# A Survey Paper on RS-MONA: Reliable and Scalable Approach for Secure Multi-Owner Data Sharing for Dynamic Groups in the Cloud

**Miss. Sunita R. Patil**
*Dr D.Y. Patil College of Engineering, Ambi, Talegaon.*
*University Of Pune, Pune, India.*

**Asst. Prof. Yogesh Sayaji**
*Dr. D.Y. Patil College of Engineering, Ambi, Talegaon.*
*University Of Pune, Pune, India.*

## Abstract

*In Today's world Cloud Computing which moves the application software and databases to the centralized large data centers, where the management of the data and services may not be fully trustworthy. Several trends are opening up the era of Cloud Computing, which is an Internet-based development and use of computer technology. One of the biggest concerns with cloud data storage is that of data integrity verification at untrusted servers. To preserve data privacy, a basic solution is to encrypt data files, and then upload the encrypted data into the cloud. To resolve this problem recently the best efficient method MONA presented for secured multi owner data sharing in however we identified some limitations in the same approach in terms of reliability and scalability. Hence in this paper we are further extending the basic MONA by adding the reliability as well as improving the scalability by increasing the number of group managers dynamically.*

*Keywords– Cloud Computing, dynamic groups, data sharing, reliability, integrity, scalability.*

## 1. Introduction

A) What is cloud computing?

Cloud computing is one of the greatest platform which provides storage of data in very lower cost and available for all time over the internet Cloud computing is Internet-based computing, whereby shared resources, software and information are provided to computers and devices on demand. Several trends are opening up the era of Cloud Computing, which is an Internet-based development and use of computer technology. Cloud computing means more than simply saving on IT implementation costs. Cloud offers enormous opportunity for new innovation, and even disruption of entire industries. Cloud computing is the long dreamed vision of computing as a utility, where data owners can remotely store their data in the cloud to enjoy on-demand high-quality applications and services from a shared pool of configurable computing resources.

B) Basic Concept

Maintaining the integrity of data plays a vital role in the establishment of trust between data subject and service provider. Although envisioned as a promising service platform for the Internet, the new data storage paradigm in "Cloud" brings about many challenging design issues which have profound influence on the security and performance of the overall system. One of the biggest concerns with cloud data storage is that of data integrity verification at untrusted servers. What is more serious is that for saving money and storage space the service provider might neglect to keep or deliberately delete rarely accessed data files which belong to an ordinary client. Consider the large size of the outsourced electronic data and the client's constrained resource capability, the core of the problem can be generalized as how can the client find an efficient way to perform periodical integrity verifications without the local copy of data files. To preserve data privacy, a basic solution is to encrypt data files, and then upload the encrypted data into the cloud [2]. CS2 provides security against the cloud provider, clients are still able not only to efficiently access their data through a search interface but also to add and delete files securely.

Several security schemes for data sharing on untrusted servers have been proposed secure file system designed to be layered over insecure network and P2P file systems such as NFS, CIFS, Ocean Store, and Yahoo! Briefcase.

### C) Advantages and Disadvantages of Cloud Computing:

Advantages:-

- 24/7 Support
- Easy to Maintain.
- Secure Storage and Management
- Location Independent
- Less cost (Pay-as-per-you-Use).
- High level computing
- Personalized Backup and recovery.
- Remote access.
- Green computing.

Disadvantages:-

- Lack of control
- Security and privacy.
- Higher operational cost.
- Reliability

## 2. Literature Survey

In the literature survey we are going to discuss some existing technique for cloud.

a) 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 data centers hardware and software is what we will call a cloud. When a cloud is made available in a pay-as-you-go manner to the general public, they call it a public cloud; the service being sold is utility computing. They use the term private cloud to refer to internal data centers of a business or other organization, not made available to the general public, when they are large enough to benefit from the advantages of cloud computing that we discuss here. Thus, cloud computing is the sum of SaaS and utility computing, but does not include small or medium-sized data centers, even if these rely on virtualization for management. People can be users or providers of SaaS, or users or providers of utility computing. They focus on SaaS providers (cloud users) and cloud providers, which have received less attention than SaaS users.

b) S. Kamara and K. Lauter [3] in this paper consider the problem of building a secure cloud storage service on top of a public cloud infrastructure where the service provider is not completely trusted by the customer. They describe, at a high level, several architectures that combine recent and non-standard cryptographic primitives in order to achieve our goal. Survey the benefits such architecture would provide to both customers and service providers and give an overview of recent advances in cryptography motivated specifically by cloud storage.

