ENABLING PUBLIC AUDIT ABILITY AND DATA DYNAMICS FOR STORAGE SECURITY IN CLOUD COMPUTING

T. Sumadhi, M. Hemalatha

ABSTRACT

Cloud computing is the delivery of computing as a service to the user rather than a product, where the shared resources, software and information are provided to computer and other devices as a utility over a network. Cloud computing is internet based computing whereby shared server provides resources, software and data to computers and other devices on demand, as with the electricity grid. The application software and databases are transferred to the centralized large data centers, in which management of the data and services may not be fully reliable or trustworthy. This unique paradigm brings about many new security challenges, which have not been well understood. These problems lead us to secure the data storage and data dynamics operation in cloud server. The cloud server checks correctness of the data in cloud server by using TPA (Third Party Auditor), this level authentication provides integrity checking on storage data. This paper achieves both public audit ability and dynamic operation by increasing the efficiency of data dynamics. The proposed method also improves the existing proof of storage models and block tag authentication.

Keywords: Cloud computing, Third party auditor, Data dynamics, Public audit ability.

I. INTRODUCTION

Cloud Computing has been envisioned as the next-generation architecture of IT Enterprise. The organization can upload the application software and databases in to the centralized large data centers, where the supervision of the data and services may not be fully reliable. This unique pattern brings about many new security challenges that has to be well analyzed. This paper deals with the problem of ensuring the integrity of data storage in Cloud Computing. In particular, the task of allowing a third party auditor (TPA) on behalf of the cloud client verifies the integrity of the dynamic data stored in the cloud. The Usage of TPA eliminates the participation of the client by auditing whether the data stored in the cloud are indeed intact, this process is important in achieving economies of scale in Cloud Computing. The services in Cloud Computing are not limited to archive or backup data only, the usage of data dynamics through the most general forms of data operation, like block modification, insertion, and deletion is also an important step toward practicality. The existing works focuses on ensuring remote data integrity but often lacks the support of either public audit ability or dynamic data operations. This paper achieves both the functionalities. 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

[1]Research Scholar, Lecturer, Department of Software systems, Karpagam University, Coimbatore-21
[2]Research Scholar, Head, department of software systems, Karpagam University, Coimbatore-21

for the seamless integration of these two salient features in our protocol design. To achieve efficient data dynamics, improvement has been made in the existing proof of storage models by manipulating the classic Merkle Hash Tree construction for block tag authentication. The technique of bilinear aggregate signature has been used for efficient handling of multiple auditing tasks, where TPA can perform multiple auditing tasks simultaneously. Performance analysis and extensive security mechanism show that the proposed method is highly efficient and provably secure. The overall architecture of our proposed methodology has been illustrated in figure.1.

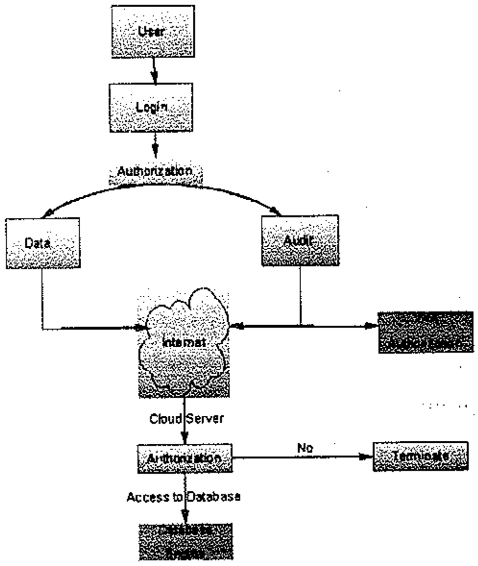


Figure 1: The overall architecture of proposed methodology

I. Drawbacks in the existing methods

1) Non-trust worthiness of the cloud provider.

2) Data may be hacked.

3) Database may get corrupted.

II. Related work

Ateniese et al. [2] [17] are the first to consider public auditability in their defined "provable data possession" (PDP) model for ensuring possession of data files on unreliable storages. Their method makes use of the RSA based Homomorphic linear authenticators for auditing outsourced data and suggests randomly sampling a few blocks of the file. But, the public auditability in their scheme demands the linear combination of sampled blocks exposed to external auditor. When their protocol is used directly, it is not provably privacy preserving, and leaks out user data information to the auditor [1].

Juels et al. [5] describe a "proof of retrievability" (PoR) model, In which they adopted the principles of 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 carry out is fixed a priori, and public auditability is not supported in their main method. Even though they depict a straightforward Merkle-tree [16] construction for public PoRs, this approach only works with encrypted data.

