ISSN 2395-695X (Print)
ISSN 2395-695X (Online)
International Journal of Advanced Research in Biology Engineering Science and Technology (IJARBEST)
Vol. 2, Special Issue 15, March 2016

PUBLIC AUDITING PRESERVES PRIVACY AND REGENERATION CODE BASED CLOUD STORAGE

M.RAJESHWARI[1] (PG SCHOLAR)
DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING
KALASALINGAM INSTITUTE OF TECHNOLOGY
KRISHNAN KOIL,INDIA
rajimohan92@gmail.com

R.PARVADHADEVI[2] (ASSISTANT PROFESSOR)
DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING
KALASALINGAM INSTITUTE OF TECHNOLOGY
KRISHNAN KOIL,INDIA
parvadha.ramar@gmail.com

***Abstract---* Outsourcing data in cloud storage to preserve data privacy based on checking the data integrity. To protect the authenticator information and regeneration of knowledge from someone can mishandles it. Therefore this job is appointed to a Proxy server. The information of the users are keep publicly and personal space of the cloud. Here only public cloud knowledge is accessed by user and personal cloud can stay additional secured. Once any unauthorized modification is formed, the initial knowledge within the personal cloud is retrieved by the Proxy server and can be come back to the user. In cloud storage public audit ability allows users to ask third party auditor (TPA) to check the integrity of the data and authenticator regenerating code based done by proxy server.**

Keywords—Cloud storage, authenticator, regenerating codes, public audit, privacy, proxy.

I. INTRODUCTION

Now a days Cloud storage is attracting everyone because it provides a easy and on demand data handling scheme with including several benefits. They are problems related to the storage management is rectified and global data access is allowed in the cloud environment, cloud data can be accessed anywhere majorly it supports location independence with the elimination of cost factors of hardware, software and safeguarding, etc. one thing we have to noted that this facility induces some security related problems to the user data because anybody can access the data independently. This kind of data handling which create problem for the outsourced data, exactness of data , reliability and availability get affected.

However, existing system are designed for personal audit, exclusively the data owner is allowed to predict the integrity and repair the broken servers. Considering the massive size of the outsourced knowledge and therefore the user's strained resource capability, the tasks of auditing and reparation within the cloud will be difficult and valued for the users. The overhead of exploitation cloud storage must to be reduced the maximum amount as attainable specified a user doesn't got to perform such a large amount of operations to their outsourced knowledge. Particularly, users might not wish to travel through the difficulties in confirmative and reparation. to totally make sure the knowledge integrity and save the users' computation resources additionally as on-line burden, we tend to propose the fully ensuring data integrity and save the users' computation resources as well as online burden through public auditing scheme for the regenerating-code-based cloud storage, in which the integrity checking and regeneration (of failed data blocks and authenticators) are invented by a third-party examiner and a semi-trusted proxy separately on behalf of the data publisher.

II. RELATED WORKS

Juels A. And Kaliski B.S.[1]POR offers an extra property that the client can actually “recover” the data outsourced to the cloud (in the flavor of “knowledge extraction” in zero-knowledge proof). This notion has been enhanced and extended in multiple aspects From the perspective of cloud storage efficiency, deduplication technique has become a common practice of many cloud vendors. In our data integrity protocol the TPA needs to store only a single cryptographic key irrespective of the size of the data file F and two functions which generate a random sequence. The TPA does not store any data with it. The TPA before storing the file at the archive, pre-processes the file and appends some meta data to the file and stores at the archive. At the time of verification the TPA uses this meta data to verify the integrity of the data. It is important to note that our proof of data integrity protocol just checks the integrity of data.

Chen H.C., Hu Y., Lee P.P And Tang Y.[2]Regenerating codes reduce the data repair traffic over traditional erasure codes subject to the same fault-tolerance level. In NCCloud, a proxy-based system designed for multiple-cloud storage. Functional Minimum Storage Regenerating code (F-MSR) metadata size with small, regardless of the file size. Take more time for repair process because using the matrix operation.

Lou W., Ren K., Wang C., and Wang Q.[3]Cloud storage enables users to remotely store their data and enjoy the on-demand high quality cloud applications without the burden of local hardware and software management. And also support of file-oriented cloud applications other than non-file application data, such as social networking data. In other words, the cloud data we are considering is not expected to be rapidly changing in a relative short period. Storage correctness: to ensure users that their data are indeed stored appropriately and kept interact all the time in the cloud. Dependability: to enhance data availability against Byzantine failures, malicious data modification and server colluding attacks, i.e. minimizing the effect brought by data errors or server failures.

III. THEORETICAL ANALYSIS

A. Project Scope

To support the external auditor for audit user’s outsourced data in the cloud without learning knowledge on the data content. And solving the regeneration problem of failed authenticators in the absence of data owners, substitute the proxy, which is privileged to regenerate the authenticators, into the traditional public auditing system model.

B. Problem Statement

The correctness of data in cloud put at risk for the following reasons such as: cloud infrastructure much more powerful & reliable than personal computing devices. It might be too late to recover the data loss or damage. The users to want to verify that archives do not delete or modify files prior to retrieval. The freshness of the response computation by the server is guaranteed by the fact that a challenge is never reused before reboot of the server.

