



## **Secure Data sharing in dynamic groups for cloud storage with backup manager**

Miss.Kulkarni Chaitali S, Prof.A.M.Wade  
Smt. Kashibai Navle College of Engineering,  
Vadgoan BK, Pune, Maharashtra, INDIA.

**Abstract:** Cloud computing is associate degree rising computing paradigm within which resources of the computing infrastructure area unit provided as services over the net. As promising because it is, this paradigm conjointly brings forth several new challenges for knowledge security and access management once users confidential against untrusted servers, existing solutions sometimes apply cytological ways by revealing knowledge cryptography keys solely to approved users. One among the largest considerations with cloud knowledge storage is that of knowledge integrity verification at untrusted servers. To preserve knowledge privacy, a basic resolution is to encrypt knowledge files, so transfer the encrypted knowledge into the cloud. To resolve this problem recently the simplest economical technique MONA given for secured multi owner data sharing in but we have a tendency to known some limitations within the same approach in terms of responsibility and quantifiability. Therefore during this paper we have a tendency to area unit more extending the fundamental by adding backup manager the responsibility still as raising the quantifiability by increasing the quantity of cluster managers dynamically.

**Keywords:** Dynamic Group, Data Sharing, Multi owner, Computing, Backup Manger.

### **I. Introduction**

In cloud computing, the cloud service suppliers (CSPs), like Amazon, square measure able to deliver numerous services to cloud users with the assistance of powerful datacenters. By migrating the native information management systems into cloud servers, users will relish high-quality services and save important investments on their native infrastructures. Cloud computing is one in every of the best platform that provides storage of information in terribly lower value and out there for all time over the web Cloud computing is Internet-based computing, whereby shared resources, computer code and knowledge square measure provided to computers and devices on demand. Many trends square measure gap up the age of Cloud Computing that is associate Internet-based development and use of engineering. Cloud Computing suggests that over merely saving thereon implementation prices. Cloud offers huge chance for brand spanking new innovation, and even disruption of entire Industries. Cloud computing is that the long unreal vision of computing as a utility, wherever information homeowners will remotely store their information within the cloud to get pleasure from on demand high-quality applications and services from a shared pool of configurable computing resources.

#### **A. Basic concept**

Maintaining the integrity information plays an important role within the institution of trust between data subject and repair supplier. though unreal as a promising service platform for the web, the new information storage paradigm in "Cloud" brings concerning several difficult style problems that have profound influence on the safety and performance of the system. one in all the most important issues with cloud information storage is that of information integrity verification at untrusted servers. what's a lot of serious is that for saving cash and space for storing the service supplier would possibly neglect to stay or deliberately delete seldom accessed information files that belong to a normal shopper. take into account the massive size of the outsourced electronic information and also the client's unnatural resource capability, the core of the matter may be generalized as however will the shopper notice associate economical thanks to perform periodical integrity verifications while not the native copy of information files. To preserve information privacy, a basic resolution is to encode information files, and so transfer the encrypted information into the cloud.

### **II. Related Work**

E. Goh, H. Shacham, N. Modadugu, and D. Boneh [4] the employment of binary is compelling in things wherever users haven't any management over the digital computer (such as Yahoo! case or the P2P file storage provided by Farsite). They believe that binary is that the most that may be done to secure associate existing network classification system while not ever-changing the digital computer or classification system protocol. Key management and revocation is easy with smallest out-of-band communication. Classification system freshness guarantees area unit supported by binary mistreatment hash tree constructions.

B. Wang, B. Li, and H. Li, [5] in this paper, we adduce Knox, a privacy-preserving auditing arrangement for aggregate abstracts with ample groups in the cloud. They advance accumulation signatures to compute analysis advice on aggregate data, so that the TPA is able to analysis the definiteness of aggregate data, but cannot acknowledge the character of the attestant on anniversary block.

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 [2] the info centers hardware and software system is what we'll decision a cloud. Once a cloud is created accessible in a very pay-as-you-go manner to the overall public, they decision it a public cloud; the service being sold is utility computing. They use the term personal cloud to check with internal knowledge centers of a business or alternative organization, not created accessible to the overall public, after they square measure massive enough to learn from the benefits of cloud computing that we have a tendency to discuss here.

