A Novel and Dynamic Protocol to Ensure Secure Data Storage and Sharing In Cloud

Ch.Venkata Ramana[*], M.V.Rajesh[#]
M.Tech Scholar[*], Associate Professor [#]
[#]Dept of CSE, Pragati Engineering college, Surampalem, A.P, India*

Abstract: Data storage over cloud is still an important research issue over cloud computing. In this paper we are proposing a novel Data storage and sharing protocol over cloud dynamically, during the data uploading to the server (Regular server/Cloud) through the data owner. Auditor plays the main role of monitoring the data transmission and data manipulations between the data owner and server. We introduced a secure and efficient dynamic auditing protocol by using the File segmentation and distribution, Tag generation, and Random Challenge and verification algorithms. Our proposed approach is efficient than the traditional protocols.

I. INTRODUCTION

Cloud storage is an important service of cloud computing [1], which allows data owners (owners) to move data from their local computing systems to the cloud. More and more owners start to store the data in the cloud [2]. However, this new paradigm of data hosting service also introduces new security challenges [3]. Owners would worry that the data could be lost in the cloud. This is because data loss could happen in any infrastructure, no matter what high degree of reliable measures cloud service providers would take [4]–[8]. Sometimes, cloud service providers might be dishonest. They could discard the data which has not been accessed or rarely accessed to save the storage space and claim that the data are still correctly stored in the cloud. Therefore, owners need to be convinced that the data are correctly stored in the cloud.

Traditionally, owners can check the data integrity based on two-party storage auditing protocols [9]–[11]. In cloud Storage system, however, it is inappropriate to let either side of cloud service providers or owners conduct such Auditing, because none of them could be guaranteed to provide unbiased auditing result. In this situation, third party auditing is a natural choice for the storage auditing in cloud computing. A third party auditor (auditor) that has expertise and capabilities can do a more efficient work and convince both cloud service providers and owners.

For the third party auditing in cloud storage systems, there are several important requirements which have been proposed in some previous works [8], [9]. The auditing protocol should have the following properties: 1) Confidentiality. The auditing protocol should keep owner's data confidential against the auditor. 2) Dynamic Auditing. The auditing protocol should support the dynamic updates of the data in the cloud. 3) Batch Auditing. The auditing protocol should also be able to support the batch auditing for multiple owners and multiple clouds.

In [13], the authors proposed a dynamic auditing protocol that can support the dynamic operations of the data on the cloud servers, but this method may leak the data content to the auditor because it requires the server to send the linear combinations of data blocks to the auditor. In [14], the authors extended their dynamic auditing scheme to be privacy-preserving and support the batch auditing for multiple owners.

However, due to the large number of data tags, their auditing protocols may incur a heavy storage overhead on the server. In [15], Zhu et al. proposed a cooperative provable data possession scheme that can support the batch auditing for multiple clouds and also extend it to support the dynamic auditing in [26]. However, their scheme cannot support the batch auditing for multiple owners. That is because parameters for generating the data tags used by each owner are different and thus they cannot combine the data tags from multiple owners to conduct the batch auditing. Another drawback is that their scheme requires an additional trusted organizer to send a commitment to the auditor during the multi-cloud batch auditing, because their scheme applies the mask technique to ensure the data privacy. However, such additional organizer is not practical in cloud storage systems. Furthermore, both Wang's schemes and Zhu's schemes incur heavy computation cost of the auditor, which makes the auditor a performance bottleneck.

II. RELATED WORK

Cloud Computing is presently one of the hottest topics in information technology (IT). Since the outsourcing of all the essential data is available with a third party, there is always having a concern of cloud service provider¨s trust-worthiness. Due to data privacy, it is essential for users to encrypt their sensitive data before storing them into the cloud. Yet, there exist some shortcomings in the situation of traditional encryption. When a secret key owner wants to look for some data that are stored in the cloud storage, he may be needed to download all encrypted data from the

cloud server, and then decrypts and searches them. If the encrypted data are huge or the client is a mobile user, then it will be very inefficient and is not convenient. Otherwise he must send his key to the cloud server which performs the decryption and search procedures. It causes a serious trouble that the cloud server obtains the secret key So many models were existed to ensure the integrity of data file.

