International Journal of
Emerging Research in Management &Technology
ISSN: 2278-9359 (Volume-3, Issue-5)

Research Article | **May 2014**

Analysis of Secure Cloud Data Sharing Within a Group

Ms. Mayuri Pande*
Department of CSE, GHRAET
Nagpur (M.S), India,

Prof. Vikrant Chole
Dept of Computer Science & Engg
Nagpur (M.S.), India

Abstract—

In this paper, we propose a secure shared group *model of* ***cloud storage. Our proposed model is based on the cryptological technology that each member in the same group has its private key respectively and shares a common public key to protect the shared data in cloud. The illegal or unauthorized users cannot access the data because they do not have the access key. Based on our model, the security of shared data can be guaranteed, neither CSP nor any third party can disclose the shared data in cloud storage.***

Keywords— CSP (Cloud service Provider), Encryption, Cloud Storage

I. INTRODUCTION

These days several trends are found related to the new era of Cloud Computing. It is an Internet-based development and use of computer technology. Data centers are being transformed into pools of computing service on huge scale with the help of powerful processors and SAAS (Software as a Service) architecture with cheaper cost and powerful processors. The increasing network bandwidth and reliable yet flexible network connections make it even possible that users can now subscribe high quality services from data and software that reside solely on remote data centers.

Moving data into the cloud offers great convenience to users since they don't have to care about the complexities of direct hardware management. Well known examples are Amazon Simple Storage Service (S3) and Amazon Elastic Compute Cloud (EC2) who are the pioneer of Cloud Computing vendors. This computing platform shift because of these internet-based online services those are providing huge amounts of storage space and customizable computing resources, responsibility of local machines for data maintenance is getting eliminated. And thus, users are dependent on cloud service providers for the availability and integrity of their data. Example for this is recent downtime of Amazon's S3. Data security is an important aspect of quality of service and Cloud Computing poses challenging security threats. Firstly, For the purpose of data security protection traditional cryptographic primitives cannot be directly adopted since users will lose control of data under Cloud Computing. Thus, data storage in the cloud must verified explicitly without knowledge of the whole data. Each user contain various kinds of data stored in the cloud and also user expects long term, continuous assurance of their data safety. Because of which verifying correctness of data storage in the cloud becomes even more challenging. Secondly, Cloud storage is not just a third party data warehouse. User frequently updates his data stored in the cloud, including insertion, deletion, modification, appending, reordering, etc. Thus ensuring storage correctness under such circumstances of frequent data update is of great importance. However, this dynamic feature makes traditional techniques of integrity insurance futile and requires new solutions. Last but not the least, data centers running in a simultaneous, cooperated and distributed manner empowers the deployment of Cloud Computing. Each user's data is stored in multiple physical locations redundantly to reduce the data integrity threats. Therefore, to achieve a robust and secure cloud data storage system in the real world, distributed protocols for storage correctness assurance is of most importance in achieving. However, such important areas are not yet explored fully in literature.

II. RELATED WORK

Some researchers did research on the availability and integrity of data that is outsourced. G.Atenies et al. [1] proposed a scheme- Provable Data Possession (PDP) that efficiently detects large fraction of file corruption at stores that are not trusted, but it does not guaranties files retrievability. Based on the PDP scheme, to overcome the problem in PDP R. D. Pietro et al. [2] proposed a Scalable Data Possession (SDP). According to it, it dynamically test the integrity of stored data.To guard the Outsourced data security, Ari Juels et al. [4] provided a Proofs of Retrievability (POR) scheme. This scheme guaranties the file retrievability and it efficiently verifies data corruptions as well.

Shacham et al. [3] proposed an innovative model of POR, enabling a lot of queries for public verifiability and reducing the overhead. Kennadi D et al. [5] then improves the JK [4] and SW [3] models and proposed an implementation and theory for the POR. Although, these schemes do not solve all security issues because of their focus on one single server. To overcome the disadvantages of above schemes, distributed protocols [6], has been proposed extending the security of data storage on multiple servers. Kennadi Brow et al. ensures the availability of data in cloud.

Schwarz et al. [6] proposed a new model that verifies the security of data in distributed storage system. This model checks a lot of data consuming minimum bandwidth in distributed storage systems. However, these protocols do not solved all the security threats for cloud storage. Wang et al[8]. introduced a homomorpic distributed verification protocol which uses Pseudorandom Data ensuring cloud storage security. This protocol sets its focus on verifying

misbehaving servers and the storage correctness as well. However, Pseudorandom Data does not cover the entire data since during identification of the cloud servers, it may miss some data corruptions since the proposed protocol do not provide full protection for cloud storage.