Dodis et.al. [18] gives a study on different variants of PoR with private auditability. Shacham et al. [7] design an improved PoR scheme built from BLS signatures [11] with full proofs of security in the security model defined in [5]. Similar to the construction in [2] [17], they use publicly verifiable homomorphism linear authenticators that are built from provably secure BLS signatures.

Based on the elegant BLS construction, public and a compact verifiable scheme are obtained. But, their approach does not support privacy-preserving auditing for the same reason as [2] [17]. Shah et al. [3], [8] propose allowing a TPA to keep online storage honest by first encrypting the data then sending a number of pre-computed symmetric-keyed hashes over the encrypted data to the auditor. The auditor checks both the integrity of the data file and the server's possession of a previously committed decryption key [9]. This scheme only works for encrypted files and it suffers from the auditor statefulness and bounded usage, which may potentially bring in online trouble to users when the keyed hashes are used up.

In other related work, Ateniese et al. [13] suggested a partially dynamic version of the prior PDP scheme, using only symmetric key cryptography, however, with a bounded number of audits.

In [14] [10], Wang et al. consider a similar support for partial dynamic data storage in a distributed scenario with additional feature of data error localization. In a subsequent work, Wang et al. [4] [10] put forward to combine BLS-based HLA with MHT to support both public auditability and full data dynamics.

Almost simultaneously, Erway et al. [15] proposed a skip lists based scheme to facilitate provable data possession with full dynamics support. However, the authentication in these two protocols requires the linear combination of sampled blocks just as [2], [7], [17], and thus does not support privacy preserving auditing. While all the above schemes provide methods for efficient auditing and provable assurance on the correctness of remotely stored data, none of them meet all the requirements for privacy preserving public auditing in cloud computing. More prominently, none of these methods consider batch auditing that can greatly decrease the computation cost on the TPA when coping with a large number of audit delegations.

III. Proposed methodology

The vital role of public audit ability and data dynamics for cloud data storage has been suggested through the efficient construction by using seamless integration of components in the protocol design. The contribution made in this paper can be summarized as follows:

1. To motivate the public auditing system for data storage security in Cloud Computing, and propose a new protocol for supporting fully dynamic data operations, particularly to insert block which is not available in most existing methods.

2. To extend the proposed method to support scalable and efficient public auditing in Cloud Computing. In particular, the proposed method achieves batch auditing where multiple delegated auditing tasks from different users can be performed at the same time by the TPA.

3. The security mechanism of our proposed method has been proved efficient and justifies the performance of our method through concrete implementation and comparisons with the state of the art methods.

The proposed method has been implemented in various stages like

1. Third Party Auditor
2. Cloud Server
3. Public Auditing
4. Batch Auditing
5. Data Dynamics

A. Third party auditor stage:

The task of allowing a third party auditor (TPA), the integrity of the dynamic data stored in the cloud is verified on behalf of the cloud client. The TPA eliminates the involvement of the client through the auditing process to check whether the data stored in the cloud are indeed intact, which is of utmost importance in achieving economies of scale for Cloud Computing. An entity, which has knowledge and capabilities that clients do not have, is trusted to access and depict risk of cloud storage services on behalf of the clients upon request. TPA can occasionally challenge the storage server to make certain the correctness of the cloud data, and the original files can be recovered by interacting with the server. The integrity of the outsourced data by demanding the server is verified by the client or TPA. The following process is depicted diagrammatically in figure 2.

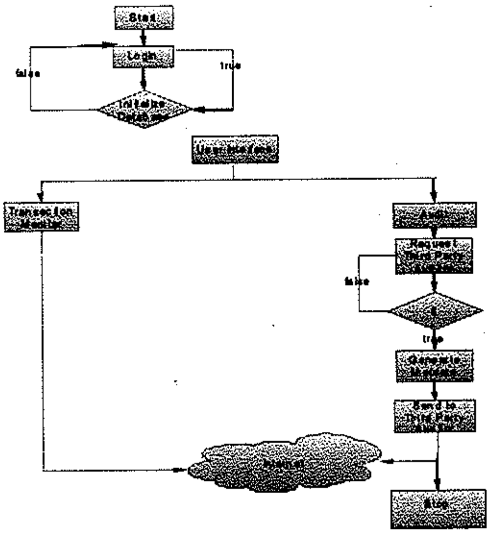


Figure 2: Third party Auditor process

B .Cloud server stage:

An entity, which is managed by Cloud Service Provider (CSP) has significant storage space and computation resource to maintain the clients data. In the cloud paradigm, by putting the large data files on the remote servers, the clients can be relieved from the burden of storage and computation. As clients no longer possess their data locally, it is of critical importance for the clients to ensure that their data are being correctly stored and maintained. That is, clients should be equipped with certain security means so that they can periodically verify the correctness of the remote data even without the existence of local copies the clients may interact with the cloud servers via CSP to access and retrieve their prestored data [6]. This process is depicted in figure 3.

