ISSN 2320 - 2602
Volume 5 No.9, September 2016
International Journal of Advances in Computer Science and Technology
Available Online at http://www.warse.org/IJACST/static/pdf/file/ijacst01592016.pdf

Enabling Public Verifiability for Storage Security in Cloud Computing

A.SRI LAKSHMI PRASANNA
M.Tech (CSE)
Mahaveer
Institute of Science And
Techonology
prasuarepalli@gmail.com

Dr.B.SHASHIDHAR
Professor of CSE
HOD
Mahaveer Institute of Science
and Technology
e3hod.cse@gmail.com

Abstract

In this paper, we have a tendency to propose a completely unique privacy-preserving mechanism that supports public auditing on shared knowledge hold on within the cloud. Especially, we have a tendency to exploit ring signatures to reason verification information required to audit the correctness of shared knowledge. With our mechanism, the identity of the signer on each block in shared data is unbroken private from public verifiers, World Health Organization area unit ready to efficiently verify shared knowledge integrity while not retrieving the whole file. Additionally, our mechanism is in a very position to perform multiple auditing tasks at a similar time instead of confirmatory them one by one.

The propose system, we've a bent to utilize ring signatures to construct similarity authenticators, therefore a public supporter is in a very position to audit shared data integrity while not retrieving the whole knowledge, nevertheless it cannot distinguish who is that the signer on every block. To boost the potency of confirmative multiple auditing tasks, we have a tendency to more extend our mechanism to support batch auditing. There square measure 2 attention-grabbing issues we are going to still study for our future work. One in every of them is traceability, which implies the flexibility for the cluster manager to reveal the identity of the signer supported verification information in some special things

Keywords: auditing, privacy, shared information

1. INTRODUCTION

Cloud storage could be a model of networked enterprise storage wherever knowledge is keep in virtualized pools of storage that are typically hosted by third parties. Cloud storage provides customers with advantages, starting from price saving and simplified convenience, to quality opportunities and ascendable service. These nice options attract additional and additional customers to utilize and storage their personal knowledge to the cloud storage: in line with the analysis report, the quantity of knowledge in cloud is anticipated to attain forty trillion gigabytes in 2020. CLOUD computing could be a promising data technology design for each enterprises and people. It launches a beautiful knowledge storage and interactive paradigm with obvious blessings, together with on-demand self services, present network access, and placement freelance resource pooling [1]. Towards the cloud computing, typical service design is something as a service (XaaS), within which infrastructures, platform, software, et al. ar applied for present interconnections. Recent studies are worked to push the cloud computing evolve towards the web of services Cloud service suppliers offer user's economical and ascendable information storage services with the approach lower cost than ancient approaches [2] It's routine for users to leverage cloud storage services to share data with others throughout a cluster, as data sharing becomes a customary feature in most cloud storage offerings, additionally as Drop box, iCloud and Google Drive. later, security and privacy problems are getting key considerations with the increasing quality of cloud services. standard security approaches primarily concentrate on the sturdy authentication to appreciate that a user will remotely access its own knowledge in ondemand mode. beside the variety of the applying needs, users might want to access and share every other's approved knowledge fields to attain productive advantages, that brings new security and privacy challenges for the cloud storage. The integrity of knowledge in cloud storage, however, is subject to skepticism and scrutiny, as data hold on at intervals the cloud will merely be lost or corrupted as a results of the inevitable hardware/software failures and human errors [3], [4]. to form this matter even worse, cloud service suppliers is also reluctant {to datarm|to tell} users with respect to these info errors thus on maintain the name of their services and avoid losing profits [5]. Therefore, the integrity of cloud knowledge ought to be verified before any knowledge utilization, like search or computation over cloud knowledge [6]. The quality approach for checking knowledge correctness is to retrieve the general knowledge from the cloud, therefore verify information integrity by checking the correctness of signatures (e.g., RSA [7]) or hash values (e.g., MD5 [8]) of the overall knowledge. Certainly, this typical approach is throughout a foothold to with success check the correctness of cloud data. However, the efficiency of exploitation this ancient approach on cloud knowledge is unsure [9]. The foremost reason is that the size of cloud data unit large normally. Downloading the whole cloud data to verify information integrity can value or maybe waste user's amounts of computation and communication resources, significantly once data unit corrupted at intervals the cloud. Besides, several uses of cloud data (e.g., method and machine learning) do not primarily need users to transfer the entire cloud data to native devices [2]. It's as a results of cloud suppliers, like Amazon, offers users computation services directly on large-scale data that already existed among the cloud.

