INNOVARE JOURNAL OF ENGINEERING & TECHNOLOGY

Vol 7, Issue 3, 2019

ISSN - 2347-1573

Review Article

ACTIVE-HASH-TABLE BASED PUBLIC AUDITING FOR SECURE CLOUD STORAGE

BALAKRISHNAN K, VIDHYA R

Department of Computer Science, SRM University, Chennai, Tamil Nadu, India. Email:K.balabalu@gmail.com

Received: 19 January 2019, Revised and Accepted: 30 March 2019

ABSTRACT

Public auditing scheme for secure cloud storage based on dynamic hash table, which is a new two-dimensional data structure located at a third-party auditor (TPA) to record the data property information for dynamic auditing. Differing form the existing works, the proposed scheme migrates the authorized information from the cloud services provider to the TPA and thereby significantly reduces the computational cost and communication overhead. Our scheme can also achieve higher updating efficiency than the state of the art schemes. In addition, we extend our scheme to support privacy preservation by combining the homomorphic authenticator based on the public key with the random masking generated by the TPA and achieve batch auditing by employing the aggregate BLS signature technique. We formally prove the security of the proposed scheme and evaluate the auditing performance by detailed experiments and comparisons with the existing ones. The results demonstrate that the proposed scheme can effectively achieve secure auditing for cloud storage and outperform the previous schemes' in computation complexity, storage costs, and communication overhead.

Keywords: Cloud storage, Cloud security, Public auditing, Dynamic hash table.

INTRODUCTION

Cloud storage is an important branch of cloud computing, whose goal is to provide powerful and on-demand outsourcing data services for users exploiting highly virtualized infrastructures. Due to the low cost and high performance of cloud storage, a growing number of organizations and individuals are tending to outsource their data storage to professional cloud services providers (CSPs), which buoy the rapid development of cloud storage and its relative techniques in recent years. However, as a new cutting-edge technology, cloud storage still faces many security challenges. One of the biggest concerns is how to determine whether a cloud storage system and its provider meet the legal expectations of customers for data security. This is mainly caused by the following reasons. First, cloud users (data owners), who outsource their data in clouds, can no longer verify the integrity of their data through traditional techniques that are often employed in local storage scenarios. Second, CSPs, which suffer byzantine failures occasionally, may choose to conceal the data errors from the data owners for their own self-interest. What is more severe, CSPs might neglect to keep or even deliberately delete rarely accessed data that belong to ordinary customers to save storage space. Therefore, it is critical and significant to develop efficient auditing techniques to strengthen data owners' trust and confidence in cloud storage, of which the core is how to effectively check data integrity remotely. So far, many solutions have been presented to overcome this problem, which can be generally divided into two categories such as private auditing and public auditing. Private auditing is the initial model for remote checking of data integrity, in which the verification operation is performed directly between data owners and CSPs with relatively low cost. However, it cannot provide convincing auditing results since the owners and CSPs often mistrust each other. Moreover, it is not advisable for the users to carry out the audit frequently since it would substantially increase the overhead that the users may not afford. Thus, Ateniese *al*first presented the public auditing scheme, in which the checking work is customarily done by an authorized third-party auditor (TPA). Compared with the former, the latter can offer dependable auditing results and significantly reduce users' unnecessary burden by introducing an independent TPA. Thus, it is more rational and practical and popularly believed to be the right direction of future development.

Privacy preserving

Data privacy protection has always been an important topic for cloud storage. In the public auditing, the core of this problem is how to preserve users' privacy while introducing a TPA. Although exploiting data encryption before outsourcing is an approach to mitigate the privacy concern in cloud storage, it cannot prevent data leakage during the verification process. Thus, it is important for the cloud auditing to include a privacy-preserving mechanism independent of data encryption.

Batch auditing

To enhance the efficiency and enable the scalability of public auditing, the TPA should deal with multiple auditing tasks from various users in a fast and cost-efficient manner, i.e., support the batching auditing.