c) S. Yu, C. Wang, K. Ren, and W. Lou [4] This paper addresses this challenging open issue by, on one hand, defining and enforcing access policies based on data attributes, and, on the other hand, allowing the data owner to delegate most of the computation tasks involved in fine-grained data access control to untrusted cloud servers without disclosing the underlying data contents. They achieve this goal by exploiting and uniquely combining techniques of attribute-based encryption (ABE), proxy re-encryption, and lazy re-encryption. Proposed scheme also has salient properties of user access privilege confidentiality and user secret key accountability.

d) E. Goh, H. Shacham, N. Modadugu, and D. Boneh [5] the use of SiRiUS is compelling in situations where users have no control over the file server (such as Yahoo! Briefcase or the P2P file storage provided by Farsite). They believe that SiRiUS is the most that can be done to secure an existing network file system without changing the file server or file system protocol. Key management and revocation is simple with minimal out-of-band communication. File system freshness guarantees are supported by SiRiUS using hash tree constructions. SiRiUS contains a novel method of performing file random access in a cryptographic file system without the use of a block server. Extensions to SiRiUS include large scale group sharing using the NNL key revocation construction.

e)R. Lu, X. Lin, X. Liang, and X. Shen [6] in this paper secure provenance is of paramount importance to the flourish of cloud computing, yet it is still challenging today. In this paper, They formally defined the secure provenance and the corresponding security model in cloud computing. Then, in proposed a concrete secure provenance SP scheme based on the bilinear pairings, and used the provable security technique to prove its security in the standard model. Due to its comprehensive security features, the proposed SP scheme provides trusted evidences for data forensics in cloud computing and thus pushes the cloud computing for wide acceptance to the public.

f) B. Waters [7] presented the first cipher text-policy attribute-based encryption systems that are efficient, expressive, and provably secure under concrete assumptions. All of our constructions fall under a common methodology of embedding an LSSS challenge matrix directly into the public parameters. Our constructions provide a trade off in terms of efficiency and the complexity of assumptions.

g) V. Goyal, O. Pandey, A. Sahai, and B. Waters [8] they develop a new cryptosystem for One-grained sharing of encrypted data that call Key-Policy Attribute-Based Encryption (KP-ABE). In cryptosystem, cipher texts are labelled with sets of attributes and private keys are associated with access structures that control which cipher texts a user is able to decrypt. They demonstrate the applicability of our construction to sharing of audit-log information and broadcast encryption. Our construction supports delegation of private keys which subsumes Hierarchical Identity-Based Encryption (HIBE).

h) A. Fiat and M. Naor [9] they introduce new theoretical measures for the qualitative and quantitative assessment of encryption schemes designed for broadcast transmissions. The goal is to allow a central broadcast site to broadcast secure transmissions to an arbitrary set of recipients while minimizing key management related transmissions. They present several schemes that allow centers to broadcast a secret to any subset of privileged users out of a universe of size so that coalitions of users not in the privileged set cannot learn the secret.

i)B. Wang, B. Li, and H. Li, [10] in this paper, we propose Knox, a privacy-preserving auditing scheme for shared data with large groups in the cloud. They utilize group signatures to compute verification information on shared data, so that the TPA is able to audit the correctness of shared data, but cannot reveal the identity o f the signer on each block. With the group manager's private key, the original user can efficiently add new users to the group and disclose the identities of signers on all blocks. The efficiency of Knox is not affected by the number of users in the group.

j) D. Pointcheval and J. Stern [11] As Explained in the Introduction, there w ere several proposals for pro v ably secure Signature schemes. However, in all cases, the security was at the cost of a considerable loss in terms of efficiency. Concerning blind signatures, Damgard, Ptzmann and Waidner and more recently at Crypto '97, Juels et al. Have presented some blind signature schemes with a complexity-based of security. Again, the security y is at the cost of inefficiency. In the weaker setting by the random oracle model, we have provided security arguments for practical and even efficient digital signature schemes and blind signature schemes. On the ground of our reductions, one can justify realistic parameters, even if they are not optimal. Further improvements are expected particularly in the case of blind signatures where it should be possible to obtain a reduction polynomial in the size of the keys and in the number of interactions with the signer

## 3 Existing System

In the literature study we have seen many methods for secure data sharing in cloud computing, however most methods failed to achieve the efficient as well as secure method for data sharing for groups. To provide the best solutions for the problems imposed by existing methods, recently the new method was presented called MONA [1]. This approach presents the design of secure data sharing scheme, Mona, for dynamic groups in an untrusted cloud. In Mona, a user is able to share data with others in the group without revealing identity privacy to the cloud. Additionally, Mona supports efficient user revocation and new user joining. More specially, efficient user revocation can be achieved through a public revocation list without updating the private keys of the remaining users, and new users can directly decrypt files stored in the cloud before their participation. Moreover, the storage overhead and the encryption computation cost are constant. Therefore practically in all cases MONA outperforms the existing methods.