2. LITERATURE SURVEY

1) **Cong Wang, *Student Member, IEEE,* Sherman S.-M. Chow, Qian Wang, *Student Member, IEEE,* Kui Ren, *Member, IEEE,* and Wenjing Lou, *Member, IEEE]***

Advantages

- A privacy-preserving public auditing system for data storage security in Cloud Computing.
- We utilize the homomorphism linear authenticator and random masking to guarantee that the TPA would not learn any knowledge about the data content stored on the cloud server during the efficient auditing process, which not only eliminates the burden of cloud user from the tedious and possibly expensive auditing task, but also alleviates the users' fear of their outsourced data leakage.
- It is provably secure and highly efficient.

Techniques

Homomorphism linear authenticator and random masking using MAC.

- The individual auditing of these growing tasks can be tedious and cumbersome.
- The technique of public key based homomorphism linear authenticator, which enables TPA to perform the auditing without demanding the local copy of data and thus drastically reduces the communication and

computation overhead as compared to the straightforward data auditing approaches.

2) Efficient and Secure Multi-Keyword Search on Encrypted Cloud Data

- The efficient and secure ranked multi-keyword search on remotely stored encrypted database model where the database users are protected against privacy violation.
- We appropriately increase the efficiency of the scheme by using symmetric-key encryption method rather than public- key encryption for document encryption.
- The ranking method proves to be efficient to return highly relevant documents corresponding to submitted search terms.

Techniques

Ranking method, Symmetric key Encryption.

- The computation and communication costs of this method are quite large since every search term in a query requires several homomorphism encryption operations both on the server and the user side.
- They retrieving all files containing the queried keyword further incurs unnecessary network traffic.

3) Privacy-Preserving Public Auditing for Shared Data in the Cloud(Boyang Wang †,††, Baochun Li †† and Hui Li † † State Key Laboratory of Integrated Services Networks, Xidian University, Xi'an, China †† Department of Electrical and Computer Engineering, University of Toronto, Toronto, Canada Email:{bywang,bli}@eecg.toronto.edu, lihui@mail.xidian.edu.cn)

- Oruta, the TPA is able to efficiently audit the integrity of shared data, yet cannot distinguish who is the signer on each block, which can preserve identity privacy for users.
- We exploit ring signatures to compute the verification information needed to audit the integrity of shared data.
- The identity of the signer on each block in shared data is kept private from a third party auditor (TPA), who is still able to verify the integrity of shared data without retrieving the entire file.
- They share the data effectively and competent.

Techniques

Ring signature

- To preserve identity privacy from the TPA, because the identities of signers on shared data may indicate that a particular user in the group or a special block in shared data is a more valuable target than others.
- The information is confidential to the group and should not be revealed to any third party.

4) Panda: Public Auditing for Shared Data with Efficient User Revocation in the Cloud

(Boyang Wang, Baochun Li, Member, IEEE, and Hui Li, Member, IEEE)

- A new public auditing mechanism for shared data with efficient user revocation in the cloud.
- When a user in the group is revoked, we allow the semi-trusted cloud to re-sign blocks that were signed by the revoked user with proxy re-signatures.
- The group can save a significant amount of computation and communication resources during user revocation.

Techniques

Resigned techniques

- This revoked user should no longer be able to access and modify shared data.
- The integrity of the entire data can still be verified with the public keys of existing users only.

5) Remote Data Checking for Network Coding-based Distributed Storage Systems(Bo Chen, Reza Curtmola Department of Computer Science New Jersey Institute of Technology {bc47,crix}@njit.edu, Giuseppe Ateniese, Randal Burns Department of Computer

Science Johns Hopkins University {ateniese, randal}@cs.jhu.edu)

- A secure and efficient RDC scheme for network coding-based distributed storage systems that rely on untrusted server..
- RDC-NC scheme can be used to ensure data remains intact when faced with data corruption, replay, and pollution attacks.
- The RDC-NC is inexpensive for both clients and servers.

Remote Data Checking.

- The code is not systematic; it does not embed the input as part of the encoded output.
- Small portions of the file cannot be read without reconstructing the entire file.
- Online storage systems do not use network coding, because they prefer to optimize performance for read (the common operation).
- They use systematic codes to support sub-file access to data. Network-coding for storage really only makes sense for systems in which data repair occurs much more often than read.

