Volume 4, Issue 5, May 2014 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Reliable and Scalable approach to Store and Share Sensitive Data for Dynamic Groups in the Cloud

Mrs. Sunita R. Patil(PG Scholar)
Department of Computer Engineering
Dr.D.Y.Patil College of Engineering,
Ambi, Talegaon, Pune, India.
University Of Pune

Assit. Prof. Sandeep Kadam
Department of Computer Engineering
Dr.D.Y.Patil College of Engineering,
Ambi, Talegaon, Pune, India
University Of Pune

Abstract—In Today's world cloud computing is very attractive environment for business world in term of providing required services in a very low cost where the management of the data and services may not be fully honest. One of the biggest concerns with cloud data storage is that of data integrity verification at untrusted servers. Several methods are opening up the period of Cloud Computing, which is an Internet-based development and use of computer technology .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. So in this method we are added extending the basic MONA by adding the reliability as well as improving the scalability by growing the number of group managers dynamically. 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, sagging of group manager in case number of requests more by sharing the workload in group managers. This method claims required efficiency, security, scalability and most importantly reliability.

Keywords— Cloud Computing; reliability; integrity; scalability; efficiency;

I. INTRODUCTION

In Cloud computing Storing data on remote cloud storage makes the maintenance affordable by data owners. The reliability and trustworthiness of these remote storage locations is the main concern for data owners and cloud service providers. When multiple data owners are involved, the aspects of membership and data sharing need to be addressed. 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.

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. With cloud computing and storage, users are able to access and to share resources offered by cloud service providers at a lower marginal cost.

With Dropbox, for example, data is stored in the cloud (operated by Amazon), and shared among a group of users in a collaborative manner. It is natural for users to wonder whether their data remain intact over a prolonged period of time. The Privacy of data stored in the cloud can become compromised. To protect the privacy of data in the cloud and to offer "peace of 653mind" to users, it is best to encrypt the data files and then upload the encrypted data into the cloud [2]. 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.

II. LITERATURE SURVEY

- **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.
- **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.
- **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.
- **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.
- **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.
- **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.
- **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 labeled 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).
- **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.
- **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.
- **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.

Table 1: Comparisons of different Methods

Sr.no	Method	Year	Parameter	Service provide	Performance
1	Encryption scheme	1993	Encryption algorithm	Designed for broadcast transmission	Minimizing key management
2	Sirius	2003	Hash tree	Key management and revocation is simple	Secure for only network file system
3	KP-ABE key policy attribute-based exceptions	2006	Private key	Supports allocation of private keys	Demonstrate sharing audit log information and broadcast encryption
4	Cryptographic Primitive	Jan-2010	Secure cloud	Data Storage	Beneficial for Customer and service Provider only
5	SAAS	April-2010	Public cloud	Utility cloud	Less attention
6	Attribute based Encryption(A BE)	2010	Proxy re-encryption	User access and user secret key confidential	Good for only untrusted cloud
7	Knox(privac y-preserving auditing scheme for shared data)	2012	Used group signatures	Efficiently add new users to the group	efficiency is not affected by number of users in the group

III. PROPOSED METHOD AND DESIGN

3.1 Problem Definition

In the literature study we have seen several approaches for secure data sharing in cloud computing, however most methods failed to accomplish the efficient as well as secure method for data sharing for groups. To provide good solutions for the problems forced by existing methods, recently the new method was presented called MONA [1]. This technique presents the design of secure data sharing scheme, Mona, for dynamic groups in an untrusted cloud.

In Mona, a user may share data with others in the group without revealing identity secrecy to the cloud. Additionally, Mona supports and new user joining and efficient user revocation. More specially, efficient user revocation can be achieved through a public revocation list without updating the private keys of remaining users, and new users can directly decrypt files stored in the cloud before their participation. Thus practically in all cases MONA outperforms the existing methods. However as per reliability and scalability concern this method needs to be test further as if the group manager stop working due to large number of requests coming from dissimilar groups of owners, then entire security system of MONA failed down. Following figure 1 is showing the current architecture of MONA.