Dynamic auditing

As it is well known that a cloud storage system is not just a data warehouse, the users often need to update the data dynamically motivated by various application requirements. Therefore, it is significant for cloud storage auditing to support data dynamics. For the dynamic data auditing, Erway *et al*. first presented a dynamic provable data possession scheme, which extends the original PDP model by introducing a rank-based authenticated skip list.

LITERATURE SURVEY

Title: A survey of cloud storage facilities

Author: H. Dewan and R. C. Hansdah

Description

As interest in the cloud increases, there has been a lot of talk about the maturity and trustworthiness of cloud storage technologies. Is it still hype or is it real? Many end users and IT managers are getting very excited about the potential benefits of cloud storage, such as being able to store and manipulate data in the cloud and capitalizing on the promise of higher performance, more scalable, and cheaper storage. In this paper, we present a typical cloud storage system architecture, a reference cloud storage model and multitenancy cloud storage model, survey the past and the state-of-the-art of cloud storage, and discuss the advantage and challenges that must be addressed to implement cloud storage. Use cases in various cloud storage offerings were also summarized.

Title: Toward secure and dependable storage services in cloud computing

Author: Jiyi WU, Jianqing FU, Zhijie LIN

Description
As interest in the cloud increases, there has been a lot of talk about the maturity and trustworthiness of cloud storage technologies. Is it still hype or is it real? Many end users and IT managers are getting very excited about the potential benefits of cloud storage, such as being able to store and manipulate data in the cloud and capitalizing on the promise of higher performance, more scalable, and cheaper storage. In this paper, we present a typical cloud storage system architecture, a reference cloud storage model and multitenancy cloud storage model, survey the past and the state-of-the-art of cloud storage, and discuss the advantage and challenges that must be addressed to implement cloud storage. Use cases in various cloud storage offerings were also summarized.

Title: Enabling public auditability and data dynamics for storage security in cloud computing

Author: Q. Wang, C. Wang, K. Ren, W. Lou and J. Li

Description
We consider the task of allowing a TPA, on behalf of the cloud client, to verify the integrity of the dynamic data stored in the cloud. The introduction of TPA eliminates the involvement of the client through the auditing of whether his data stored in the cloud are indeed intact, which can be important in achieving economies of scale for cloud computing. The support for data dynamics through the most general forms of data operation, such as block modification, insertion, and deletion, is also a significant step toward practicality since services in cloud computing are not limited to archive or backup data only. While prior works on ensuring remote data integrity often lack the support of either public auditability or dynamic data operations, this paper achieves both. We first identify the difficulties and potential security problems of direct extensions with fully dynamic data updates from prior works and then show how to construct an elegant verification scheme for the seamless integration of these two salient features in our protocol design. In particular, to achieve efficient data dynamics, we improve the existing proof of storage models by manipulating the classic Merkle Hash Tree construction for block tag authentication. To support efficient handling of multiple auditing tasks, we further explore the technique of bilinear aggregate signature to extend our main result into a multiuser setting, where TPA can perform multiple auditing tasks simultaneously. Extensive security and performance analysis show that the proposed schemes are highly efficient and provably secure.

PROPOSED SYSTEM

In the proposed work, the data owner uploads the files on the cloud storage with some security. The uploaded file is encrypted and splitted using the hash table concept and upload into the cloud storage. The end user can able to download the data from the cloud storage with the original date name, at the receiving end decrypt the original files.

Problem statement
In this work, we concentrate on the design of an effective public auditing scheme based on the dynamic hash table (DHT) illustrated in which involves the following three entities: User, who stores a great quantity of data files in the cloud, can be an individual or an organization; cloud service provider who manages and coordinates a number of cloud servers to offer scalable and on-demand outsourcing data services for users; and TPA, who can verify the reliability of the cloud storage services credibly and dependably on behalf of the users upon request. Users can be relieved of the burden of storage and computation while enjoying the storage and maintenance service by outsourcing their data into the CSP. However, due to the loss of local possession of the data, they are keen to ensure the correctness and integrity of their data periodically. To obtain a convincing answer as well as alleviate the users' burden potentially induced by the frequent verification, the TPA is involved to check the integrity of the user's data stored in the cloud. However, in the whole verification process, the TPA is not expected to be able to learn the actual content of the user's data for privacy protection. We assume that the TPA is credible but curious. In other words, the TPA can perform the audit reliably but may be curious about the user's data. In addition, the CSP is considered to be dishonest. That is to say, the CSP may choose to hide the fact of some data being corrupted motivated by self-interest. Especially, the CSP may launch the following attacks to the TPA:

