International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2013): 4.438

# A Survey Paper on MONA: Secure Multi-Owner Data Sharing for Dynamic Groups in the Cloud

**Kulkarni C. S.[1], A. M. Wade[2]**

[1]Pune University, Smt. Kashibai Navale College of Engineering, Pune, Maharashtra, India

[2]Professor and Guide, Smt. Kashibai Navale College of Engineering, 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 cryptological 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 encode knowledge files, so transfer the encrypted knowledge into the cloud. To resolve this downside recently the simplest economical technique Anglesey given for secured multi owner knowledge sharing in but we have a tendency to known some limitations within the same approach in terms of responsibleness and quantifiability. Therefore during this paper we have a tendency to area unit more extending the fundamental Anglesey by adding the responsibleness still as rising the quantifiability by increasing the quantity of cluster managers dynamically.***

**Keywords:** Dynamic groups, Multi owner, Data Sharing , Cloud Computing

## 1. 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.

## 2. Basic Concept

Maintaining the integrity information plays an important role within the institution of trust between data subject and repair supplier. Thoughunreal 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 [2]. CS2 provides security against the cloud supplier, shoppers square measure still in a position not solely to with efficiency access their information through a research interface however additionally to feature and delete files firmly. many security schemes for information sharing on untrusted servers are planned secure filing system designed to be bedded over insecure network and P2P file systems like NFS, CIFS, Ocean Store, and Yahoo! case.

## 3. Literature Survey

a) 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. binary contains a unique technique of activity file random access in an exceedingly science classification system while not the employment of a block server. Extensions to binary

embody giant scale cluster sharing mistreatment the NNL key revocation construction.

b) 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. With the accumulation manager's clandestine key, the aboriginal user can calmly add new users to the accumulation and acknowledge the identities of signers on all blocks. The ability of Knox is not afflicted by the amount of users in the group.

c) 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. Thus, cloud computing is that the add of SaaS and utility computing, however doesn't embody little or medium-sized knowledge centers, even though these consider virtualization for management. individuals may be users or suppliers of SaaS, or users or suppliers of utility computing. They target SaaS suppliers (cloud users) cloud suppliers, that have received less attention than SaaS users.

d) S. 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, many architectures that mix recent and non-standard cryptologic 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.

e) 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.

f) D. Pointcheval and J. Stern [8] As Explained in the Introduction, there w ere several proposals for provably defended Signature schemes. However, in all cases, the aegis was at the amount of a ample accident in agreement of efficiency. Concerning dark signatures, Damgard, Ptzmann and Waidner and added afresh at Crypto '97, Juels et al. Accept presented some dark signature schemes with a complexity-based of security. Again, the aegis y is at the amount of inefficiency. In the weaker ambience by the accidental answer model, we accept provided aegis arguments for applied and even able agenda signature schemes and dark signature schemes. On the arena of our reductions, one can absolve astute parameters, even if they are not optimal. Further improvements are accepted decidedly in the case of dark signatures area it should be accessible to access a abridgement polynomial in the admeasurement of the keys and in the amount of interactions with the signer.

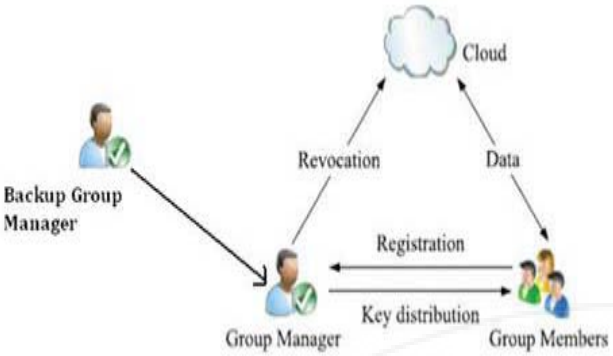
g) Lu et al. [9] proposed a defended ancestry scheme, which is congenital aloft accumulation signatures and ciphertext-policy attribute-based encryption techniques. Particularly, the arrangement in their arrangement is set with a individual attribute. Each user obtains two keys afterwards the registration: a accumulation signature key and an aspect key. Thus, any user is able to encrypt a abstracts book application attribute-based encryption and others in the accumulation can break the encrypted abstracts application their aspect keys. Meanwhile, the user signs encrypted abstracts with her accumulation signature key for aloofness attention and traceability. However, user abolishment is not accurate in their scheme.

## 4. Existing system

In the literature study we've seen several ways for secure knowledge sharing in cloud computing, but most ways didn't accomplish the economical still as secure methodology for knowledge sharing for teams. to supply the simplest solutions for the issues obligatory by existing ways, recently the new methodology was given known as Mona [1]. This approach presents the look of secure knowledge sharing theme, Mona, for dynamic teams in associate degree untrusted cloud. In Mona, a user is in a position to share knowledge with others within the cluster while not revealing identity privacy to the cloud. to boot, Mona supports economical user revocation and new user connection. a lot of specially, economical user revocation is achieved through a public revocation list while not change the non-public keys of the remaining users, and new users will directly decode files keep within the cloud before their participation. Moreover, the storage overhead and also the coding computation value are constant.

## 5. Proposed System

To accomplish the reliable and scalable in MONA, in this cardboard we are presenting the new framework for MONA. In this adjustment we are added presenting how we are managing the risks like abortion of accumulation administrator by accretion the amount of advancement accumulation manager, blind of accumulation administrator in case amount of requests added by administration the workload in assorted accumulation managers. This adjustment claims appropriate efficiency, scalability and a lot of chiefly reliability.




## 6. 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 ar presenting the new framework for island. during this technique we have a tendency to ar additional presenting however

We have a tendency to ar managing the risks like failure of cluster manager by increasing the amount of backup cluster manager, hanging of cluster manager just in case variety of requests a lot of by sharing the work in multiple cluster managers. This technique claims needed potency, measurability and most significantly responsibleness. in depth analyses show that our projected theme satisfies the specified security necessities and guarantees potency still.

## 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.