In "Provable Data Possession" (PDP) model [4] ensures the possession of data files on untrusted storages. It uses a RSA based homomorphic linear authenticator for auditing outsourced data, but this model leaks the data to external auditors and hence was not provably privacy preserving. Juels et.al [5] describes a "Proof of Retrievability" (PoR) model, where spot-checking and error correcting codes are used in order to ensure the possession and retrievability. But this approach works only with encrypted data. Improved versions of PoR protocols had been proposed which guarantees private auditability and one which make use of BLS signatures. But these approaches were not privacy-preserving. Then comes the TPA based approach to keep online storage honest. This scheme only works for encrypted files which requires the auditor to keep state, and suffers from bounded usage, which potentially brings in online burden to users when the keyed hashes are used up.Thus to provide secure cloud storage supporting privacy-preserving many methodologies, frameworks and protocols have been proposed

III. PROPOSED WORK

In this paper we proposed an efficient dynamic auditing protocol between data owner, auditor and cloud server. The following dynamic auditing protocol contains the following implementations like File segmentation and distribution, Tag generations, Challenge generation and verification, architecture of the system is shown below.

Auditing protocol

Data owner fragment the entire content in to number of blocks and generates the tags for individual block and uploads the data in to the server and forwards the hash code and a random challenge. Abstract information, tag generation keys and random challenge are forwarded to the third part auditor

A)Dynamic auditing protocol

Before describing the auditing protocol, we first define some notations

Symbol Meaning

M Data component

T Set of tag generation keys

RA Random challenge to Auditor(Large Prime Number)

RB Random Challenge to Cloud server(Large Prime Number)

H(RA XOR RB) Hash code after XOR Over RA and RB

Minfo Meta or abstract information of M

N Number of blocks in the each component

B)Data Owner Initialization

Suppose a file F has m data components as F = (F1, • • • ,Fm). Each data component has its physical meanings and can be updated dynamically by the data owners, data owner needs to encrypt it with its corresponding key. Each data component Fk is divided into nk data blocks denoted as Fk = (mk1,mk2, • • • ,mknk).

After dividing the file in to number of blocks and encrypts the blocks with key that can be considered as tag key Ti, encrypt the all file until the data component is encrypted with tag keys, now data owner generates a random challenge RA and forwards to the cloud service provider along with data component (m1,m2,....mn) and hash code ,which is generated by the two random challenges which are distributed by the data owner,for encryption process we used Rijndael algorithm .

C. Rijandael algorithm

Our paper uses an advanced cryptographic algorithm for secure data transmission and it uses the key, which is generated from the multikey exchange group key protocol and the brief structure of the novel cryptographic algorithm as shown below ,the system mainly works on substitution and affine transformation techniques

1. KeyExpansion—round keys are derived from the cipher key using key schedule

2. Initial Round

1. AddRoundKey—each byte of the state is combined with the round key using bitwise xor

3. Rounds

1. SubBytes—a non-linear substitution step where each byte is replaced with another according to a lookup table.

2. ShiftRows—a transposition step where each row of the state is shifted cyclically a certain number of steps.

3. MixColumns—a mixing operation which operates on the columns of the state, combining the four bytes in each column.

4. AddRoundKey

4. Final Round (no MixColumns)

1. SubBytes

2. ShiftRows

3. AddRoundKey

Complete implemention of the subbytes,shiftrows,mix columns and add round key as follows[16], for implementation details we had used builtin algorithm from the dotnet namespaces.

