2:1–2:46, Feb. 2009.

[10] Q. Zheng and S. Xu, "Fair and dynamic proofs of retrievability,"in Proc. 1st ACM Conf. Data Appl. Security Privacy, 2011, pp. 237–248.

[11] Y. Zhu, H. Wang, Z. Hu, G.-J. Ahn, H. Hu, and S. S. Yau, "Dynamic audit services for integrity verification of outsourced storages in clouds," in Proc. ACM Symp. Appl. Comput., 2011,pp. 1550–1557.

[12] Q. Zheng, and S. Xu, "Secure and efficient proof of storage with deduplication," in Proc. ACM Conf. Data Appl. Security Privacy, 2012, pp. 1–12.

[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, Dec. 2012.

[14] H. Li, B. Wang, and B. Li, "Oruta: Privacy-preserving public auditing for shared data in the cloud," IEEE Trans. Cloud Comput., vol. 2, no. 1, pp. 43–56, Jan.–Mar. 2014

[15] Q. Wang, C. Wang, J. Li, K. Ren, and W. Lou, "Enabling public verifiability and data dynamics for storage security in cloud computing," in Proc. 14th Eur. Symp. Res. Comput. Security, 2009, pp. 355–370

Saurabhee Wandhekar received the Bachelors degree in Computer Engineering and currently pursuing Masters degree in Computer Engineering both from Savitribai Phule Pune University.Her research interests include cloud computing.

Aradhana Deshmukh received M.E., M.A. (Economics), Ph.D (pursing).Shehas an excellent academic background. She has almost 11years of teaching experience. She is currently working as Assistant Professor in the Department of computer Engineering, STES's, Smt. Kashibai Nawale College of Engineering, Pune. She has published 81 papers in Internationl Journals, Conferences. She has received Gold Medal at International level Paper Presentationon 'UWB Technology based Adhoc Network', received 'Gunawant Nagrik Puraskar'for the year 2004-2005, 'Anushka Purskar' form Pimpari ChinchwadMunicipal Corporation, Pune. She was elected from Computer Engineering division in Institution of Engineers (India) continuously from 2002 to 2014. She is a member of Computer, Society of India (CSI), Member IAENG, Hongkong, Member UACEA, USA.