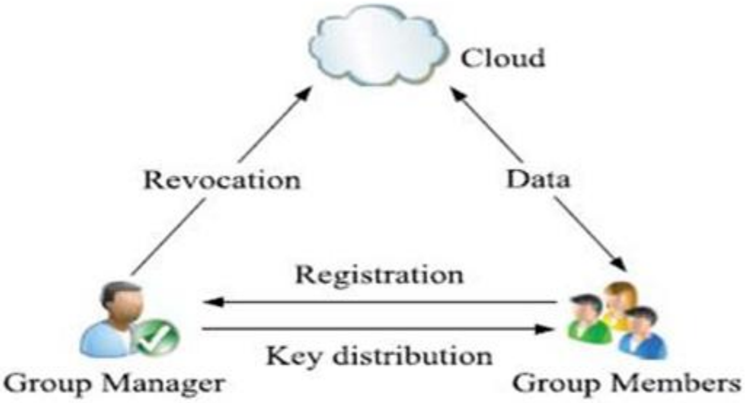


Fig 1. Existing System Model

3.2 Proposed Architecture and Design: RS-MONA

Thus to achieve the reliable and scalable MONA approach, in this project we are proposing 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 growing the number of backup group manager, sagging of group manager in case number of requests more by sharing the workload in group managers. This technique claims required efficiency, scalability , security and most importantly reliability. Following figure 2 and 3 are showing the proposed design and implementation flow respectively.

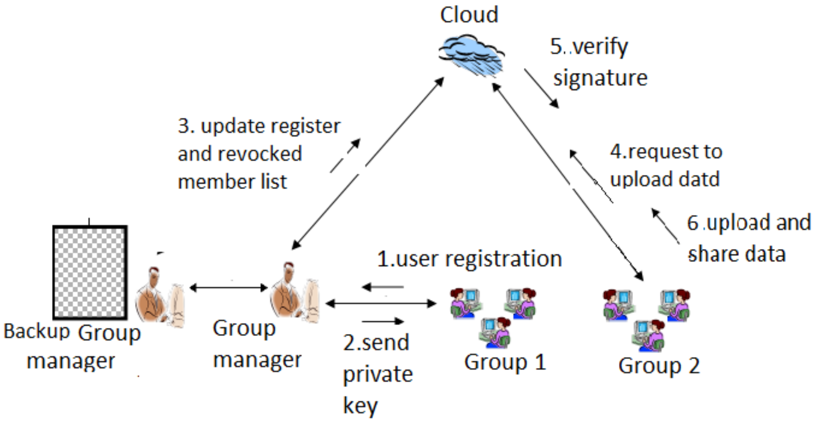


Fig.2 Proposed System Architecture

The system model consists of four different entities: as illustrated in below Figure, the backup group manager, a group manager (i.e., the company manager),cloud, and a large number of group members (i.e., the staffs) .Cloud is operated by CSPs and provides priced abundant storage services. However, the cloud is not fully trusted by users since the CSPs are very likely to be outside of the cloud users' trusted domain. Group manager takes charge of system parameters generation, user registration, user revocation, and revealing the real identity of a dispute data owner. Group members are a set of registered users that will store their reserved data into the cloud server and share them with others in the group. .

IV. SCHEME DESCRIPTION

My proposed system consists following entities and techniques:

4.1) System Setup: System initialization can be done by creating a cloud architecture in which data owner creates an account with cloud server. Further, more users can join with data owner to share files. This is possible through making a request to data owner. During registration process users need to fill their personal information which will be evaluated by data owner to provide an approval for data access in cloud. Once, user got registered with the cloud system, he is free to access any file until life time expiry or revocation on the basis of request. Initially, Data Owner collects attributes relevant to the data file units and are encrypted, then uploaded to cloud server. Policy engine used in the system automatically runs and generates access structure of the data file. Also, generates user's public key. Once the access structure satisfies the attributes given by the user the decrypted file can be downloaded by them.

4.2) User Registration: After successful creation of cloud setup, users need to get registered with the system through user registration process. While registering, users need to submit their personal details for completion of registration process. But, the system guarantees Identity privacy. During registration process, user got unique identity *I* and access structure *T*. This generates secret key S_k for I. Data file *F* can be then encrypted by using *I*'s Public Key *Pk* to generate Cipher text *C*.

4.3) User Revocation: User revocation is the process of removal of user from system user list which is performed by Data Owner. The system keeps Revocation List (RL) for each attributes. For the user to be revoked, his access structure is removed from RL, so that they can't have more access to cloud.