E)Auditor Implementation

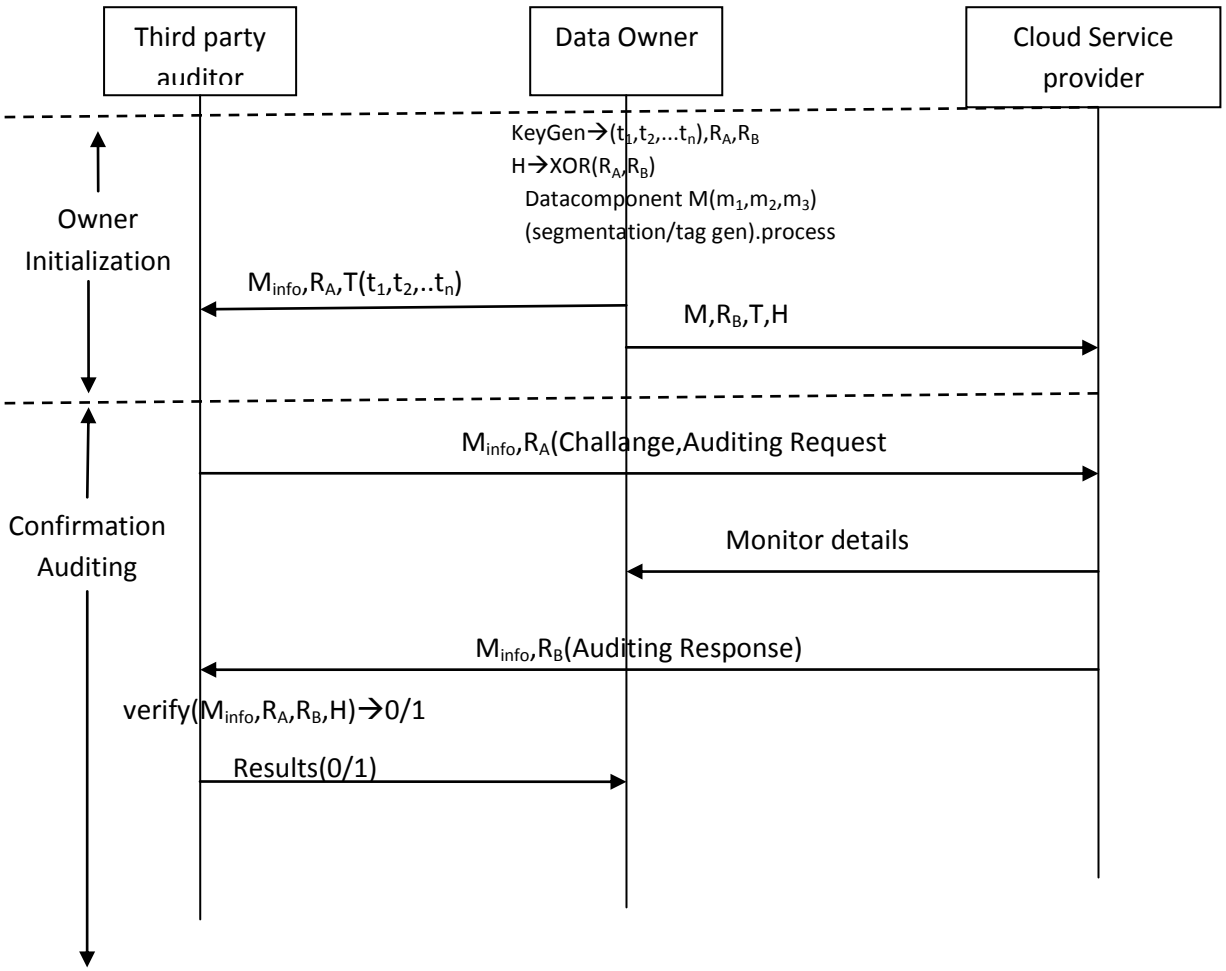
Auditor monitors the manipulations between the data owner and cloud service provider, receives the meta information of the data component, tag generation key and random challenge from the data owner, now by making a request to the cloud server auditor gets the meta information of the data component, before processing the request checks for authentication the and checks with the meta information which is received from the data owner.

