Secure Audit Service by Using TPA for Data Integrity in Cloud System

Shingare Vidya Marshal

Abstract— Cloud computing is the vast computing utility, where users can remotely store their data into the cloud so to have the benefit of the on-demand availability of huge and different applications and services from a shared pool of configurable computing resources.

Cloud-based outsourced storage space reduces the patron load of storage management. It also reduces the maintenance load of customer by providing a comparably low-cost, scalable, location-independent platform.

This new model of data hosting service commence a new security challenges, which requires an independent auditing service which audit the data integrity of cloud. There are different existing auditing services available in cloud which audit data integrity remotely in static motion but these are not applicable whenever data is dynamically updated in cloud. Since it require efficient and secure dynamic auditing method for data owner. However in cloud, the clients no have direct physical possession of data. It shows client faces different formidable risk like missing or corruption of data. To keep away from the security and integrity risk of data, audit services are essential to ensure the integrity and availability of outsourced data and to achieve digital forensics and credibility on cloud computing.

Provable data possession (PDP), which is a cryptographic technique for verifying the integrity of data without retrieving it at an untrusted server, can be used to realize audit services. In this paper, profiting from the interactive proof system, we address the construction of an interactive PDP protocol to prevent the fraudulence of prove (soundness property) and the leakage of verified data (zero-knowledge property) [1] [17] [20].

Index Terms— Data integrity, Storage auditing, dynamic auditing, privacy-preserving auditing, cloud computing, zero knowledge.

I. INTRODUCTION

In recent years, the emerging cloud-computing is rapidly gaining thrust as an alternative to traditional computing system. Cloud computing provides a scalability environment for growing amounts of data and processes that work on various applications and services by means of on-demand self-services. But By seeing the popularities of cloud computing services, it's fast development and advance technologies anyone can voted it as a future of computing world. Cloud stores the information that is locally stores in the computer, it contains spreadsheets, presentations, audio, photos, word processing documents, videos, records, photos. But for sensitive and confidential data there should be some security mechanism, so as to provide protection for private data [19] [20].

Conventionally, client can verify the data integrity based on two-party storage auditing protocols [4] [5] [6]. But it is inefficient for auditing, because no one can give (i.e. client or cloud service provider) assurance to provide balance auditing.

Therefore third-party auditing (TPA) is play important role for the storage auditing in cloud computing. It is very convenient for both side i.e. owner side and cloud service provider side.

One fundamental aspect of this paradigm shifting is that data are being centralized and outsourced into clouds. This kind of outsourced storage services in clouds have become a new profit growth point by providing a comparably low-cost, scalable, location-independent platform for managing clients' data.

The cloud storage service (CSS) relieves the burden of storage management and maintenance. However, if such an important service is susceptible to attacks or failures, it would bring irretrievable losses to users since their data or archives are stored into an uncertain storage pool outside the enterprises. These security risks come from the following reasons: the cloud infrastructures are much more powerful and reliable than personal computing devices. However, they are still susceptible to security threats both from outside and inside the cloud for the benefits of their possession, there exist various motivations for cloud service providers (CSP) to behave unfaithfully toward the cloud users furthermore, the dispute occasionally suffers from the lack of trust on CSP [1].

Consequently, their behaviors may not be known by the cloud users, even if this dispute may result from the users' own improper operations. Therefore, it is necessary for cloud service providers to offer an efficient audit service to check the integrity and availability of the stored data. Traditional cryptographic technologies for data integrity and availability, based on hash functions and signature scheme, cannot work on the outsourced data without a local copy of data.

In addition, it is not a practical solution for data validation by downloading them due to the expensive transaction, especially for large-size files. Moreover, the solutions to audit the correctness of the data in a cloud environment can be formidable and expensive for the cloud users [1] [2] [3].

Therefore, it is crucial to realize public audit ability for CSS, so that data owners may resort to a third party auditor (TPA), who has expertise and capabilities that a common user does not have, for periodically auditing the outsourced data. This audit service is significantly important for digital forensics and data assurance in clouds.

II. EXISTING SYSTEM AND CHALLENGES

Ateniese et al. [7] are the first to consider public auditability in their "provable data possession" (PDP) model for ensuring possession of data files on untrusted storages. They utilize the RSA-based homomorphic linear authenticators for auditing outsourced data and suggest randomly sampling a few blocks of the file.

Manuscript received September, 2013.

Mrs. Shingare Vidya Marshal CSE department, Jagruti Institute of Engineering & Technology, Hyderabad.

However, among their two proposed schemes, the one with public auditability exposes the linear combination of sampled blocks to external auditor. When used directly, their protocol is not provably privacy preserving, and thus may leak user data information to the external auditor.