- Forge attack: The CSP may forge the data blocks and/or their tags to deceive the verifier.
- Replacing attack: The CSP may want to pass the verification by replacing a required block and its tag, which have been corrupted, with another block and its corresponding tag.
- Reply attack: The CSP may attempt to pass the verification using the proof generated from the previous ones or other former information.

To enable secure and efficient public auditing for cloud storage, our scheme is designed to achieve the following objectives:

1. Public auditing: Anyone (not only the users) is allowed to have the capability to verify the correctness and integrity of the user's data stored in the cloud.
2. Storage correctness: The CSP, which does not correctly store user's data as required, cannot pass the verification.
3. Block less verification: No data block needs to be retrieved by the TPA during the verification process.
4. Dynamic data auditing: Dynamic data operations should be supported while the efficient public auditing is achieved.
5. Privacy preserving: The TPA cannot derive any actual content of user's data from the received auditing information.
6. Batch auditing: The TPA can handle multiple auditing tasks from various users in a fast and cost-efficient manner.
7. Lightweight: The verification should be performed with the minimum.

Dynamic verification with privacy preserving
Let $\Re 1$ and $\Re 2$ be multiplicative cyclic groups of a large prime order p, and e be a bilinear map $\Re 1 \times \Re 1 \rightarrow \Re 2$. H is a secure hash function with $H:\{0, 1\}^* \rightarrow \Re 1$; assume that, the file (denoted by F) to be outsourced to the CSP is divided into n blocks, i.e., $F= \{m1, m2,..., mn\}$. Our dynamic auditing scheme involves two phases: Setup and verification. The setup phase can be completed by the following steps:

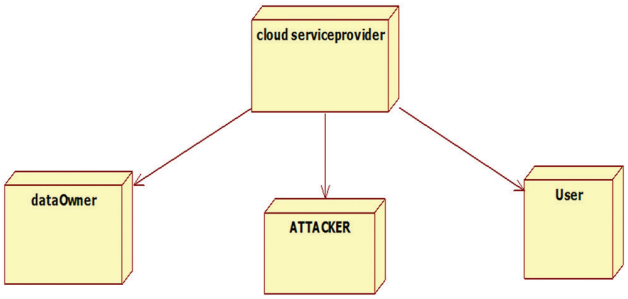
- Step 1 (key initiation): The user generates a key pair ($SK = \{a, sk\}$, $PK = \{g, y, u, pk\}$), where (sk, pk) is a random key pair of the user for signature, $a \in \Im p$ is a random number, g and u are the random elements of $\Re 1$ and $y = ga$
- Step 2 (data information initiation): The user sends the data information (ID, $\Phi=\{(vi, ti)|1\leq i\leq n\}$) to the TPA, Where, ID is the unique identifier of F, $\Phi=\{(vi,ti)|1\leq i\leq n\}$ is the set of all blocks' VI, and vi and ti are, respectively, the version and timestamp of the block mi. On receiving the data information, the TPA will add it into the DHT
- Step 3 (Signature Generation): For each block mi, the user generates a signature σi with the public key u, which can be described as follows: Moreover, to ensure the integrity of the unique file identifier ID, the user computes the file tag $\vartheta = ID \parallel \mathrm{SIG}(sk, ID)$, where SIG ($sk$, ID) is the signature on ID under the private key sk. Let the set of all blocks' signatures be $\sigma = \{\sigma i|1\leq i\leq n\}$. The User uploads F, ϑ, and σ to the CSP, and deletes them from the local storage
- Step 4 (tag generation): For each block mi, the CSP further creates a tag θi based on the received signature σi using the bilinear map e, namely (,) i i $\theta=e$ σ y. Let the set of all block tags be $\theta=\{\theta i|1\leq i\leq n\}$. At last, the CSP should store the verification metadata (ϑ, θ) along with the file $F=\{m1, m2, mn\}$.