To prevent cheating in a P2P systems, Fiho et al.[9] uses a secured hash function , however it is cannot be used for cloud storage when file is large. Shah et al. introduced an auditing scheme, involving a Third Party Auditor (TPA) keeping online storage honesty with hash values that are calculated by user on encrypted file. However, this scheme is applicable only for encrypted files.

Kamara [11] et al. then introduced a framework of a cryptographic storage service (ACSS) considering the issue of building a secure cloud storage service on cloud infrastructure where one cannot trust the service provider. It consists of three basic components (DP, DV, and TG) and practices encryption, storage and integrity validation through a group of protocols. However, ACSS is difficult to build since it needs to modify lots of the source code of cloud storage platform. Further, users have to request data owner in order to access the shared data, due to which it will make a communication a bottle neck since the number of users will rapidly increase. Moreover, ACSS is just a conceptual model and the design did not yet implemented completely. Secure group communication and data sharing also need to consider the member of group increasing.

Using asymmetric cryptography containing public and private key pair to achieve the data security, for example RSA, the most popular asymmetric algorithm. The RSA algorithm can be used in both encryption and decryption, digital signature and identification. However, o use such asymmetric cryptography in group needs a PKI infrastructure and the trusted Certificate Authority (CA) in the system and each entity need to request the public key of other entity, which will be an overhead as group may contain large amount of group members.

III. IMPLEMENTATION

A. Main Modules

1) *Client Module:* Very firstly client authorization process takes place which includes entering username and password for security purpose. If user not yet register he can register and then login. After login the client sends the query to receive certain file from the server. Server searches the queried file in the database and then responds with the requested file to the client. Server sends the alternative path to the intruders if found any.

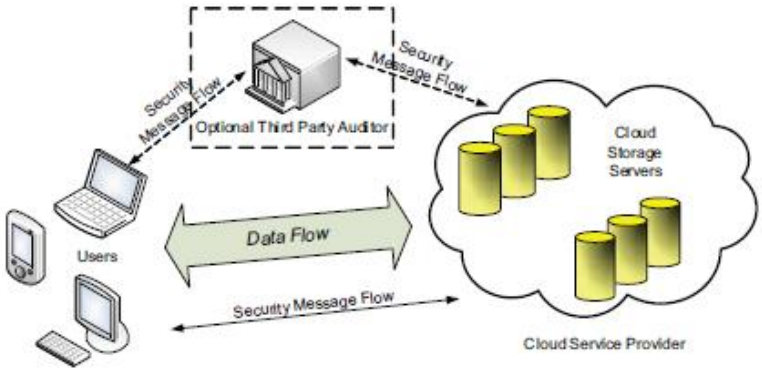

Fig. 1 Network architecture for cloud data storage

2) *System Module:* Fig 1 shows the network architecture of cloud data storage containing three different network entities as follows:

- User: Individual consumers or organizations whose data is to be stored in the cloud. Users rely on the cloud for data computation.
- Cloud Service Provider (CSP): A CSP having sufficient resources and expertise in building in terms of hardware. CSP manages distributed cloud storage servers and owns and operates live Cloud Computing systems.
- Third Party Auditor (TPA): It is an optional component having expertise and capabilities that normal users may not have. On behalf of the users upon request. It is trusted to assess and expose risk of cloud storage services

3) *Cloud data storage Module:* CSP has various clod servers running simultaneously. Through CSP a user stores his into a set of servers. The user contacts with the cloud servers through CSP to access or to retrieve his data stored there. Sometimes user may need to access data in block. For the users to access block data they should have security means to make continuous correctness assurance for their own stored data even if local copies are not existing. An optional trusted TPA comes into picture when user does not necessarily have the time,

feasibility or resources to manage their data, in that case they can give these tasks to TPA of their respective choices. In our model, the assumption is that the point-to-point communication channels between user and each cloud server is authenticated and reliable, though achieving this in practice will increase little overhead.

4) *Cloud Authentication Server:* The function of Authentication Server (AS) is any other Authentication Server would as the typical client-authentication protocol along with few additional behaviors added. First addition is sending the information regarding client authentication to the masquerading router. The AS in this model also acts as a ticketing authority who controls permissions on the application network. Other optional functionality that AS should support is updating lists of client, which causes reduction in time of authentication or even the client removal as a valid client depending upon the request

5) *Unauthorized data modification and corruption module:* One of the important issues is to detect any unauthorized data modification and corruption effectively, this may be due to server compromise and/or random Byzantine failures. Moreover, in the case of distributed architecture when such inconsistencies are detected successfully, finding which server containing the data error is also of great significance.

6) Adversary Module: There are two sources of Security threats that cloud data storage faces. Firstly, a CSP itself can be untrusted, self-interested, and possibly malicious. It may desire to move data that is rarely or has not been accessed to a lower tier of storage than agreed for monetary reasons, as well as it may also attempt to hide a data loss incident due to management errors, called Byzantine failures that is not accepted and so on.

