ISSN: 2278 – 1323
International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)
Volume 2 Issue 8, August 2013

DYNAMIC AUDIT SERVICE OUTSOURCING FOR DATA INTEGRITY IN CLOUDS

CH. MUTYALANNA[1], P. SRINIVASULU[2], M. KIRAN[3]

1, M.TECH Scholar, VEC, Kavali
2, Associate Professor, VEC, Kavali
3, Assistant Professor, JCET

ABSTRACT:

Cloud-based outsourced storage relieves the client's load for storage management and preservation by providing an equivalently scalable, low-cost, location-independent platform. Clients no longer have physical control of data indicates that they are facing a potentially frightening risk for missing or corrupted data. To keep away from the security risks, audit services are significant to make sure that the integrity and availability of outsourced data. 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 recognize audit services. In this we introduced the construction of an well-organized audit service for data integrity in clouds. Profiting from the typical interactive verification system, we projected an interactive audit procedure to implement the audit service based on a third party auditor. In this audit examination, the third party auditor can concern a periodic authentication to check the change of outsourced data by providing an optimized to-do list. To understand the audit model, we only need to preserve the security of the third party auditor and organize an insubstantial daemon to execute the verification protocol. We present an capable method for selecting an optimal parameter value to minimize computational expenditure of cloud audit services. Our results demonstrate the effectiveness of our approach.

Index Terms— ***Security, Interactive proof system, Cloud storage, Provable data possession, Audit service***

1. INTRODUCTION

In present days, the up-and-coming cloud-computing model is rapidly in advance force as an unconventional to traditional information technology. Cloud computing make available a scalability environment for emergent amounts of data and processes that work on a variety of services and applications by means of on-demand self-services. One fundamental aspect of this model shifting is that data are being centralized and outsourced into clouds. This category of outsourced storage space services in clouds have turn out to be a new profit growth point by given that a comparably low-cost, scalable, location-independent policy for managing clients' data.

Fig.1: Cloud Storage Structure

The cloud storage service (CSS) mitigates the load of maintenance and storage management. However, if such a significant service is weak to attacks or failures, it would take permanent losses to users since their data or records are stored into an unsure storage space pool outside the enterprises. These security risks move about in the direction of from the following reasons: the cloud infrastructures are much more authoritative and reliable than personal computing devices. If they are still susceptible to security threats both from inside and outside the cloud for the benefits of their control, there exist various motivations for cloud service providers (CSP) to behave falsely toward the cloud users in addition, the dispute infrequently suffers from the lack of trust on cloud service provider. As a result, their behaviors may not be known by the cloud users. Therefore, it is necessary for cloud service providers to offer a scalable audit service to check the integrity and accessibility of the stored data. While Cloud Computing makes these advantages more appealing than ever, it also brings new challenging security threats towards users' outsourced data. Since cloud service provider is separate administrative units, data outsourcing is actually resigning user's control over the destiny of their data. The correctness of the data in the cloud is being put at risk due to the subsequent reasons. First of all, although the infrastructures beneath the cloud are much more powerful and reliable than private computing devices, they are silent facing the broad range of both internal and external threats for data integrity.

Traditional cryptographic technologies for data integrity and accessibility, based hash functions and on signature schemes cannot work on the outsourced data lacking a local copy of data. In accumulation, it is not a realistic solution for data validation by downloading them due to the exclusive 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. Therefore, it is critical to recognize public audit ability for Cloud Storage Service, so that data owners may remedy to a third party auditor (TPA), who has proficiency and capabilities that a common user does not have, for from time to time auditing the outsourced data. This audit service is extensively significant for digital forensics and data assurance in clouds.

2. AUDIT SYSTEM ARCHITECTURE

The audit system architecture for outsourced data in clouds in which can work in an audit service outsourcing approach. In this architecture, we reflect on a data storage service containing four entities:

1) Data owner (DO): who has data files to be stored in the cloud and relies on the cloud for data maintenance, can be an individual customer or an organization.

2) Cloud Storage Service Provider (CSP): who provides data storage service and has enough storage space to maintain client's data.

3) Third Party Auditor (TPA): a trusted person who manage or monitor outsourced data under request of the data owner.

4) Authorized Application (AA): who have the right to access and manipulate stored data.

