Volume 2, Issue 12, December-2015, pp. 1212-1216 ISSN (O): 2349-7084

International Journal of Computer Engineering In Research

Available online at: www.ijcert.org

Enable Batch Auditing for Secure Cloud Storage Using TPA

[1] PRATHIBHA MAGULURI , [2] B.RANJITHKUMAR

[1] *M.Tech (CSE), Priyadarshini Institute of Technology & Science for women's*

[2] *Associate Professor (Dept.of CSE), Priyadarshini Institute of Technology & Science for women's*

Abstract— In this paper we used cloud storage servers remotely in order to store and share the data and enjoy the on-demand high-quality applications and services from a shared pool of configurable computing resources, without communication challenges However, the fact that users no longer have physical control over outsourcing data in this connection data integrity over public cloud is a challenging task, thus this integrity will audited by trusted third party behalf of cloud without reviling any user privacy and also TPA executes multiple task simultaneously i.e batch auditing our proposed framework provides high security and high performance.

Keywords:

I.INTRODUCTION

In The cloud computing has rapidly grown in recent years due to the advantages of greater flexibility and availability of computing resources at lower cost. Security and privacy, however, are a concern for agencies and organizations considering migrating applications to public cloud computing environments. Cloud Computing has been envisioned as the next generation architecture of IT enterprise, due to its long list of unprecedented advantages in the IT history: on-demand self-service, ubiquitous network access, location independent resource pooling, rapid resource elasticity, usage-based pricing and transference of risk [1]. As a disruptive technology with profound implications, Cloud Computing is transforming the very nature of how businesses use information technology. One fundamental aspect of this paradigm shifting is that data is being centralized or outsourced into the Cloud. The Cloud Computing makes these advantages more appealing than ever, it also brings new and challenging security threats towards users' outsourced data. Since cloud service providers (CSP) are separate administrative entities, data outsourcing is actually relinquishing user's ultimate control over the fate of their data. As a result, the correctness of the data in the cloud is being put at risk due to the following reasons. First of all, although the infrastructures under the cloud are much more powerful and reliable than personal computing devices, they are still facing the broad range of both internal and external threats for data integrity.

II. PROBLEM STATEMENT

The Cloud and Threat Model the Cloud security responsibilities can be taken on by the customer, if he is managing the cloud, but in the case of a public cloud, such responsibilities are more on the cloud provider and the customer can just try to assess if the cloud provider is able to provide security. Cloud data storage service involving three different entities. the cloud user (U), who has large amount of data files to be stored in the cloud; the cloud server (CS), which is managed by cloud service provider (CSP) to provide data storage service and has significant storage space and computation resources (we will not differentiate CS and CSP hereafter.); the third party auditor (TPA), who has expertise and capabilities that cloud users do not have and is trusted to assess the cloud storage service security on behalf of the user upon request. Cloud users dynamically interact with the CS to access and update their stored data for various application purposes. The traditional cryptographic technologies for data integrity and availability, cannot work on the outsourced data without a local copy of data. it is not a practical solution for data validation by downloading them due to the expensive communications, especially for large size files. The ability to

audit the correctness of the data in a cloud environment can be formidable and expensive for the cloud users. 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 credibility in clouds. The users may resort to TPA for ensuring the storage security of their outsourced data, while hoping to keep their data private from TPA. We consider the existence of a semi-trusted CS as [11] does. Namely, in most of time it behaves properly and does not deviate from the prescribed protocol execution. However, during providing the cloud data storage based services, for their own benefits the CS might neglect to keep or deliberately delete rarely accessed data files which belong to ordinary cloud users. Moreover, the CS may decide to hide the data corruptions caused by server hacks or Byzantine failures to maintain reputation. We assume the TPA, who is in the business of auditing, is reliable and independent, and thus has no incentive to collude with either the CS or the users during the auditing process. TPA should be able to efficiently audit the cloud data storage without local copy of data and without bringing in additional on-line burden to cloud users. However, any possible leakage of user's outsourced data towards TPA through the auditing protocol should be prohibited. the audit delegation and authorize CS to respond to TPA's audits, the user can sign a certificate granting audit rights to the TPA's public key, and all audits from the TPA are authenticated against such a certificate. Design Goals The privacy-preserving public auditing for cloud data storage under the aforementioned model, our protocol design should follow the security and performance. Public Audit: It allows TPA to verify the correctness of the cloud data on demand without retrieving a copy of the whole data. Storage Consistency: the data in cloud server 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 content from the information collected during the auditing process. Batch Auditing: It enable TPA with secure and efficient auditing capability to cope with multiple auditing delegations from possibly large number of different users simultaneously. Light Weight: It allow TPA to perform auditing with minimum communication and computation overhead.