Note: That we assume that the CSP creates a tag θi for each block mi here. However, it is not the best choice.

Since each tag is an element of $\Re 1$, the n tags for n blocks would cost a great deal of extra storage space, which is evidently uneconomic in terms of the pay-as-you-go pricing model. Therefore, the segment strategy is popularly adopted to reduce the space cost. Specifically, each data block is further divided into s segments, i.e., $mi= \{mi,1, mi,2,..., mi, s\}$, and its corresponding signature is calculated as follows: Instead

of Equation (3). In this way, the storage overhead can be reduced to $1/s$ of the original one. However, it is worthwhile to emphasize that each signature and each tag still corresponds to a block rather than a segment. In other words, the segment strategy performed by the user is just an approach to reduce the storage overhead of tags in the CSP, and it is transparent (invisible) to the TPA.

SYSTEM ARCHITECTURE



MODULES

- Data owner/file upload module
- End user/file download module
- Dynamic updating
- Batch verification
- Storage provider.

Data owner (file upload) module

In this module, files are uploaded by the data owner to the cloud server. For this, he has to first register. The owner has to fill the details in the registration form. The file uploaded is encrypted using the bit exchanging method. The data owner can view the secret key generated for the file. Data owner can update the ciphertext.

End user (file download) module

In this module, user selects a particular file and requests for the key. The key authority provides the secret key. Along with the key, user receives one-time password (OTP) on their mail. The file is decrypted only when the user enters the correct key and OTP. User downloads the file in decrypted format. For the decryption process also, BEM is used. If the wrong key is entered more than twice, the user's account is revoked. After downloading the file, the user will logout the session.

Dynamic updating

To support the efficient management of dynamic data uploading and download manner. We design updating operations on the DHT for the data blocks and files, respectively. The updating operations of data blocks include block modification block insertion and block deletion.

Batch verification

The core of the batch auditing is how to concurrently handle multiple verification tasks from different users. Specifically, this is equivalent to the verification of many signatures on different messages by different users. Thus, we introduce the aggregate BLS signature technique from bilinear maps to achieve the batch verification, which the idea behind is to aggregate all the signatures by different users on various data blocks into a single short one and verify it for only one time to reduce the communication cost in the verification process. Assume that, there are k challenges launched by k different users.

Storage provider

Storage provider is the administrator. The storage provider can login and view storage server files, view. Secret key, view users, view data owners, view transactions.

CONCLUSIONS

Nowadays, cloud storage, which can offer on-demand outsourcing data services for both organizations and individuals, has been attracting more and more attention. However, one of the most serious obstacles to its development is that users may not fully trust the CSPs in that it is difficult to determine whether the CSPs meet their legal expectations for data security. Therefore, it is critical and significant to develop efficient auditing techniques to strengthen data owners' trust and confidence in cloud storage. In this paper, we are motivated to present a novel public auditing scheme for secure cloud storage using DHT, which is a new two-dimensional data structure used to record the data property information for dynamic auditing. Differing from the existing works, our scheme migrates the auditing metadata excerpt the block tags from the CSP to the TPA and thereby significantly reduces the computational cost and communication overhead. Meanwhile, exploiting the structural advantages of the DHT, our scheme can also achieve better performance than the state-of-the-art schemes in the updating phase. In addition, for privacy preservation, our scheme introduces a random masking provided by the TPA into the process of generating proof to blind the data information.