B)Service Provider

Data owner hosts the data over cloud servers. Here the data which is fragmented and encrypted by the data owner, data owner can access the information when ever required from the cloud server. Auditor access the information for auditing purpose if he is authenticated, Submits the access process to the data owner when ever required.

a)Novel Dynamic Auditing Protocol

The following protocol describes over novel auditing protocol as follows



Data owner initializes the data component by fragmentation, encryption and by forwarding the Meta information about the data component and random challenge and data can be hosted in to the server and

hash/authentication code forwarded to the cloud server for authenticated monitor

Auditor receives the Random challenge (a large prime number) and (Minfo) meta information and makes a monitor request to the cloud server. Cloud service provider authenticate the auditor and forward the meta information to the Auditor,CSP forwards the monitor details when ever requested.

IV. CONCLUSION

In this paper we Introduced an efficient novel dynamic auditing protocol for secure data manipulations and auditing,aprt from the traditional approaches we are not completely rely on the third part auditors, So over protocol allows the auditor to monitors the data component meta information only that provides the abstract information of the data component. Data owner can receive the regular monitoring details.

REFERENCES

[1] P. Mell and T. Grance, "The NIST definition of cloud computing,"National Institute of Standards and Technology, Tech. Rep., 2009.

[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," Commun. ACM, vol. 53, no. 4, pp. 50–58, 2010.CA, USA, 2004, pp.

[3] L. N. Bairavasundaram, G. R. Goodson, S. Pasupathy, and J. Schindler, "An analysis of latent sector errors in disk drives," in SIGMETRICS, L. Golubchik, M. H. Ammar, and M. Harchol-Balter, Eds. ACM, 2007, pp. 289–300

[4] B. Schroeder and G. A. Gibson, "Disk failures in the real world: What does an mttf of 1, 000, 000 hours mean to you?" in FAST. USENIX, 2007, pp. 1–16.

[5] M. Lillibridge, S. Elnikety, A. Birrell, M. Burrows, and M. Isard, "A cooperative internet backup scheme," in USENIX Annual Technical Conference, General Track. USENIX, 2003, pp. 29–41.

[6] Y. Deswarte, J. Quisquater, and A. Saidane, "Remote integrity checking," in The Sixth Working Conference on Integrity and Internal Control in Information Systems (IICIS). Springer Netherlands,November 2004.

[7] M. Naor and G. N. Rothblum, "The complexity of online memory checking," J. ACM, vol. 56, no. 1, 2009.

[8] A. Juels and B. S. K. Jr., "Pors: proofs of retrievability for large files," in ACM Conference on Computer and Communications Security, P. Ning, S. D. C. di Vimercati, and P. F. Syverson, Eds. ACM, 2007, pp. 584–597.

[9] T. J. E. Schwarz and E. L. Miller, "Store, forget, and check: Using algebraic signatures to check remotely administered storage," in ICDCS. IEEE Computer Society, 2006, p. 12.

[10] D. L. G. Filho and P. S. L. M. Barreto, "Demonstrating data possession and uncheatable data transfer," IACR Cryptology ePrint Archive, vol. 2006, p. 150, 2006.

[11] F. Seb´e, J. Domingo-Ferrer, A. Mart´ınez-Ballest´e, Y. Deswarte, and J.-J. Quisquater, "Efficient remote data possession checking incritical information

[12]http://en.wikipedia.org/wiki/Advanced_Encryption_Standard

[13] T. Velte, A. Velte, and R. Elsenpeter, Cloud Computing: A Practical

Approach, 1st ed. New York, NY, USA: McGraw-Hill, Inc., 2010, ch. 7.

[14] J. Li, M. N. Krohn, D. Mazi`eres, and D. Shasha, "Secure untrusted data repository (sundr)," in Proceedings of the 6th conference on Symposium on Operating Systems.

BIOGRAPHIES

Ch Venkata Ramana working towards the Masters degree of computer science and at Pragati engineering college in India. His work is focused on virtualization technology and Cloud computing.

M V RAJESH received the M Tech degree from JNTUCE,K, Jawarharlal Nehru Technological University, Hyderabad in 2006. Currently he is working as Associate Professor in PRAGATI Engineering College, Surampalem, Andhra Pradesh, India. He has five years of experience in teaching and five years of experience in software industry. Previously he has worked with SIEMENS Information Systems Ltd, as Associate Consulatnt in the role of Software Developer in the HealthCare domain. His research interests include object oriented programming, cloud computing