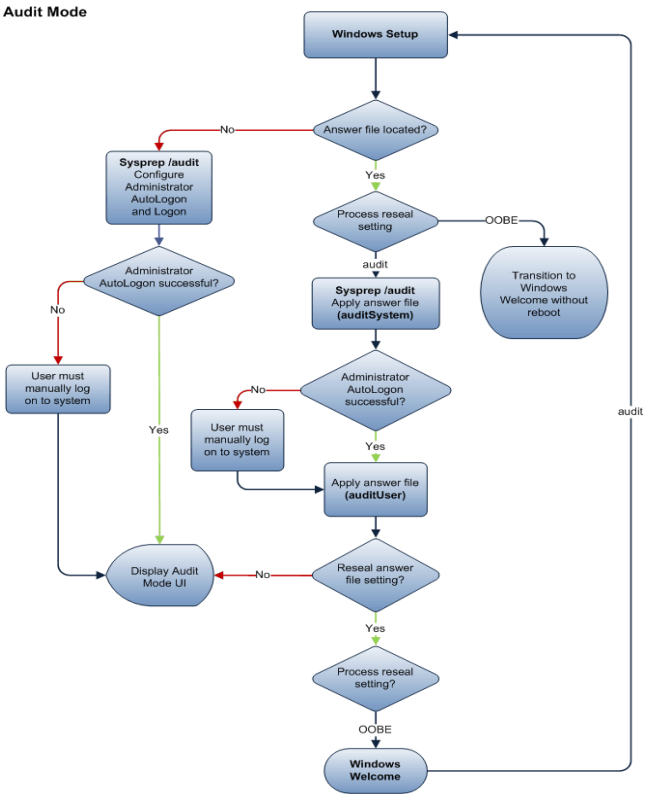

Fig.2: Flow chart for Audit service

The data which the data owner wants to store in cloud first reaches the authorized application which will create digital signature and sends the data to the cloud storage. If the user needs to verify data means the verification request should be send to third party auditor (TPA), the TPA will retrieve the digital signature from the database and will send the verification request to the management server. The management server in turn will generate the digital signature for the data stored in the cloud and it will send only that digital signature instead of the whole data to the TPA. The TPA will decrypt the digital signature and compares the message digest for verifying correctness of data.

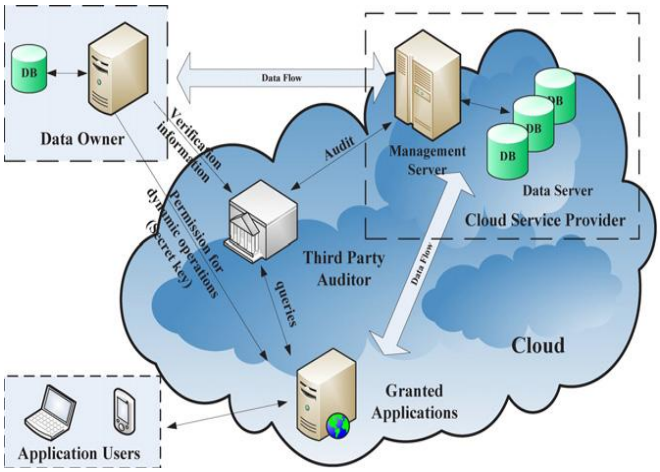

Fig.3: Audit System Architecture

This architecture is known as the audit service outsourcing due to data integrity authentication can be implemented by Third Party Auditor without help of data owner. Architecture contains the data owner and granted clients need to dynamically interact with cloud service provider to access or update their data for various application purposes. However, we neither assume that cloud service provider is trust to guarantee the security of stored data, or suppose that the data owner has the capability to collect the verifications of cloud service provider's fault after errors occur. Hence, third party auditor, as a trust third party (TTP), is used to ensure the storage security of their outsourced data. We assume the third party auditor is reliable and independent, and thus has no encouragement to join together with either the cloud service provider or the clients during the auditing process:

• TPA must be able to make regular check on the integrity and availability of these delegated data at appropriate intervals;

• TPA must be able to take the evidences for the disputes about the inconsistency of data in terms of authentic records for all data operations.

To facilitate privacy-preserving public auditing for cloud data storage beneath the architecture, the protocol design should attain subsequent security and performance guarantees:

1) Audit-without-downloading: to allow TPA (or other clients with the help of TPA) to authenticate the correctness of cloud data on demand without recovering a copy of whole data or bring in additional on-line burden to the cloud users;
2) Verification-correctness: to make sure there exists no unethical CSP that can pass the audit from TPA without indeed storing users' data intact;
3) Privacy-preserving: to make sure that there exists no way for TPA to derive users' data from the in sequence collected during the auditing process;
4) High-performance: to allow TPA to perform auditing with minimum overheads in storage, communication and computation, and to maintain statistical audit sampling and optimized audit schedule with a long enough period of time.