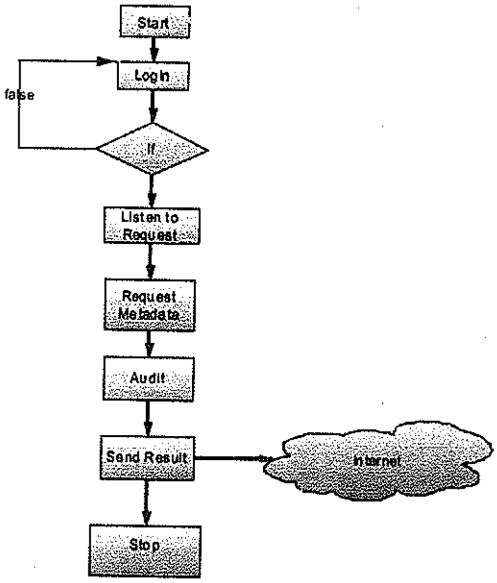


Figure 3: Cloud server Process

C. Public Auditing stage

Public auditability also allows clients to hand over the integrity verification tasks to TPA,but they themselves can be untrustworthy or not be able to entrust necessary computation resources performing continuous verifications. Public auditability allows anyone, not just the client (data owner), to challenge the cloud server for correctness of data storage while keeping no private information. Then, clients are able to handover the evaluation of the service performance to an independent third party auditor (TPA), without dedication of their computation resources. In the cloud, the clients themselves are undependable or may not be able to afford the overhead of performing frequent integrity checks. Thus, for practical use, it seems more rational to equip the verification protocol with public auditability, which is expected to play an important role in achieving economies of scale in Cloud Computing. Homomorphic authentication and unforgeable verification of metadata generated from individual data blocks. This secured aggregated data assures an auditor by verifying that a linear combination of data blocks is correctly computed. This process is diagrammatically depicted in figure 4.

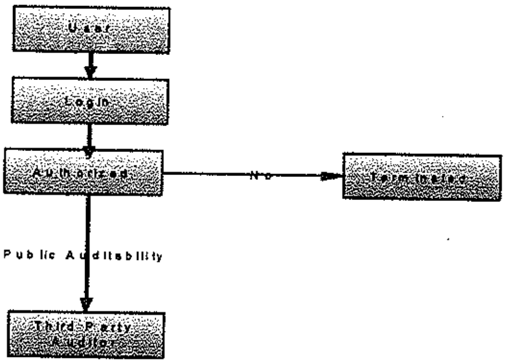


Figure 4: public auditing process

D. Batch Auditing stage:

The proposed method has been extended to support scalable and efficient public auditing in Cloud Computing. In particular, the proposed method achieves batch auditing by integrating multiple delegated auditing tasks from different users simultaneously using the TPA. As cloud servers may concurrently handle multiple verification sessions from different clients, batch auditing not only enables simultaneous verification from multiple-client, but also reduces the computation cost on the TPA side. To support efficient handling of multiple auditing tasks, bilinear aggregate signature technique has been used into a multiuser setting, where TPA can perform multiple auditing tasks simultaneously [12]. The process performed in this batch auditing stage has been illustrated in figure 5.

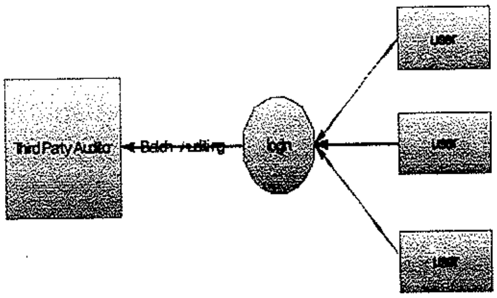


Figure 5: Batch auditing process

E. Data Dynamics Stage

Data dynamics uses the most general forms of data operation, such as block modification, insertion and deletion. It is the most important step toward practicality, because services in cloud computing are not restricted to archive or backup data only. To achieve efficient data dynamics, the improvement is made in the storage models by implementing the classic Merkle Hash Tree construction for block tag authentication. This helps in supporting data dynamics for privacy-preserving public risk auditing which is of dominant importance [16]. The proposed method can be adapted to build upon the existing work to support data dynamics, to achieve privacy-preserving public risk auditing with support of data dynamics. The workflow of this process is depicted in figure 6.