Juels et al. [9] describe a "proof of retrievability" (PoR) model, where spot-checking and error-correcting codes are used to ensure both "possession" and "retrievability" of data files on remote archive service systems. However, the number of audit challenges a user can perform is fixed a priori, and public auditability is not supported in their main scheme. The authors complete their dynamic auditing system to be privacy preserving and it support the batch auditing for multiple owners [11]. However, due to the large number of data tags, their auditing protocols will incur a heavy storage overhead on the server.

In [10], the authors proposed a dynamic auditing protocol that can support the dynamic operations of the data on the cloud servers, but this method may leak the data content to the auditor because it requires the server to send the linear combinations of data blocks to the auditor.

In Yan Zhu used [1] a quantified new audit approach based on probabilistic queries and periodic verification, as well as an optimization method of parameters of cloud audit services. This approach greatly reduces the workload on the storage servers, while still achieves the detection of servers' misbehavior with a high probability.

By referring different existing system, we have described some suggested requirements for public auditing services and the state of threat that fulfills them. However, this is still not enough for a publicly auditable secure cloud data storage system, and further challenging issues remain to be supported and resolved.

(1) What will happen if the data owner and TPA are unreliable? In this case the auditing result should identify the data correctness as well as it should be able to determine which entity is responsible for the problem like owner, TPA or cloud server. So systems accountability should be achieved.

(2) Performance is another important aspect in cloud computing data storage security and its integrity for any physical system.

(3) Cloud data storage provides dynamic and scalable storage services. It also allows easy on-demand file sharing on cloud. The challenge in this case is that legacy users, who access data and it can also modify the owner's data in the cloud. So major challenge is dynamics support for public auditing services while maintaining system runtime.

To securely launch an effective third party auditor (TPA), the following two essential requirements should be met;

1) TPA should be able to efficiently audit the cloud data storage without demanding the local copy of data, and introduce no additional on-line burden to the cloud user.
2) The third party auditing process should bring in no new vulnerabilities towards user data privacy.

Therefore our system protocol provide Confidentiality, Dynamic auditing and Batch auditing i.e. auditing protocol is able to support the batch auditing for many owners and many clouds[12][13].

III. PROPOSED SYSTEM AND IMPLEMENTATION

In this paper, we utilize the public Provable data possession (PDP), which is a cryptographic technique for verifying the integrity of data without retrieving it at an un trusted server; can be used to realize audit services. It with random mask technique to achieve a privacy-preserving public auditing system for cloud data storage security while keeping all above requirements in mind.

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 shows the proposed schemes are provably secure and highly efficient. We also show how to extent our main scheme to support batch auditing for TPA upon delegations from multi-users. We are integrating following modules in our proposed system.

Modules:

1. Audit Service System
2. Data Storage Service System
3. Audit Outsourcing Service System
4. Secure and Performance Analysis

1. Audit Service System:

In this module we provide an efficient and secure cryptographic interactive audit scheme for public audit ability. We provide an efficient and secure cryptographic interactive retains the soundness property and zero-knowledge property of proof systems. These two properties ensure that our scheme can not only prevent the deception and forgery of cloud storage providers, but also prevent the leakage of outsourced data in the process of verification.

2. Data Storage Service System:

In this module, we considered FOUR entities to store the data in secure manner:

1. Data owner (DO):
Who has a large amount of data to be stored in the cloud.
2. Cloud service provider (CSP):
Who provides data storage service and has enough storage spaces and computation resources.
3. Third party auditor (TPA):
Who has capabilities to manage or monitor – outsourced data under the delegation of data owner.
4. Granted applications (GA):
Who have the right to access and manipulate stored data. These applications can be either inside clouds or outside clouds according to the specific requirements.

3. Audit Outsourcing Service System:

In this module the client (data owner) uses the secret key to preprocess the file, which consists of a collection of blocks, generates a set of public verification information that is stored in TPA, transmits the file and some verification tags to Cloud service provider CSP, and may delete its local copy.

At a later time, using a protocol of proof of retrievability, TPA (as an audit agent of clients) issues a challenge to audit (or check) the integrity and availability of the outsourced data in terms of the public verification information.

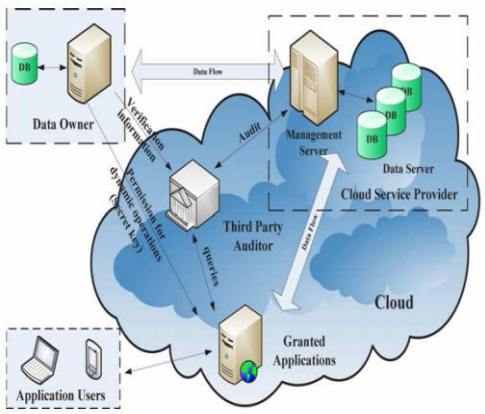
It is necessary to give an alarm for abnormal events.