4.4) File Upload: Before uploading files, Data Owner assign File identity *ID* to selected data files and then encrypts file using his public key *Pk.* Along with encryption attributes for encryption is added.

4.5) File Access: Users can access data files if they have valid secret key. While accessing files, user's secret key is validated against access structure of the user. If it satisfies user's access structure, decrypted data file can be downloaded by Data Consumer.

4.6)File Deletion: This operation can be performed by Data Owners, if they no longer needed that files. For file deletion, Data Owner wants to provide File Identifier along with secret key. If owner's signature is verified successfully then cloud server positively deletes the file with specified identity.

V. ALGORITHMS USED

For implementation 3 algorithms are used, details given in below.

Algorithm 1: Signature Generation

Step 1: Input Private key (A, x), and System parameter (P, U, V, H,W) And data M.
Step 2: Select random numbers
Step 3: Set $\delta 1$ and $\delta 1$ Computes the following values

```
        T1,T2 ,T3 ,R1,R2,R3,R4,R5
Step 4:   Set c =f(M;T1; T2; T3;R1;R2;R3;R4;R5) Construct the following numbers
                    $s_{\alpha,} s_{\beta,} s_{x,} s_{\delta1,} s_{\delta1}$
Step 5:   Return$\sigma$ = (T1, T2, T3, c,$s_{\alpha,} s_{\beta,} s_{x,} s_{\delta1,} s_{\delta1}$)
Step 6: Generate a valid group signature on M.
```

Algorithm 2: Signature Verification

```
Step 1: Set System parameter (P, U, V, H, W) and
                    Signature $\sigma$ = (T1, T2, T3, c,$s_{\alpha,} s_{\beta,} s_{x,} s_{\delta1,} s_{\delta1}$)
Step 2: Compute the Following value.
                    $\widetilde{R1}, \widetilde{R2}, \widetilde{R3}, \widetilde{R4}, \widetilde{R5}$
Step 3: if c = f (M, T1,T2, T3,$\widetilde{R1}, \widetilde{R2}, \widetilde{R3}, \widetilde{R4}, \widetilde{R5}$)
                    Return true
Step 4: else
                    Return false
```

Algorithm 3: Revocation Verification

```
Step 1: Input System Parameter (H0,H1,H2), Group signature $\sigma$ and set of revocation  Key A1,…,Ar
Step 2: set temp = e (T1,H1)e(T2,H2)
Step 3: for   i=1 to n
                    If e (T3 – Ai,H0) == temp
                            Return valid
                            End if
                        End for
                Return invalid
```

VI. SYSTEM REQUIREMENT SPECIFICATION

6.1. Input: Data (files) for sharing.

6.2 Software Requirements:

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

6.3. 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

VII. RESULTS

7.1 Practical Result

Practical implementation’s results are shown in following diagrams. Fig.4 shows main screen of project. the list file presented on system are given in this main screen.