REFERENCES

1. Dewan H, Hansdah RC. A Survey of Cloud Storage Facilities. Proceeding 7th IEEE World Congress on Services; 2011. p. 224-231.
2. Wang C, Wang Q, Ren K, Cao N, Lou W. Toward secure and dependable storage services in cloud computing. IEEE Trans Service Comput 2012;5:220-32.
3. Ren K, Wang C, Wang Q. Security challenges for the public cloud. IEEE Internet Comput 2012;16:69-73.
4. Ryoo J, Rizvi S, Aiken W, Kissell J. Cloud security auditing: Challenges and emerging approaches. IEEE Secur Priv 2014;12:68-74.
5. Wang C, Ren K, Lou W, Li J. Toward publicly auditable secure cloud data storage services. IEEE Netw 2010;24:19-24.
6. Wang Q, Wang C, Ren K, Lou W, Li J. Enabling public auditability and data dynamics for storage security in cloud computing. IEEE Trans Parallel Distrib Syst 2011;22:847-59.
7. Sebé F, Domingo-Ferrer J, Martínez-Ballesté A, Deswarte Y, Quisquater JJ. Efficient remote data possession checking in critical information infrastructures. IEEE Trans Knowl Data Eng 2008;20:1034-8.
8. Juels A, Kaliski BS Jr. PoRs: Proofs of Retrievability for Large Files. Proceeding ACM Conference Computer and Communications Security CCS '07; 2007 p. 584-597.
9. Ateniese G, Johns RB, Curtmola R, Herring J, Kissner L, Peterson Z, *et al*. Provable Data Possession at Untrusted Stores. Proceeding 14th ACM Conference on Computer and Communication Security; 2007. p. 598-609.
10. Yang K, Jia X. Data storage auditing service in cloud computing: Challenges, methods and opportunities. World Wide Web 2012;15:409-28.
11. Wang C, Wang Q, Ren K, Lou W. Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing. Proceeding IEEE INFOCOM; 2010. p. 1-9.
12. Wang C, Chow SM, Wang Q, Ren K, Lou W. Privacy-preserving public auditing for secure cloud storage. IEEE Trans Comput 2013;62:362-75.
13. Zhu Y, Hu H, Ahn G, Yu M. Cooperative provable data possession for integrity verification in multi-cloud storage. IEEE Trans Parallel Distrib Syst 2012;23:2231-44.
14. Yang K, Jia X. An efficient and secure dynamic auditing protocol for data storage in cloud computing. IEEE Trans Parallel Distrib Syst 2013;24:1717-26.
15. Erway CC, Küpçü A, Papamanthou C, Tamassia R. Dynamic Provable Data Possession. Proceeding 16th ACM Conference Computer and Communication Security; 2009. p. 213-22.
16. Zhu Y, Wang H, Hu Z, Ahn GJ, Hu H, Yau SS. Dynamic audit services for outsourced storage in clouds. IEEE Trans Serv Comput 2013;6:227-38.
17. Boneh D, Lynn B, Shacham H. Short Signatures from the Weil Pairing. Vol. 2248. Proceeding ASIACRYPT LNCS; 2001. p. 514-32.
18. Wang B, Li B, Li H. Panda: Public auditing for shared data with efficient user revocation in the cloud. IEEE Trans Serv Comput 2015;8:92-106.
19. Liu C, Ranjian R, Zhang X, Yang C, Georgakopoulos D, Chen J. Public Auditing for Big Data Storage in Cloud Computing a Survey. Proceeding 16th IEEE International Conference Computational Science and Engineering; 2013.p. 1128-35.
20. Liu C, Chen J, Yang LT, Zhang X, Yang C, Ranjan R, Ramamohanarao K. Authorized public auditing of dynamic big data storage on cloud with

efficient verifiable fine-grained updates. IEEE Trans Parallel Distrib Syst 2014;25:2234-44.

21. Boneh D, Gentry C, Lynn B, Shacham H. Aggregate and Verifiably Encrypted Signatures from Bilinear Maps. Proceeding 22nd Int'l Conference Theory and Applications of Cryptographic Techniques Eurocrypt '03; 2003. p. 416-432.
22. Shacham H, Waters B. Compact Proofs of Retrievability. Proceeding 14th Int'l Conference Theory and Application of Cryptology and Information Security: Advances in Cryptology ASIACRYPT '08; 2008. p.90-107.