Kamara and K. Lauter [3] during this paper think about the matter of building a secure cloud storage service on high of a public cloud infrastructure wherever the service supplier isn't utterly trustworthy by the client. They describe, at a high level, much architecture that mixes recent and non-standard crypto logic primitives so as to realize our goal. Survey the advantages such design would supply to each customers and repair suppliers and provides an outline of recent advances in cryptography actuated specifically by cloud storage.

A. Fiat and M. Naor [6] they introduce new theoretical measures for the qualitative and quantitative assessment of secret writing schemes designed for broadcast transmissions. The goal is to permit a central broadcast website to broadcast secure transmissions to associate capricious set of recipients whereas minimizing key management connected transmissions. They gift many schemes that permit centers to broadcast a secret to any set of privileged users out of a universe of size in order that coalitions of users not within the privileged set cannot learn the key.

### III. Existing System

In the literature study we have seen many ways that for secure information sharing in cloud computing, however most ways that did not accomplish the economical still as secure methodology for information sharing for groups. To produce the best solutions for the problems obligatory by existing ways that, recently the new methodology was given called MONA [1]. This approach presents the planning of secure information sharing theme, Mona, for dynamic groups in associate untrusted cloud. In Mona, a user is in an exceedingly position to share information with others among the cluster whereas not revealing identity privacy to the cloud. to boot, MONA supports economical user revocation and new user association. plenty of specially, economical user revocation is achieved through a public revocation list whereas not amendment the private keys of the remaining users, and new users can directly decrypt files keep among the cloud before their participation. Moreover, the storage overhead and additionally the writing computation worth square measure constant.

### IV. Proposed system

To accomplish the reliable and scalable in MONA, during this cardboard we tend to square measure presenting the new framework for MONA. During this adjustment we tend to square measure additional presenting however we tend to square measure managing the risks like abortion of accumulation administrator by accretion the number of advancement accumulation manager, blind of accumulation administrator just in case quantity of requests additional by administration the employment in different accumulation managers. This adjustment claims acceptable efficiency, quantifiability and plenty of primarily reliableness.

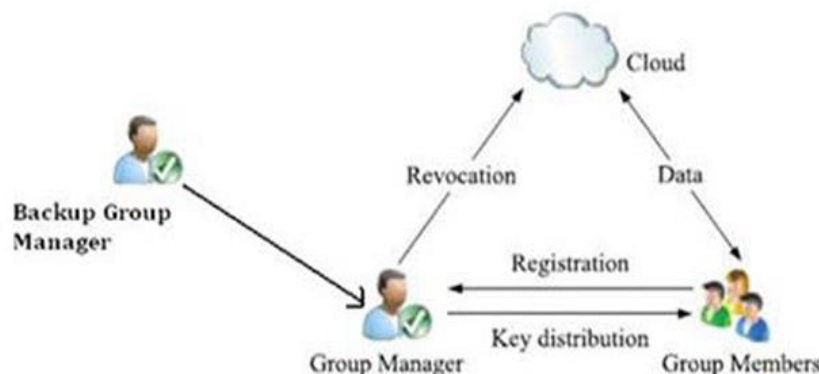


Fig. 1: Architecture

#### A. Mathematical Model

Let S be the set of proposed system

$$S = \{GM, M, C, BM\}$$

Where, GM=Group Manager M=Group members C=Cloud BM=Backup Manager

(1)

**Identify the inputs.**

$I = \{MID, RL\}$

(2)

Where, MID=Group Member ID ,RL=Revocation List

**Identify the function.**

Let F be the set of function

$F = \{F1, F2, F3, F4\}$

(3)

Where,

F1=Verify the member

F2=Generate the group signature

F3=Data encryption

F4=Taking backup

**Identify the output.**

Let O be the set of outputs

$O = \{O1, O2\}$

(4)

Where,

O1=Sharing data,O2=Accessing data

**Final Status.**

Fs = Secure data sharing with backup manager

**Failure Case.**

Fc = Revoked user accessing the file

**Constraints.**

Let  $\Phi$  be the constraints = CI

Where CI=Hiding the identity of user.