C. Proposed System

In this paper, propose public auditing scheme for the regenerating-code-based cloud storage space. To resolve the regeneration difficulty of failed authenticators in the lack of information owners, we initiate a proxy, which is advantaged to redevelop the authenticators, into the usual public auditing scheme model. our method can completely free data owners from online load. In adding, we randomize the code coefficients with a pseudorandom function to protect data privacy.

D. Design Goals

To appropriately and efficiently prove the honesty of data and keep the stored file existing for cloud storage, our proposed examining scheme should get the following properties:

- Public audit ability: To permit TPA to verify the intactness of the information in the cloud on order without introducing extra operative burden to the information owner.
- Storage soundness*:* To make sure that the cloud server can in no way pass the examining

procedure except when it to be sure manage the owner's information intact.

- Confidentiality preserving: To make sure that neither the examiner nor the proxy can derive users' information content from the examining and reparation procedure.
- Authenticator regeneration*:* The authenticator of the repaired blocks can be properly renewal in the absence of the data owner.

IV. SYSTEM DESIGN

A.. Architecture Diagram

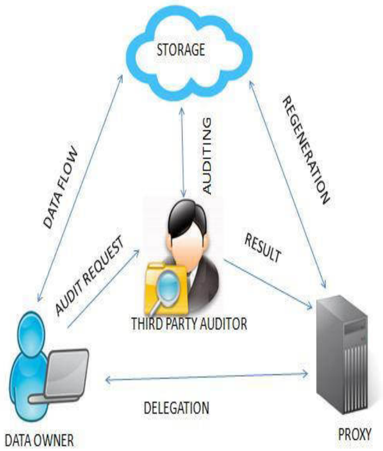

Figure: The system model

If data owner having doubt about their outsourced data then send audit request to third party auditor. TPA perform verify the correctness of file. To protect the authenticator information and regeneration of knowledge from someone can mishandles it. Therefore this job is appointed to a Proxy server.TPA can retrieve data from data storage and proxy able to forward the originality about data to owner.

B. Algorithm

The Boneh–Lynn–Shacham (BLS) signature scheme allows a user to verify that a signer is authentic. The scheme uses a bilinear pairing for verification. Signatures are often referred to as short signatures, BLS short signatures, or simply BLS signatures. The signature scheme is provably secure.A signature scheme consists of three functions: generate, sign, and verify.

Step1:Key generation

Selects a random integer x in the interval [0, r − 1]. The private key is x. The data owner have private key publishes the public key,g^x.

Step 2:Signing

Given the private key x, and some message m, we compute the signature by hashing the bitstring m, as $h = H(m)$. We output the signature $\sigma = h^x$.

Step 3:Verification

Given a signature σ and a public key g^x, we verify that $e(\sigma, g) = e(H(m), g^x)$

V. CONCLUSION

Here the data owners are confidential to delegate third party auditor*(*TPA) for their data validity checking. Data owner need not to stay online for regenerate process. Proxy server using BLS signature for mapping the authenticator and regenerate the code. This signature is purely secure.Therfore data owner online burden reduced on regenerate the authenticator and correctness of outsources data.

REFERENCES

[1]Jian Liu, Kun Huang, Hong Rong, Huimei Wang, and Ming Xian," Privacy-Preserving Public Auditing for Regenerating-Code-Based Cloud Storage" IEEE transactions on information forensics and security, vol. 10, no. 7, july 2015

[2] A. Juels and B. S. Kaliski, Jr., "PORs: Proofs of retrievability for large files," in Proc. 14th ACM Conf. Comput. Commun. Secur., 2007, pp. 584–597.

[3] S. G. Worku, C. Xu, J. Zhao, and X. He, "Secure and efficient privacy preserving public auditing scheme for cloud storage," Comput. Elect. Eng., vol. 40, no. 5, pp. 1703–1713, 2013.

[4] M. Armbrust et al., "Above the clouds: A Berkeley view of cloud computing," Dept. Elect. Eng. Comput. Sci., Univ. California, Berkeley, CA, USA, Tech. Rep. UCB/EECS-2009-28, 2009.

[5] C. Wang, Q. Wang, K. Ren, and W. Lou, “Privacy-preserving public auditing for data storage security in cloud computing,” in Proc.

[6] C. Wang, Q. Wang, K. Ren, N. Cao, and W. Lou, “Toward secure and dependable storage services in cloud computing,” IEEE Trans. Service Comput., vol. 5, no. 2, pp. 220–232, Apr./Jun. 2012.

[7] A. G. Dimakis, K. Ramchandran, Y. Wu, and C. Suh, “A survey on network codes for distributed storage,” Proc. IEEE, vol. 99, no. 3, pp. 476–489, Mar. 2011.

[8] H. Shacham and B. Waters, “Compact proofs of retrievability,” in Advances in Cryptology. Berlin, Germany: Springer-Verlag, 2008,pp. 90–107.

[9] Y. Hu, H. C. H. Chen, P. P. C. Lee, and Y. Tang, “NCCloud: Applying network coding for the storage repair in a cloud-of-clouds,” in Proc.USENIX FAST, 2012, p. 21.

[10] Y. Hu, H. C. H. Chen, P. P. C. Lee, and Y. Tang, “NCCloud: Applying network coding for the storage repair in a cloud-of-clouds,” in Proc.USENIX FAST, 2012, p. 21.

[11] K. D. Bowers, A. Juels, and A. Oprea, “HAIL: A high-availability and integrity layer for cloud storage,” in Proc. 16th ACM Conf. Comput.Commun. Secur., 2009, pp. 187–198.