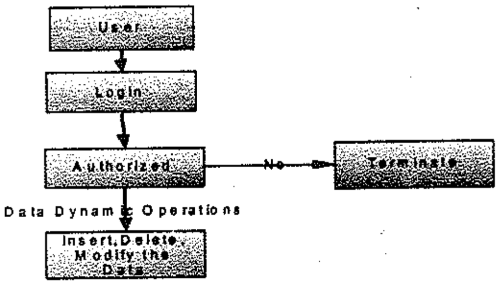
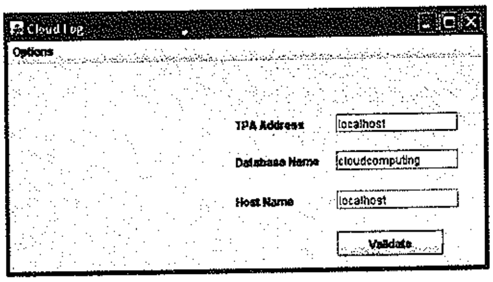


Figure 6: data dynamics process

IV. Results and Discussion

The proposed method has been implemented in java using SQL server as back end. Whenever the client needs the services of the cloud server it checks the validity of the cloud. Once the validation is successful only then the client can access the server for their needs. Figure 7 and 8 shows the validation checking process. Figure 9 and 10 below shows the auditing and server monitoring process.

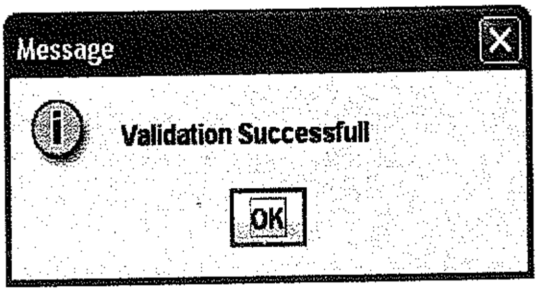


TPA Address localhost

Database Name cloudcomputing

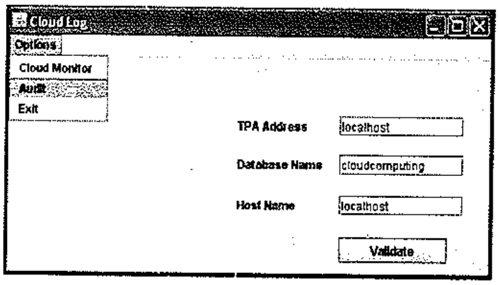
Host Name localhost

Figure 7: validation registration process



Validation Successfull

Figure 8: server monitoring process

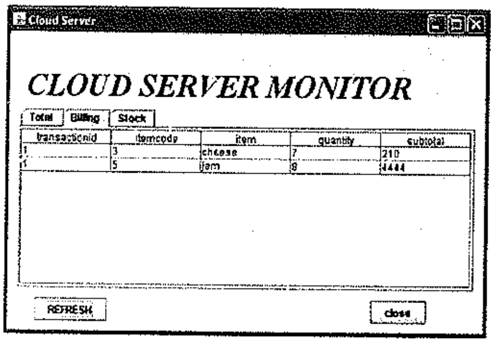


TPA Address: localhost

Database Name: cloudcomputing

Host Name: localhost

Figure 9: validation verification



transactionid	itemcode	item	quantity	subtotal
1	3	cheese	7	210
1	5	jam	8	4444

Figure 10: auditing process

V. Conclusion

To ensure cloud data storage security, it is critical to enable a TPA to evaluate the service quality from an objective and independent perspective. Public auditability also allows clients to delegate the integrity verification tasks to TPA while they themselves can be unreliable or not be able to commit necessary computation resources performing continuous verifications. Another major concern is how to construct verification protocols that can accommodate dynamic data files. In this paper, we explored the problem of providing simultaneous public auditability and data dynamics for remote data integrity check in Cloud uting.

Our construction is deliberately designed to meet these two important goals while efficiency being kept closely in mind. 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 scheme is highly efficient and provably secure.