Secondly, there may also be an economically motivated adversary, having the capability to compromise a number of cloud data storage servers in different time intervals and at the same time is able to modify or delete users' data while remaining undetected by CSPs for a certain period. Thus, we consider that there are two types of adversary with different levels of capability in this paper:

- Weak Adversary: The adversary who is interested in corrupting the user's data files that are stored on individual servers. Once a server is comprised, an adversary can pollute the original data files by introducing its own fraudulent data or modifying that prevent the user to retrieve his original data.
- Strong Adversary: This is considered as the worst case scenario, where we assume that the adversary can compromise all the storage servers so that he can modify the data files intentionally as long as they are consistent internally. In fact, this is equivalent to the case in which all servers are colluding together to hide a corruption incident or data loss.

B. Implementation

In previous implementation public key cryptography is used to provide storage security of files over cloud.
Drawbacks of existing RSA are-

1) Speed is slow
2) Not feasible for decrypting bulk messages
3) If an attacker identifies the private key of any party, the entire message can be easily encrypted.

Thus we implemented encryption as follow-

1) Public key generator(PKG) generates public key and assign unique key to each group member
2) PKG sends the file to the cloud by encrypting it using public key

F(public key, hash(unique key))

3) Private key of each user is already with the respective user and performs the decryption as-

F(private key,hash(unique key))

4) In this way user can easily decrypt the message.

IV. RESULT ANALYSIS

File name	File Size in kb	RSA execution time (ms)	RSA extended (ID Based RSA) Our Approach execution time (ms)
supervisisor_list2012.pdf	337	1185.8	909.375
hi.doc	10	839.2	525
app_menu.txt	4	342.1	194.3