3 EXISTING SYSTEM

Existing mechanism a brand new vital privacy issue introduced within the case of shared knowledge with the utilization of the discharge of identity privacy to public verifiers. the conventional approach for checking information correctness is to retrieve the entire information from the cloud, then verify information integrity by checking the correctness of signatures.

To firmly introduce an efficient third party auditor (TPA), the subsequent 2 basic needs ought to be met: 1) TPA ought to be able to with efficiency audit the cloud knowledge storage while not strict the native copy of information, and introduce no extra on-line burden to the cloud user; 2) The third party auditing method ought to herald no new vulnerabilities towards user knowledge privacy

LIMITATIONS

•As users not physically possess the storage of their knowledge, ancient cryptographical primitives for the aim of information security protection can not be directly adopted.

•They don't perform the multiple auditing tasks in at the same time.

4 PROPOSED SYSTEM

The propose system, we have a tendency to tend to tend to utilize ring signatures to construct similarity authenticators, thus a public supporter is throughout an edge to audit shared knowledge integrity whereas not retrieving the entire knowledge, however it cannot distinguish world organisation agency is that the signer on every block. To bolster the potency of decide multiple auditing tasks; we have a tendency to tend to tend to extra extend our mechanism to support batch auditing. There square measure 2 fascinating issues we'll still study for our future work One altogether them is traceability, that suggests the flexibility for the cluster manager to reveal the identity of the signer supported verification information in some special things.

LIMITATIONS

• The projected system will perform multiple auditing tasks at the same time

• They improve the potency of verification for multiple auditing tasks.

•High security offers for file sharing.

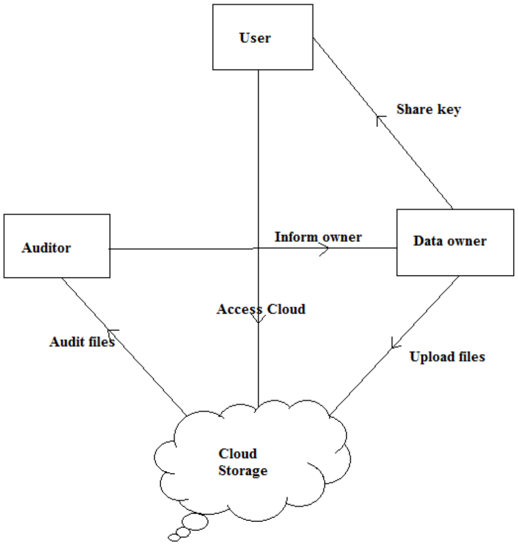
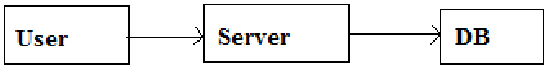


FIG: 1 ARCHITECTURE DIAGRAM

Module

1. User Registration

For the registration of user with identity ID the cluster manager arbitrarily selects variety. Then the cluster manager adds into the cluster user list which is able to be employed in the traceability part. When the registration, user obtains a non-public key which is able to be used for cluster signature generation and file cryptography.



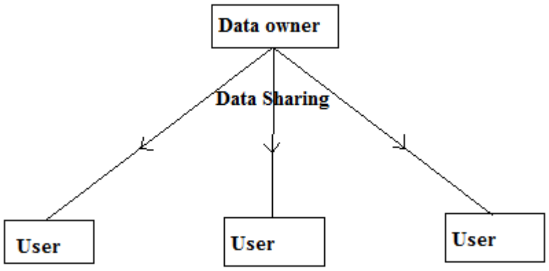
2. Public Auditing

Homomorphic authenticators square measure unforgeable verification information generated from individual knowledge blocks, which may be firmly aggregative in such how to assure associate degree auditor that a linear combination of information blocks is properly computed by confirmative solely the aggregative critic. summary to realize privacy-preserving public auditing, we have a tendency to propose to unambiguously integrate the Homomorphic critic with random mask technique In our protocol, the linear combination of sampled blocks among the server's response is disguised with randomness generated by a pseudo random perform (PRF).. The projected theme is as follows:

- Setup Phase
- Audit Phase

3. Sharing Data

The canonical application is knowledge sharing. the overall public auditing property is especially useful once we have a tendency to expect the delegation to be economical and versatile. The schemes change a content supplier to share her knowledge in a very confidential and selective method, with a set and little cipher text enlargement, by distributing to every approved user one and little mixture key.