III.SYSTEM STUDY

EXISTING SYSTEM:

In the Existing systems, the notion of public auditability has been proposed in the context of ensuring remotely stored data integrity under different system and security models. Public auditability allows an external party, in addition to the user himself, to verify the correctness of remotely stored data. However, most of these schemes do not consider the privacy protection of users' data against external auditors. Indeed, they may potentially reveal user's data to auditors. This severe drawback greatly affects the security of these protocols in cloud computing. From the perspective of protecting data privacy, the users, who own the data and rely on TPA just for the storage security of their data, do not want this auditing process introducing new vulnerabilities of unauthorized information leakage toward their data security.

DISADVANTAGES OF EXISTING SYSTEM:

- Although the infrastructures under the cloud are much more powerful and reliable than personal computing devices, they are still facing the broad range of both internal and external threats for data integrity.
- Second, there do exist various motivations for CSP to behave unfaithfully toward the cloud users regarding their outsourced data status.
- In particular, simply downloading all the data for its integrity verification is not a practical solution due to the expensiveness in I/O and transmission cost across the network. Besides, it is often insufficient to detect the data corruption only when accessing the data, as it does not give users correctness assurance for those unaccessed data and might be too late to recover the data loss or damage.
- Encryption does not completely solve the problem of protecting data privacy against third-party auditing but just reduces it to the complex key management domain. Unauthorized data leakage still remains possible due to the potential exposure of decryption keys.

PROPOSED SYSTEM:

In this paper, we utilize the public key based homomorphic authenticator and uniquely integrate 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 multi-user 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.

ADVANTAGES OF PROPOSED SYSTEM:

- **Public auditability:** to allow TPA to verify the correctness of the cloud data on demand without retrieving a copy of the whole data or introducing additional online burden to the cloud users.

- **Storage correctness:** to ensure that there exists no cheating cloud server that can pass the TPA's audit without indeed storing users' data intact.
- **Privacy preserving:** to ensure that the TPA cannot derive users' data content from the information collected during the auditing process.
- **Batch auditing:** to enable TPA with secure and efficient auditing capability to cope with multiple auditing delegations from possibly large number of different users simultaneously
- **Lightweight:** to allow TPA to perform auditing with minimum communication and computation overhead.

IV.ALGORITHMS USED:

The Privacy-Preserving Public Auditing Protocol

TPA		Cloud Server
1. Retrieve file tag t, verify its signature, and quit if fail;		
2. Generate a random challenge $chal = \{(i, \nu_i)\}_{i \in I}$;	$\xrightarrow{\{(i,\nu_i)\}_{i\in I}}$ challenge request $chal$	3. Compute $\mu' = \sum_{i \in I} \nu_i m_i$, and $\sigma = \prod_{i \in I} \sigma_i^{\nu_i}$; 4. Randomly pick $r \leftarrow \mathbb{Z}_p$, and $R = e(u, v)^r$ and $\gamma = h(R)$;
	$\xleftarrow{\{\mu,\sigma,R\}}$ storage correctness proof	5. Compute $\mu = r + \gamma\mu' \mod p$;
6. Compute $\gamma = h(R)$, and then verify $\{\mu, \sigma, R\}$ via Equation 1.		

The Batch Auditing Protocol

TPA		Cloud Server
1. Verify file tag t_k for each user k, and quit if fail;		For each user k ($1 \le k \le K$):
2. Generate a random challenge $chal = \{(i, \nu_i)\}_{i \in I}$;	$\xrightarrow{\{(i,\nu_i)\}_{i\in I}}$ challenge request $chal$	3. Compute μ'_k, σ_k, R_k as single user case; 4. Compute $\mathcal{R} = R_1 \cdot R_2 \cdots R_K$, $\mathcal{L} = vk_1 \| vk_2 \| \cdots \| vk_K$ and $\gamma_k = h(\mathcal{R} \| v_k \| \mathcal{L})$;
	$\xleftarrow{\{\{\sigma_k,\mu_k\}_{1\le k\le K},\mathcal{R}\}}$ storage correctness proof	5. Compute $\mu_k = r_k + \gamma_k \mu'_k \mod p$;
6. Compute $\gamma_k = h(\mathcal{R} \| v_k \| \mathcal{L})$ for each user k and do batch auditing via Equation 3.		