Table . 1 Comparison between RSA and extended RSA for time taken to encrypt file

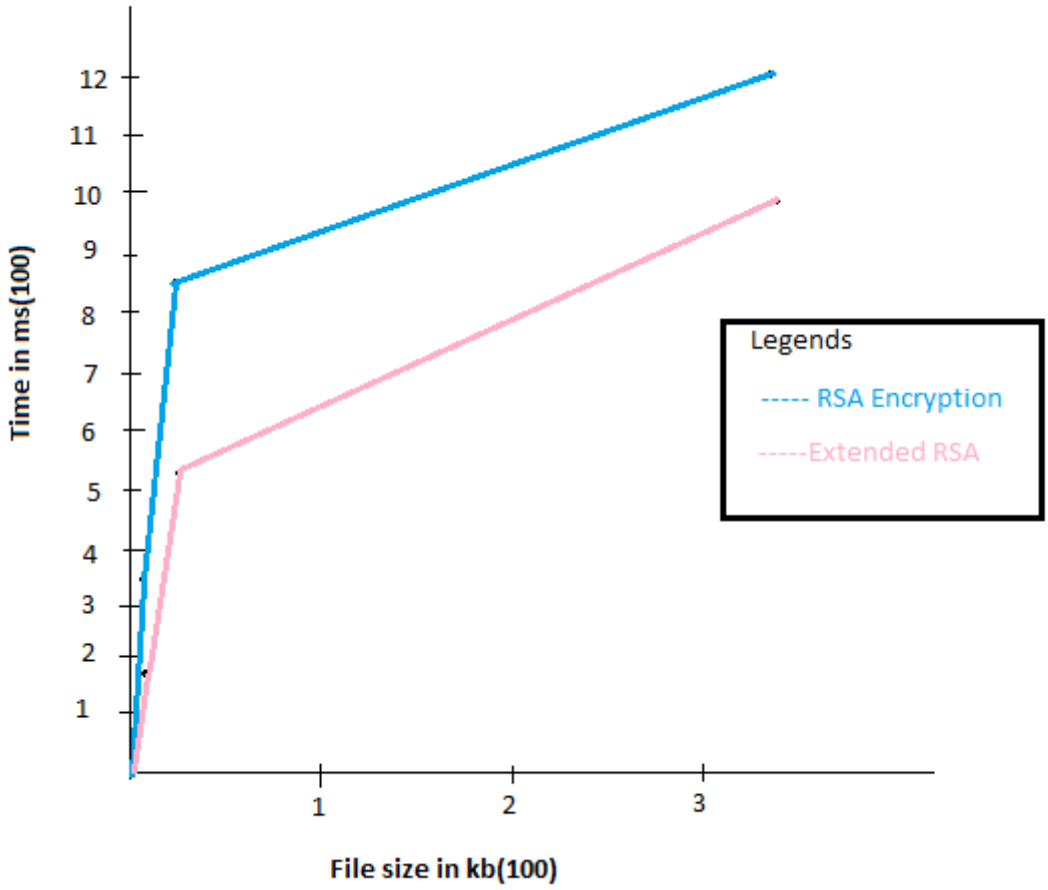

Fig. 2 Graph showing the comparison

V. CONCLUSIONS

In this paper, we analyzed the problem of security of data in cloud data storage, which is a distributed storage system. To ensure users' data correctness in cloud data storage, we proposed a flexible and effective distributed scheme with explicit dynamic data support, with block update, delete, and append. We are dependent on erasure-correcting code in the preparation of file distribution to provide redundancy parity vectors and guarantee the dependability of data. Utilizing the homomorphic token along with distributed verification of erasure coded data, our scheme achieves the integration of data error localization and storage correctness insurance, i.e., whenever data corruption has been occurred during the verification of storage correctness across the distributed servers, we can guarantee identification of the misbehaving server(s) simultaneously. Through detailed analysis of security and performance, we shown that our scheme is highly efficient and resilient to Byzantine failure, even server colluding attacks and malicious data modification attack.

We believe that security of data storage in Cloud Computing is an area full of challenges and of great importance, and is still in its earlier stage now, and many research problems are yet to be identified and done. We found several possible directions for future research on this area. We believe that the most promising one is a model in which public verifiability is enforced. Where Public verifiability is supported, it allows TPA to audit the cloud data storage without demanding time of users, resources or feasibility. An interesting question in this model is that if we can construct a scheme to achieve public verifiability as well as storage correctness assurance of dynamic data. Also, along with our research on dynamic cloud data storage, we are planning to investigate the problem localization of fine-grained data error.

REFERENCES

[1] Ching-Hung Yeh, "A Secure Shared Group Model of Cloud Storage" 27th International Conference on Advanced Information Networking and Applications Workshops, 2013.

[2] Takabi, H.; Joshi, J.B.D.; Ahn, G.;"Security and Privacy Challenges in Cloud Computing Environments," *Security & Privacy, IEEE* , vol.8, no.6, pp.24-31, Nov.-Dec 2010.

[3] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner,Z. Peterson,and D. Song, "Provable Data Possessionat Untrusted Stores, *14th ACM conference on Computerand communications security*, pp. 598609, 2007.

[4] G. Ateniese, R. D. Pietro, L. V. Mancini, and G. Tsudik,"Scalable and Efficient Provable Data Possession, *4th international conference on Security and privacy in communication networks*, pp. 110, 2008.
[5] H. Shacham and B. Waters, Compact Proofs of Retrievability, *14th International Conference on the Theory and Applicationof Cryptology and Information Security: Advances in Cryptology*, pp. 90 - 107, Dec. 2008
[6] A. Juels and J. Burton S. Kaliski,"PORs: Proofs of Retrievability for Large Files, *14th ACM conference on Computerand communications security*, pp. 584-597, 2007.
[7] K. D. Bowers, A. Juels, and A. Oprea, Proofs of Retrievability: Theory and Implementation, *CCSW '09 Proceedings of the2009 ACM workshop on Cloud computing security*, pp. 43-54,2009.
[8] Schwarz, T.S.J.; Miller, E.L.;, "Store, Forget, and Check: Using Algebraic Signatures to Check Remotely Administered Storage," *Distributed Computing Systems, 2006. ICDCS2006. 26th IEEE International Conference on*, pp. 12, 2006.
[9] Cong Wang; Qian Wang; KuiRen; Wenjing Lou; , "Ensuring data storage security in Cloud Computing," *Quality of Service, 2009*. July 2009.
[10] D. L. G. Filho and P. S. L. M. Barreto, Demonstrating Data Possession and Uncheatable Data Transfer, cryptology ePrint Archive, Report 2006/150, 2006, http://eprint.iacr.org/.
[11] M. A. Shah, M. Baker, J. C. Mogul, and R. Swaminathan, Auditing to Keep Online Storage Services Honest, *Proc. 11th* pp.16, 2007.
[12] Kamara, Seny and Lauter, Kristin, Cryptographic cloud storage, *FC'10 Proceedings of the 14th international conference on Financialcryptograpy and data security*, pp.136-149, 2010.
[13] Yeh, Ching-Hung and Huang, Yueh-Min and Wang, Tzone- I and Chen, Hsiao-Hwa, "DESCVA Secure Wireless Communication Scheme for Vehicle ad hoc Networking," *Mobile Networks and Applications, Springer Netherlands*, vol.14, no.5, pp.611-624, 2009.
[14] R. Rivest, A. Shamir and L. Adleman,"A method for obtaining digital signature and public key cryptosystems" *Communication of the ACM*, Vol. 21, No.2, Feb. 2009.