4. Secure and Performance Analysis:

In this module, we considered to secure the data and give performance to the following:
Audit-without-downloading:
To allow TPA (or other clients with the help of TPA) to verify the correctness of cloud data on demand without retrieving a copy of whole data or introducing additional on-line burden to the cloud users.
Verification-correctness:
To ensure there exists no cheating CSP that can pass the audit from TPA without indeed storing users' data intact.
Privacy-preserving:
To ensure that there exists no way for TPA to derive users' data from the information collected during the auditing process.
High-performance:
To allow TPA to perform auditing with minimum overheads in storage, communication and computation, and to support statistical audit sampling and optimized audit schedule with a long enough period of time.

IV. SYSTEM ARCHITECTURE

Figure 1 shows architecture of Audit System architecture [1] for cloud computing like data storage services. At its core, the architecture consists of four different entities: data owner, user, cloud server (CS), and TPA. Here the TPA is the trusted entity that has expertise and capabilities to assess cloud storage security on behalf of a data owner upon request. Under the cloud system, the data owner may represent either the individual or the enterprise customer, who relies on the cloud server for remote data storage and maintenance, and thus is relieved of the burden of building and maintaining local storage infrastructure.
Cloud data storage services also provide benefits like availability, relative low cost i.e. paying on basis of function need, and on demand sharing among a group of trusted users. For simplicity, we assume a single writer/many readers scenario here. Only the data owner can dynamically interact with the CS to update her stored data, while users just have the privilege of file reading [1].
Considering the possibly large cost in terms of resources and expertise, the data owner may resort to a TPA for the data auditing task to ensure the storage security of her data, while hoping to keep the data private from the TPA. We assume the TPA, who is in the business of auditing, is reliable and independent, and thus has no reason to plot with either the CS or the owners during the auditing process.
The TPA should be able to efficiently audit the cloud data storage without local copy of data and without any additional online burden for data owners. Besides, any possible leakage of an owner's outsourced data toward a TPA through the auditing protocol should be prohibited [1].



Audit system architecture for cloud computing

Figure. 1

Following Use Case diagram shows all functionality of Dynamic audit service by TPA for data integrity in cloud system in which Third Party viewer verifies data as a agent of data owner.

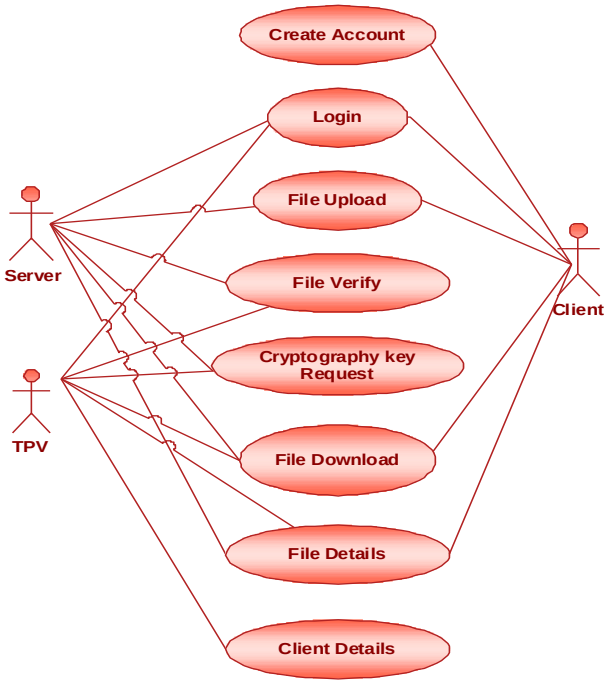


Figure 2: Use case Diagram of Secure audit service by using TPV for data integrity in cloud system

V. CONCLUSIONS

In this paper, we proposed an efficient and essentially secure dynamic auditing system. We can achieve guarantee of data integrity and availability in cloud and implement the worth system for user by using TPA. So client can trust on cloud storage service which is provided by cloud because TPA works as a representative of data owner.
It also works periodically without disturbing and imposing extra workload on cloud system by maintaining security of third party auditor. Therefore it is very easy to deploy in cloud computing environment to replace the traditional Hash-based solution.
Since we propose an effective and flexible efficient audit service outsourcing for data integrity in cloud system with precise data support dynamically.

ACKNOWLEDGMENTS

I am very thankful to the people those who have provided me continuous encouragement and support to all the stages and ideas visualize. I am very much grateful to the entire CSE department of Jagruti Institute of Engineering & Technology, Hyderabad for giving me all facilities and work environment which enable me to complete my task. I am also thankful to all researchers which I have mentioned in reference list and I regret if I forget to mention name of anybody here as well as in reference list.