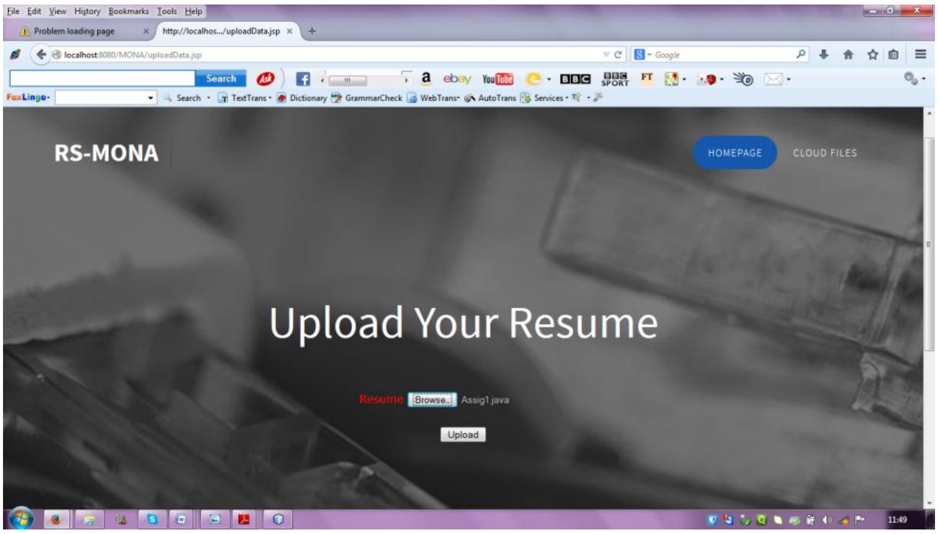
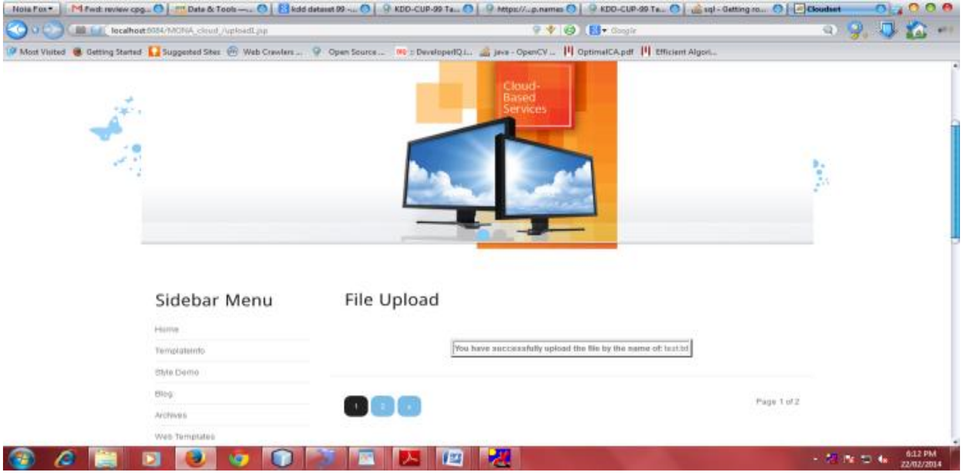