V.SYSTEM STRCTURE

1. Third Party Auditor
2. Cryptography
3. Cloud Computing
4. Privacy-preserving

1. Third Party Auditor

In this module, Auditor views the all user data and verifying data .Auditor directly views all user data without key. Admin provided the permission to Auditor. After auditing data, store to the cloud.

2. Cryptography

The art of protecting information by transforming it (*encrypting* it) into an unreadable format, called cipher text. Only those who possess a secret *key* can decipher (or *decrypt*) the message into plain text. Encrypted messages can sometimes be broken by cryptanalysis, also called *code breaking*, although modern cryptography techniques are virtually unbreakable.

3. Cloud Computing

Cloud computing is the provision of dynamically scalable and often virtualized resources as a services over the internet Users need not have knowledge of, expertise in, or control over the technology infrastructure in the "cloud" that supports them. Cloud computing represents a major change in how we store information and run applications. Instead of hosting apps and data on an individual desktop computer, everything is hosted in the "cloud"—an assemblage of computers and servers accessed via the Internet.

4. Privacy-preserving

To ensure that the TPA cannot derive users' data content from the information Collected during the auditing process.

Cloud computing exhibits the following key characteristics:

1. Agility improves with users' ability to re-provision technological infrastructure resources.

2. Multi tenancy enables sharing of resources and costs across a large pool of users thus allowing for:

3. Utilization and efficiency improvements for systems that are often only 10–20% utilized.

4. Reliability is improved if multiple redundant sites are used, which makes well-designed cloud computing suitable for business continuity and disaster recovery.

5. Performance is monitored and consistent and loosely coupled architectures are constructed using web services as the system interface.

6. Security could improve due to centralization of data, increased security-focused resources, etc., but concerns can persist about loss of control over certain sensitive data, and the lack of security for stored kernels. Security is often as good as or better than other traditional systems, in part because providers are able to devote resources to solving security issues that many customers cannot afford. However, the complexity of security is greatly increased when data is distributed over a wider area or greater number of devices and in multi-tenant systems that are being shared by unrelated users. In addition, user access to security audit logs may be difficult or impossible. Private cloud installations are in part motivated by users' desire to retain control over the infrastructure and avoid losing control of information security.

7. Maintenance of cloud computing applications is easier, because they do not need to be installed on each user's computer and can be accessed from different places.

Architecture of Cloud Computing:

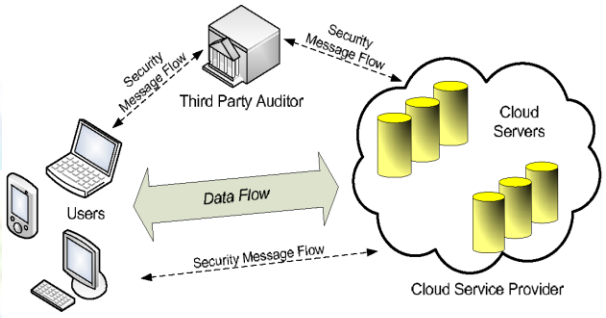

Fig. 1: The architecture of cloud data storage service

To enable privacy-preserving public auditing for cloud data storage under the aforementioned model, our protocol design should achieve the following security and performance guarantee:

VI.PRIVACY-PRESERVING PUBLIC AUDITING MODULE:

Homomorphic authenticators are unforgeable verification metadata generated from individual data blocks, which can be securely aggregated in such a way to assure an auditor that a linear combination of data blocks is correctly computed by verifying only the aggregated authenticator. Overview to achieve privacy-preserving public auditing, we propose to uniquely integrate the homomorphic authenticator with random mask technique. In our protocol, the linear combination of sampled blocks in the server's response is masked with randomness generated by a pseudo random function (PRF). The proposed scheme is as follows:

- Setup Phase
- Audit Phase

Batch Auditing Module:

With the establishment of privacy-preserving public auditing in Cloud Computing, TPA may concurrently handle multiple auditing delegations upon different users' requests. The individual auditing of these tasks for TPA can be tedious and very inefficient. Batch auditing not only allows TPA to perform the multiple auditing tasks simultaneously, but also greatly reduces the computation cost on the TPA side.