4. Integrity Checking

Hence, supporting knowledge dynamics for privacy-preserving public risk auditing is additionally of preponderating importance. Currently we have a tendency to show however our main theme will be tailored to make upon the present work to support knowledge dynamics, together with block level operations of modification, deletion and insertion. We will adopt this system in our style to realize privacy-preserving public risk auditing with support of information dynamics. The user transfer the actual file not transfer entire file.

EXPERIMENTAL RESULTS

Survey

	Schemes				
Metric	“Provable data possession at untrusted stores	Compact proofs of retrievability	Scalable and efficient provable data possession	“Dynamic provable data possession	Our Scheme
Data dynamics	No	No	Yes	Yes	Yes
Public verifiability	Yes	Yes	No	No	Yes
Sever comp. complexity	No	No	Yes	Yes	Yes
Verifier comp. complexity	No	Yes	No	Yes	Yes
Comm. complexity	No	No	No	Yes	Yes
Verifier storage complexity	Yes	Yes	Yes	Yes	No

5. CONCLUSION

In this paper, we've an inclination to tend to propose, a privacy protecting public auditing mechanism for shared information at intervals the cloud. We’ve an inclination to utilize ring signatures to construct homomorphism authenticators, So that a public booster is during a very position to audit shared information integrity whereas not retrieving the full information, withal it cannot distinguish World Health Organization is that the signer on every block. To spice up the potency of authority multiple auditing tasks, we've an inclination to a lot of extend our mechanism to support batch auditing.

REFERENCES

[1] B. Wang, B. Li, and H. Li, “Oruta: Privacy- Preserving Public Auditing for Shared Data in the Cloud,” Proc. IEEE Fifth Int’l Conf. Cloud Computing, pp. 295-302, 2012.

[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, Apr. 2010.

[3] K. Ren, C. Wang, and Q. Wang, “Security Challenges for the Public Cloud,” IEEE Internet Computing, vol. 16, no. 1, pp. 69-73, 2012.

[4] D. Song, E. Shi, I. Fischer, and U. Shankar, “Cloud Data Protection for the Masses,” Computer, vol. 45, no. 1, pp. 39-45, 2012.

[5] 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.

[6] B. Wang, M. Li, S.S. Chow, and H. Li, “Computing Encrypted Cloud Data Efficiently under Multiple Keys,” Proc. IEEE Conf. Comm. And Network Security (CNS ’13), pp. 90-99, 2013.

[7] R. Rivest, A. Shamir, and L. Adleman, “A Method for Obtaining Digital Signatures and Public Key Cryptosystems,” Comm. ACM, vol. 21, no. 2, pp. 120-126, 1978.

[8] B. Wang, S.S. Chow, M. Li, and H. Li, “Storing Shared Data on the Cloud via Security-Mediator,” Proc. IEEE 33rd Int’l Conf. Distributed Computing Systems (ICDCS’13), pp. 124-133, 2013.

[9] D. Boneh, X. Boyen, and H. Shacham, “Short Group Signatures,” Proc. 24th Ann. Int’l Cryptology Conf. (CRYPTO’04), pp. 41-55, 2004.

[10] B. Wang, B. Li, and H. Li, “Knox: Privacy-Preserving Auditing for Shared

Data with Large Groups in the Cloud,” Proc. 10th Int’l Conf. Applied Cryptography and Network Security (ACNS’12), pp. 507-525, June 2012.

[11] E. Brickell, J. Camenisch, and L. Chen, “Direct Anonymous Attestation,” Proc. 11th ACM Conf. Computer and Comm. Security (CCS’04), pp. 132-145, 2004.

[12] D. Boneh, B. Lynn, and H. Shacham, “Short Signatures from the Weil Pairing,” Proc. Seventh Int’l Conf. Theory and Application of Cryptology and Information Security: Advances in Cryptology (ASIACRYPT’01), pp. 514-532, 2001.

[13] R.L. Rivest, A. Shamir, and Y. Tauman, “How to Leak a Secret,” Proc. Seventh Int’l Conf. Theory and Application of Cryptology and Information Security: Advances in Cryptology (ASIACRYPT’01), pp. 552-565, 2001.