## V. Expected Results

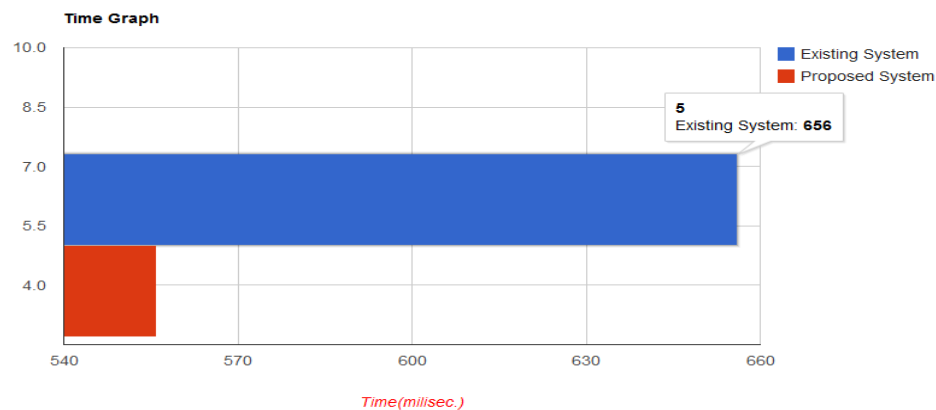


**Fig. 2: Result**

BY using R-feedback k means for proposed in this process they stored the logs if any text we are search related to that then it is used that log rather than search projects files stored place the time complexity are low as compare to existing .Fig shows the dynamically generated graph of the system. From the given graph time required to upload and download the file in the system is less as compared to previous system.

## VI. Conclusion

In conclusion, cloud computing terribly is enticing surroundings for business world in term of providing needed services during a very value effective approach. However, reassuring and enhancing security and privacy practices can attract a lot of enterprises to world of the cloud computing in so to attain the reliable and climbable in island, during this paper we have a tendency to presenting the new framework for island. In this paper, securely share the data file among the dynamic groups. Without revealing their identity members in the same group can share the data efficiently. By adding group manager execution becomes fast because if group manager fails then system may fail and stop working. So this technique is very efficient.

## References

- [1] Xuefeng Liu, Yuqing Zhang, Boyang Wang, and Jingbo Yan, "Mona: Secure Multi-Owner Data Sharing for Dynamic Groups in the Cloud", IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 24, NO. 6, JUNE 2013.
- [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] S. Kamara and K. Lauter, "Cryptographic Cloud Storage," Proc. Int'l Conf. Financial Cryptography and Data Security (FC), pp. 136- 149, Jan. 2010.
- [4] E. Goh, H. Shacham, N. Modadugu, and D. Boneh, "Sirius: Securing Remote Untrusted Storage," Proc. Network and Distributed Systems Security Symp. (NDSS), pp. 131- 145, 2003
- [5] 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, pp. 507-525, 2012.
- [6] A. Fiat and M. Naor, "Broadcast Encryption," Proc. Int'l Cryptology Conf. Advances in Cryptology (CRYPTO), pp. 480-491, 1993.
- [7] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute- Based Encryption for Fine-Grained Access Control of Encrypted Data," Proc. ACM Conf. Computer and Comm. Security (CCS), pp. 89-98, 2006.
- [8] D. Pointcheval and J. Stern, "Security Arguments for Digital Signatures and Blind Signatures," J. Cryptology, vol. 13, no. 3, pp. 361-396, 2000.
- [9] R. Lu, X. Lin, X. Liang, and X. Shen, "Secure Provenance: The Essential of Bread and Butter of Data Forensics in Cloud Computing," Proc. ACM Symp. Information, Computer and Comm. Security, pp. 282-292, 2010.

### **Acknowledgments**

I would like to thanks Prof. A. M. Wade for helping me out in selecting the topic and contents,giving valuable suggestions in preparation of paper