Data Dynamics Module:

Hence, supporting data dynamics for privacy-preserving public risk auditing is also of paramount importance. Now we show how our main scheme can be adapted to build upon the existing work to support data dynamics, including block level operations of modification, deletion and insertion. We can adopt this technique in our design to achieve privacy-preserving public risk auditing with support of data dynamics.

VII.CONCLUSION

We propose a privacy-preserving public auditing framework for information storage security in Cloud Computing. We use the homomorphic straight authenticator and irregular covering to ensure that the TPA would not realize any learning about the information content put away on the cloud server amid the effective auditing process, which not just disposes of the weight of cloud client from the repetitive and perhaps costly auditing errand, additionally reduces the clients' trepidation of their outsourced information spillage. Considering TPA might simultaneously handle numerous review sessions from various clients for their outsourced information documents, we assist expand our privacy-preserving public auditing convention into a multi-client setting, where the TPA can perform different auditing assignments in a cluster way for better proficiency. Broad examination demonstrates that our plans are provably secure and exceedingly productive.

REFERENCES:

[1] R. Buyya, C.S. Yeo, S. Venugopal, J. Broberg, and I. Brandic, ''Cloud Computing and Emerging IT Platforms: Vision, Hype, Reality for Delivering Computing as the 5th Utility,'' Future Gen. Comput. Syst., vol. 25, no. 6, pp. 599-616, June 2009.
[2]M.Armbrust,A.Fox,R.Griffith,A.D.Jose ph,R.Katz,A.Konwinski,G.Lee,D.Patterso n,A.Rabkin,I.Stoica,andM.Zaharia,''AVie wof Cloud Computing,'' Commun. ACM, vol. 53, no. 4, pp. 50-58, Apr. 2010.
[3] Customer Presentations on Amazon Summit Australia, Sydney, 2012, accessed on: March 25, 2013. [Online]. Available: http:// aws.amazon.com/apac/awssummitau/.

[4] J. Yao, S. Chen, S. Nepal, D. Levy, and J. Zic, ''TrustStore: Making Amazon S3 Trustworthy With Services Composition,'' in Proc. 10th IEEE/ACM Int'l Symposium on Cluster, Cloud and Grid Computing (CCGRID), 2010, pp. 600-605.
[5] D. Zissis and D. Lekkas, ''Addressing Cloud Computing Secu- rity Issues,'' Future Gen. Comput. Syst., vol. 28, no. 3, pp. 583-592, Mar. 2011.
[6] 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 Distrib. Syst., vol. 22, no. 5, pp. 847-859, May 2011.
[7] C. Wang, Q. Wang, K. Ren, and W. Lou, ''Privacy-Preserving Public Auditing for Data Storage Security in Cloud INTERNATIONAL JOURNAL OF AD-VANCE RESEARCH, IJOAR .ORG ISSN 2320-9194 12 IJOAR© 2015 http://www.ijoar.org Computing,'' in Proc. 30st IEEE Conf. on Comput. and Commun. (IN-FOCOM), 2010, pp. 1-9.
[8] G. Ateniese, R.D. Pietro, L.V. Mancini, and G. Tsudik, ''Scalable and Efficient Provable Data Possession,'' in Proc. 4th Int'l Conf. Security and Privacy in Commun. Netw. (SecureComm), 2008, pp. 1-10.
[9] G. Ateniese, R. Burns, R. Curtmola, J. Herring, O. Khan, L. Kissner, Z. Peterson, and D. Song, ''Remote Data Checking Using Provable Data Possession,'' ACM Trans. Inf. Syst. Security, vol. 14, no. 1, May 2011, Article 12.
[10]G.Ateniese,R.B.Johns, R.Curtmola,J.Herring,L.Kissner, Z.Peterson, and D. Song, ''Provable Data Possession at Untrusted Stores,'' in Proc. 14th ACM Conf. on Comput. and Commun. Security (CCS), 2007, pp. 598- 609.