References

[1] Cong Wang, Sherman S.-M. Chow, Qian Wang, Kui Ren and Wenjing Lou " *Privacy - Preserving Public Auditing for Secure Cloud Storage*" Proc. 14th European Conf. Research in Computer Security (ESORICS '09), pp. 355-370, 2009.

[2] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, *"Provable data possession at untrusted stores,"* in Proc. of CCS'07, Alexandria, VA, October, 2007, pp.598–609.

[3] M. A. Shah, R. Swaminathan, and M. Baker, *"Privacy preserving audit and extraction of digital contents,"* Cryptology ePrint Archive, Report 2008/186, 2008.

[4] 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. of ESORICS'09, volume 5789 of LNCS. Springer-Verlag, Sep. 2009, pp. 355–370.

[5] Juels and J. Burton S. Kaliski, *"Pors: Proofs of retrievability for large files,"* in Proc. of CCS' 07, Alexandria, VA, October2007, pp. 584–597.

[6] Cloud Security Alliance, *"Security guidance for critical areas of focus in cloud Computing,"* 2009, http:// www.cloudsecurityalliance.org.

[7] H. Shacham and B. Waters, *"Compact proofs of retrievability,"* in Proc. of Asiacrypt 2008, vol. 5350, Dec 2008, pp. 90–107.

[8] M. A. Shah, M. Baker, J. C. Mogul, and R. Swaminathan, *"Auditing to keep online storage services honest,"* in Proc.Of HotOS'07. Berkeley, CA, USA: USENIX Association, 2007, pp.1–6.

[9] 104th United States Congress, *"Health Insurance Portability and Accountability Act of 1996 (HIPPA),"* Online at http://aspe.hhs. gov/ admn simp/pl104191.htm, 1996.

[10] S. Yu, C. Wang, K. Ren, and W. Lou, *"Achieving secure, scalable, and fine-grained access control in cloud computing,"* in Proc. of IEEE INFO COM'10, San Diego, CA, USA, March 2010.

[11] D. Boneh, B. Lynn, and H. Shacham, *"Short signatures from the Weil pairing,"* J. Cryptology, vol. 17, no. 4, pp. 297–319, 2004.

[12] L. Ferrara, M. Greeny, S. Hohenberger, and M. Pedersen, *"Practical short signature batch verification,"* in Proceedings ofCT-RSA, volume 5473 of LNCS. Springer-Verlag, 2009, pp. 309–324.

[13] G . Ateniese, R. D. Pietro, L. V. Mancini, and G. Tsudik, *"Scalable and efficient provable data possession,"* in Proc. Of Secure Comm'08, 2008, pp. 1–10.

[14] C.Wang, Q.Wang, K. Ren, and W. Lou, *"Ensuring data storage security in cloud computing,"* in Proc. of IWQoS'09, July 2009, pp. 1–9.

[15] C. Erway, A. Kupcu, C. Papamanthou, and R.Tamassia, *"Dynamic provable data possession,"* in Proc. of CCS'09, 2009, pp. 213–222.

[16] R. C.Merkle, *"Protocols for public key cryptosy stems,"* in Proc.of IEEE Symposium on Security and Privacy, Los Alamitos, CA,USA, 1980.

[17] G. Ateniese, S. Kamara, and J. Katz, *"Proofs of storage from homomorphic identification protocols,"* in ASIACRYPT, 2009, pp. 319–333.

[18] Y. Dodis, S. P. Vadhan, and D. Wichs, *"Proofs of retrievability via hardness amplification,"* in TCC, 2009, pp. 109–127

AUTHORS BIOGRAPHY

Dr. M. Hemalatha : completed M.Sc., M.C.A., M. Phil., Ph.D (Ph.D, Mother Terasa women's University, Kodaikanal). She is Professor & Head and guiding Ph.D Scholars in Department of Computer Science at Karpagam University, Coimbatore. Twelve years of experience in teaching and published more than hundred papers in International Journals and also presented more than eighty papers in various national and international conferences. She received best researcher award in the year 2012 from Karpagam University. Her research areas include Data Mining, Image Processing, Computer Networks, Cloud Computing, Software Engineering, Bioinformatics and Neural Network. She is a reviewer in several National and International Journals.

T. Sumathi is presently doing Ph.D in Karpagam University, Coimbatore, Tamilnadu, India and has completed M.Phil (computer science) in the year 2006 and MCA degree in 1999 and B. Sc(computer science) in 1996. Major research area is Image processing and title for the research is image annotation. At Present, she is working as Lecturer in Karpagam University, Coimbatore.