Fig.3 Select file for uploading

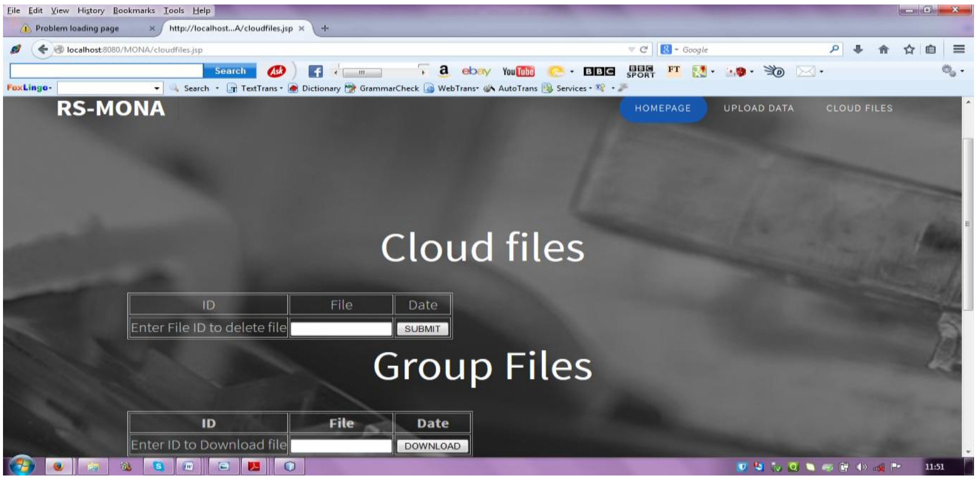


Sidebar Menu

File Upload

You have successfully upload the file by the name of: test.txt

Fig.4 File Successfully Uploaded



Cloud files

ID	File	Date
Enter File ID to delete file		

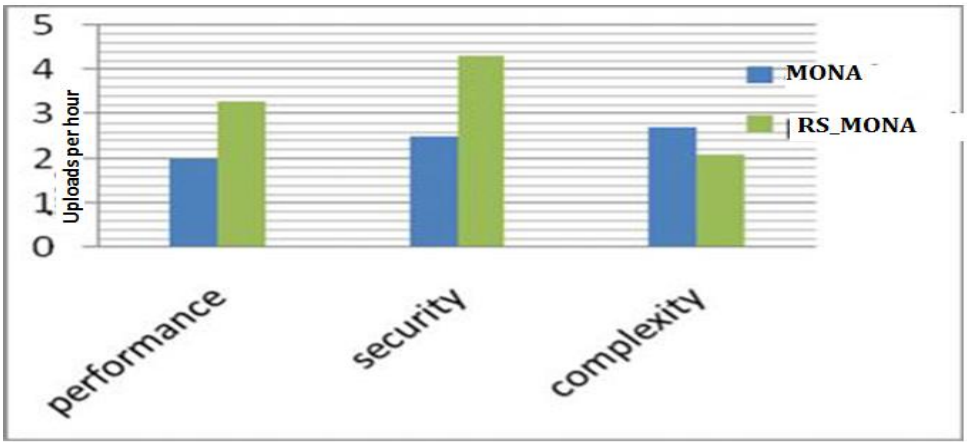
Group Files

ID	File	Date
Enter ID to Download file		

Fig.5 Shows Cloud & Group files

VIII. PROPOSED MODEL (RS-MONA) EVALUATION

In this section we present the performance report of our proposed model with the existing model. The below graph describes the performance, security and complexity attributes of the proposed model.



8.1 Performance:
The performance of proposed system is more compare to existing one, because in proposed system if group manager fail then backup group manager will remains present all time . So the performance of the proposed system is high.

8.2 Security: The security of proposed system is high compare to existing one. Since the group members only recognise the secret key. Suppose an unfamiliar person enter into group he does not discover the secret key i.e. the user enters into group authorise that he must be a group member.

8.3 Complexity: The complexity of proposed system is low compare to existing one. Because the new user does not concern about getting the secret key i.e. the new user does not depend on the remaining group members. The new user openly communicates with group key manager and acquires the secret key. The encryption and decryption of file also take less time.

IX. COMPARATIVE GRAPH

We list the comparison on computation cost of clients for data generation operations between Mona and original dynamic broadcast encryption (ODBE) with our proposed approach (RS-MONA). It is easily observed that the computation cost of proposed system is better than Mona; Mona is irrelevant to the number of revoked users.

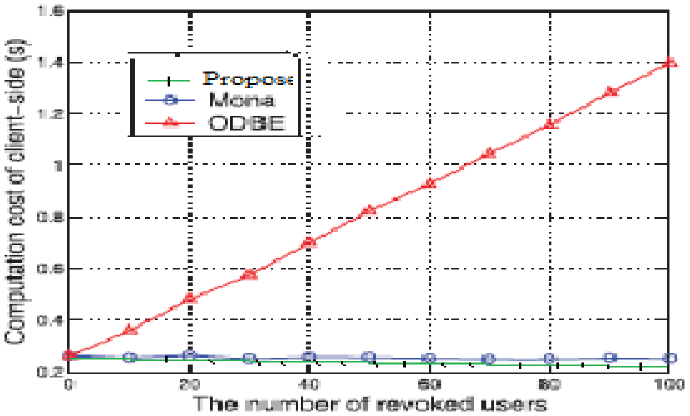


Fig 6: Comparison Cost Computation.

X. CONCLUSION AND FUTURE WORK

In conclusion, cloud computing is very good atmosphere for business world in term of providing essential facilities in a very cost effective way. However, promising and attractive safety and privacy practices will attract more enterprises to world of the cloud computing. In Thus to accomplish the reliable and scalable MONA approach; in this paper we are presenting the new creation for MONA called as RS-MONA (Reliable Scalable-MONA). In this method we are in addition presenting how we are managing the hazards like failure of group manager by growing the number of backup group manager, sagging of group manager in case number of requests more by sharing the workload in group managers. This method claims required efficiency, security, scalability and most importantly reliability. Extensive studies show that our proposed scheme satisfies the desired security necessities and assurances efficiency as well.

ACKNOWLEDGEMENT

I would like to express my gratitude to all those who gave me the possibility to complete this project. I deeply indebted to my project guide Prof. Sandip Kadam whose help, stimulating suggestion and encouragement helped me in the all time. I have furthermore to thank to all staff member, ME, PG Coordinator Prof. Anupkumar Bongale, who gave and confirmed this permission and encouraged me to go ahead with my project.

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.