REFERENCES

1. Yan Zhua,b, Hongxin Huc, Gail-Joon Ahnc, Stephen S. Yauc. "Efficient audit service outsourcing for data integrity in clouds". In "The Journal of Systems and Software 85 (2012) 1083– 1095".
2. M. Armbrust, A. Fox, R. Griffith, A.D. Joseph, R.H. Katz, A. Konwinski, G. Lee, D.A. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, "A View of Cloud Computing," Comm. ACM, vol. 53, no. 4, pp. 50-58, 2010.
3. T. Velte, A. Velte, and R. Elsenpeter, Cloud Computing: A Practical Approach, first ed., ch. 7. McGraw-Hill, 2010.
4. A. Juels and B.S. Kaliski Jr., "PORs: Proofs of Retrievability for Large Files," Proc. 14th ACM Conf. Computer and Comm. Security (CCS '07), pp. 584-597, Oct. 2007.
5. G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, "Provable Data Possession at Untrusted Stores," Proc. 14th ACM Conf. Computer and Comm. Security (CCS '07), pp. 598-609, Oct. 2007.
6. M.A. Shah, M. Baker, J.C. Mogul, and R. Swaminathan, "Auditing to Keep Online Storage Services Honest," Proc. 11th USENIX Workshop Hot Topics in Operating Systems (HotOS '07), pp. 1-6, 2007.
7. G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, "Provable Data Possession at Untrusted Stores," Proc. 14th ACM Conf. Computer and Comm. Security (CCS '07), pp. 598-609, 2007.
8. M.A. Shah, R. Swaminathan, and M. Baker, "Privacy-Preserving Audit and Extraction of Digital Contents," Cryptology ePrint Archive, Report 2008/186, 2008.
9. A. Juels and J. Burton, S. Kaliski, "PORs: Proofs of Retrievability for Large Files," Proc. ACM Conf. Computer and Comm. Security (CCS '07), pp. 584-597, Oct. 2007.
10. 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 Distributed Systems, vol. 22, no. 5, pp. 847-859, May 2011.
11. C. Wang, Q. Wang, K. Ren, and W. Lou, "Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing," Proc. IEEE INFOCOM, pp. 525-533, 2010.
12. 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, July/Aug. 2010.
13. K. Yang and X. Jia, "Data Storage Auditing Service in Cloud Computing: Challenges, Methods and Opportunities," World Wide Web, vol. 15, no. 4, pp. 409-428, 2012.
14. Q. Wang et al., "Enabling Public Verifiability and Data Dynamics for Storage Security in Cloud Computing," Proc. ESORICS '09, Sept. 2009, pp. 355–70.
15. C. Erway et al., "Dynamic Provable Data Possession," Proc. ACM CCS '09, Nov. 2009, pp. 213–222.
16. [16] C. Wang et al., "Privacy-Preserving Public Auditing for Storage Security in Cloud Computing," Proc. IEEE INFOCOM '10, Mar. 2010.
17. Cong Wang and Kui Ren, Illinois Institute of Technology Wenjing Lou, Worcester Polytechnic Institute Jin Li, Illinois Institute of Technology "Toward Publicly Auditable Secure Cloud Data Storage Services". 0890-8044/10/2010 IEEE.
18. Cong Wang, Student Member, IEEE, Qian Wang, Student Member, IEEE, Kui Ren, Senior Member, IEEE, Ning Cao, and Wenjing Lou, Senior Member, IEEE "Toward Secure and Dependable Storage Services in Cloud Computing" IEEE TRANSACTIONS ON SERVICES COMPUTING, VOL. 5, NO. 2, APRIL-JUNE 2012.
19. Kan Yang, Student Member, IEEE, and Xiaohua Jia, Fellow, IEEE "An Efficient and Secure Dynamic Auditing Protocol for Data Storage in Cloud Computing" IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 24, NO. 9, SEPTEMBER 2013.
20. Cong Wang, Member, IEEE, Sherman S.M. Chow, Qian Wang, Member, IEEE, Kui Ren, Senior Member, IEEE, and Wenjing Lou, Senior Member, IEEE "Privacy-Preserving Public Auditing for Secure Cloud Storage" IEEE TRANSACTIONS ON COMPUTERS, VOL. 62, NO. 2, FEBRUARY 2013.

AUTHORS PROFILE

Mrs. Shingare Vidya Marshal, CSE department, Jagruti Institute of Engineering & Technology, Hyderabad Pursuing M.Tech Computer Engineering from Jagruti Institute of Engineering & Technology, Hyderabad.