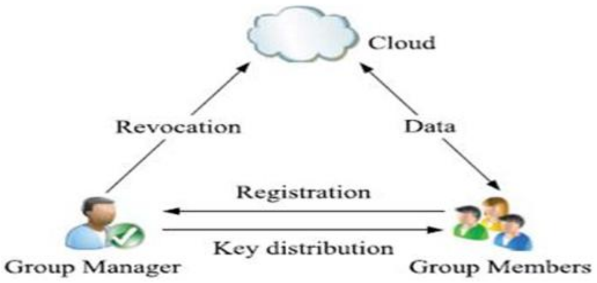

Fig 3.1 Existing System Model

## 3.1 Disadvantages of Existing System

However as per reliability and scalability concern this method needs to be workout further as if the group manager stop working due to large number of requests coming from different groups of owners, then entire security system of MONA failed down.

## 4 Proposed Solution

Thus to achieve the reliable and scalable MONA approach, in this project we are presenting the new framework for MONA called as RS-MONA (Reliable Scalable-MONA). In this method we are further presenting how we are managing the risks like failure of group manager by increasing the number of backup group manager, hanging of group manager in case number of requests more by sharing the workload in multiple group managers. This method claims required efficiency, scalability and most importantly reliability.

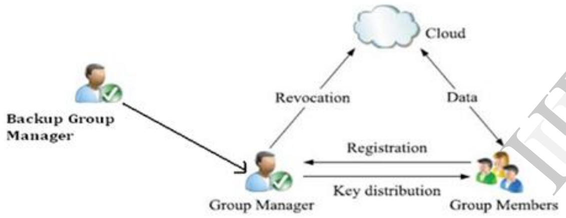

Fig 4.1 Proposed System Model

## 4.1Advantage of Proposed System

To overcome the disadvantage of existing system MONA, the proposed RS-MONA is if the group manager stop working due to large number of requests coming from different groups of owners, then backup group manager will remains available.

## 5 System Requirement & Specification

### 5.1 Software Requirements:

Front End: Java
Tools Used: Eclipse/Net beans
Operating System: Windows 7

### 5.2 Hardware Requirements:

Processor: Pentium IV 2.6 GHz
Ram: 512 Mb
Monitor: 15” Colour
Hard Disk: 20 Gb
Floppy Drive: 1.44 Mb
Keyboard: Standard 102 Keys
Mouse: 3 Button

## 6. Conclusions

In conclusion, cloud computing is very attractive environment for business world in term of providing required services in a very cost effective way. However, assuring and enhancing security and privacy practices will attract more enterprises to world of the cloud computing In Thus to achieve the reliable and scalable MONA approach; in this paper we are presenting the new framework for MONA called as RS-MONA (Reliable Scalable-MONA). In this method we are further presenting how we are managing the risks like failure of group manager by increasing the number of backup group manager, hanging of group manager in case number of requests more by sharing the workload in multiple group managers. This method claims required efficiency, scalability and most importantly reliability. Extensive analyses show that our proposed scheme satisfies the desired security requirements and guarantees efficiency as well.

## 7 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] S. Yu, C. Wang, K. Ren, and W. Lou, “Achieving Secure, Scalable, and Fine-Grained Data Access Control in Cloud Computing,” Proc. IEEE INFOCOM, pp. 534-542, 2010.
[5] 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.
[6]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.
[7] B. Waters, “Cipher text-Policy Attribute-Based Encryption: An Expressive, Efficient, and Provably Secure Realization,” Proc. Int’l Conf. Practice and Theory in Public

Key Cryptography Conf. Public Key Cryptography, http://eprint.iacr.org/2008/290.pdf, 2008.

[8] 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.

[9] A. Fiat and M. Naor, "Broadcast Encryption," Proc. Int'l Cryptology Conf. Advances in Cryptology (CRYPTO), pp. 480-491, 1993.

[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, pp. 507-525, 2012.

[11] D. Pointcheval and J. Stern, "Security Arguments for Digital Signatures and Blind Signatures," J. Cryptology, vol. 13, no. 3, pp. 361-396, 2000.