The above processes involve some procedures: TagGen, KeyGen, Update, Insert, Delete, algorithms as well as an interactive proof protocol of retrievability. In order to improve security and performance, we make use of following techniques to construct corresponding algorithms and protocols.

3. CONSTRUCTION OF INTERACTIVE AUDIT SCHEME

In this section, we propose a cryptographic interactive audit scheme to support our audit system in clouds. This scheme is constructed on the standard model of interactive proof system, which can ensure the confidentiality of secret data (zero-knowledge property) and un decidability of invalid tags (soundness property).

KeyGen(1^κ)**:** Let $\mathbb{S} = (p, \mathbb{G}, \mathbb{G}_T, e)$ be a bilinear map group system with randomly selected generators $g, h \in_R \mathbb{G}$, where $\mathbb{G}$, $\mathbb{G}_T$ are two group of large prime order p, $|p| = O(\kappa)$. Generate a collision-resistant hash function $H_k(\cdot)$ and chooses a random $\alpha, \beta \in_R \mathbb{Z}_p$ and computes $H_1 = h^\alpha$ and $H_2 = h^\beta \in \mathbb{G}$. Thus, the secret key is $sk = (\alpha, \beta)$ and the public key is $pk = (g, h, H_1, H_2)$.

TagGen(sk, F)**:** Splits the file F into $n \times s$ sectors $F = \{m_{i,j}\} \in \mathbb{Z}_p^{n \times s}$. Chooses s random $\tau_1, \cdots, \tau_s \in \mathbb{Z}_p$ as the secret of this file and computes $u_i = g^{\tau_i} \in \mathbb{G}$ for $i \in [1, s]$ and $\xi^{(1)} = H_\xi(\text{“}Fn\text{”})$, where $\xi = \sum_{i=1}^{s} \tau_i$ and Fn is the file name. Builds an index table $\chi = \{\chi_i\}_{i=1}^{n}$, then calculates its tag as

$$\sigma_i \leftarrow (\xi_i^{(2)})^\alpha \cdot g^{\sum_{j=1}^{s} \tau_j \cdot m_{i,j} \cdot \beta} \in \mathbb{G}.$$

where $\xi_i^{(2)} = H_{\xi^{(1)}}(\chi_i)$ and $i \in [1, n]$. Finally, sets $u = (\xi^{(1)}, u_1, \cdots, u_s)$ and outputs $\zeta = (\tau_1, \cdots, \tau_s)$, $\psi = (u, \chi)$ to TTP, and $\sigma = (\sigma_1, \cdots, \sigma_n)$ to CSP.

Proof(CSP, TPA)**:** This is a 3-move protocol between CSP and TPA with the common input (pk, ψ), as follows:

- **Commitment**$(CSP \rightarrow TPA)$: CSP chooses a random $\gamma \in \mathbb{Z}_p$ and s random $\lambda_j \in_R \mathbb{Z}_p$ for $j \in [1, s]$, and sends its commitment $C = (H_1', \pi)$ to TPA, where $H_1' = H_1^\gamma$ and $\pi \leftarrow e(\prod_{j=1}^{s} u_j^{\lambda_j}, H_2)$;
- **Challenge**$(CSP \leftarrow TPA)$: TPA chooses a random challenge set I of t indexes along with t random coefficients $v_i \in \mathbb{Z}_p$. Let Q be the set $\{(i, v_i)\}_{i \in I}$ of challenge index coefficient pairs. TPA sends Q to CSP;
- **Response**$(CSP \rightarrow TPA)$: CSP calculates the response θ, μ as

$$\begin{cases} \sigma' \leftarrow \prod_{(i,v_i) \in Q} \sigma_i^{\gamma \cdot v_i}, \\ \mu_j \leftarrow \lambda_j + \gamma \cdot \sum_{(i,v_i) \in Q} v_i \cdot m_{i,j}, \end{cases}$$

where $\mu = \{\mu_j\}_{j \in [1,s]}$. P sends $\theta = (\sigma', \mu)$ to V;

Verification: TPA can check that the response was correctly formed by checking that

$$\pi \cdot e(\sigma', h) \stackrel{?}{=} e(\prod_{(i,v_i) \in Q} (\xi_i^{(2)})^{v_i}, H_1') \cdot e(\prod_{j=1}^{s} u_j^{\mu_j}, H_2).$$

Fig.4: Interactive Audit Protocol

4. IMPLEMENTATION AND RESULTS

To authorize the effectiveness of our approach, we have implemented a prototype of an audit system based on our proposed solution. This system have been developed in an experimental cloud computing system environment, which is constructed within the framework of the IaaS to provide powerful virtualization, distributed storage, and automated management.

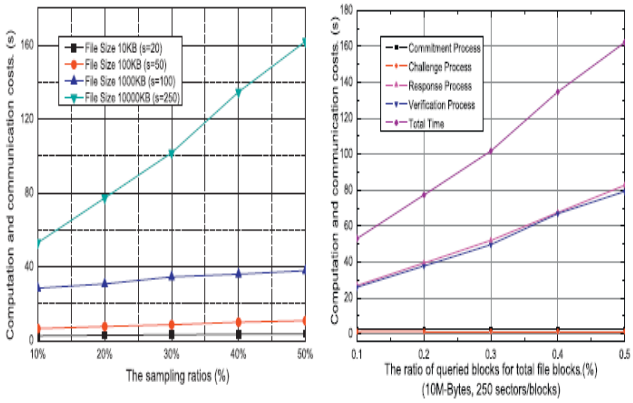

Fig.5: Experiment results under different file size, sampling ratio, and sector number.

5. CONCLUSION

Cloud Computing releases the world of computing to a wider range of uses and increases the ease of usage by giving access through any kind of internet connection. Though with these increased ease of usage also come drawbacks. Privacy security is a key issue for cloud storage and is to be considered very important. To ensure that the risks of privacy have been mitigated a variety of techniques that may be used in order to achieve privacy. This paper has addressed some privacy approaches for overcoming the issues in privacy on un trusted data stores in cloud computing. Categories the methodologies in the literature as encryption based methods, access control based mechanisms, query integrity/ keyword search schemes, and audit ability schemes. The work is giving an efficient privacy-preserving storage compared to other works. Even though there are many approaches in the literature for mitigating the concerns in privacy, no

approach is fully sophisticated to give a privacy-preserving storage that overcomes all the other privacy concerns. Thus to deal with the concerns of privacy, we need to develop privacy–preserving framework that overcomes the worries in privacy security and encourage users to adopt cloud storage services more confidently.

6. REFERENCES

[1] Yan Zhu, Hongxin Hue, Gail-Joon Ahn, Stephen S. Yau, "Efficient audit service outsourcing for data integrity in clouds", Elsevier Journal Of Systems and Software, vol.85, pp.1083-1095, 2012.

[2] Bhagyaraj Gowrigolla, Sathyalakshmi Sivaji, M. Roberts Masillamani "Design and Auditing of Cloud Computing Security", IEEE International Conference on Information and Automation for Sustainability, 2010.

[3] Cong Wang and Kui Ren, Wenjing Lou, Jin Li "Toward Publicly Auditable Secure Cloud Data Storage Services", IEEE International Journal On Networks, 2010.

[4] Cloud Security Alliance, "Top Threats to cloud computing",http://www.cloud securityalliance. org., 2010.

[5] Q. Wang, C.Wang, K. Ren, W.Lou and J.Li, "Enabling public auditability and data dynamics for storage security in cloud computing", IEEE Transactions on Parallel and Distributed Systems, vol. 22, no.5, pp.847-459, 2011.

[6] G. Ateniese, R. Burns, R. Curtola, J. Herring, L.Kisser and D. Song, "Provable data possession at untrusted stores", in Proc. Of CCS'07, pp.598-609.

[7] Daniel J. Abadi "Data Management in the Cloud: Limitations and Opportunities**",** IEEE International Conference on Data Engineering, 2009.

[8] Jianfeng Yang & Zhibin Chen, "Cloud Computing Research and Security Issues", IEEE International Conference on Computational Intelligence & Software Engineering, 2010.

[9] Ling Li, Lin Xu, Jing Li and Changchun Zhang **"**Study on the Thirdparty Audit in Cloud Storage Service**"** IEEE International Conference on Cloud & Service Computing, 2011.

[10] Giuseppe Ateniese, Randal Burns, Reza Curtmola, Joseph Herring, Lea Kissner, Zachary Peterson "Provable Data Possession at untrusted stores", in the ACM, 2007

[11] B. Priyadharshini, P. Parvathi "Data Integrity in Cloud Storage", IEEE International Conference On Advances In Engineering, Science And Management, 2012.