RS-MONA: Reliable and Scalable Secure Method to Store and Share Secrete Data for Groups in Cloud

Sunita R. Patil
Dr.D.Y.Patil College of Engg.
Ambi,Talegaon,Pune.
University of Pune

Sandeep Kadam
Dr.D.Y.Patil College of Engg.
Ambi,Talegaon,Pune.
University of Pune

ABSTRACT
This paper presents various issues related to privacy and security while storing user's data on untrusted cloud. In today's world Sharing of group resource among the cloud users is a major problem. There is a lot of research being made to find out the issues with these cloud service providers and cloud security in general. In this paper system proposes a secure multi-owner data sharing scheme, for dynamic group in the cloud. By providing group signature and encryption techniques, any cloud user can securely share data with others. The main objective of this paper include: to provide security for dynamic group system integrates Image based authentication and one time password (OTP) to achieve high level of security. In addition system identified some limitations in the same approach in terms of reliability and scalability .To resolve the drawbacksystem extends the basic MONA by adding the reliability as well as improving the scalability by growing the backup group managers dynamically. In this method System further presenting how system manage 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 .This method claims required reliability ,security,scalability and most importantly efficiency..

Keywords
Cloud Computing; reliability; integrity;one time password; authentication;

1. INTRODUCTION
Security is essential element for strong privacy in all online computing scenarios, but security only is not enough. Customers and businesses are ready to use online computing only if they have the confidence that their data will stay private and secure. So to create a trusted environment for customers, there is need to develop software, processes and services with privacy in intelligence.

1.1 Basic Concept
At present world Cloud Computing which moves the application software and databases to the centralized large data centers, where the management of the information and services may not be completely trustworthy. Some trends are opening up the period of Cloud Computing, which is an Internet-based improvement and utilize of computer technology. One of the largest concerns with cloud data storage is that of data integrity authentication at untrusted servers. Let us consider a practical data application. A department allows its staffs in the same group to store and share files in the cloud. However, it also poses a significant risk to the confidentiality of those stored files. Explicitly, the cloud servers managed by cloud providers are not fully trusted by users while the data files stored in the cloud may be sensitive and confidential, such as business plans, important papers. To protect data privacy, a basic answer is to encrypt data files, and then upload the encrypted data into the cloud.

Identity privacy is one of the important obstacles for the wide deployment of cloud computing. Without the assurance of identity privacy, users may be unwilling to join in cloud computing systems because their real identities could be easily disclosed to cloud providers and attackers. On the other hand, unconditional identity privacy may incur the abuse of privacy. For example, a misbehaved staff can mislead others in the department by sharing false files without being traceable. Therefore, traceability, which enables the group manager (e.g., a manager of firm, HOD, Team leader) to reveal the real identity of a user, is also highly desirable. Second, it is highly possible that any member in a group should be able to fully enjoy the data storing and sharing services provided by the cloud, which is defined as the multiple-owner manner. Compared with the single-owner manner [3], where only the group manager can store and modify data in the cloud, the multiple-owner manner is more flexible in practical applications.

More concretely, each user in the group is able to not only read data, but also modify his/her part of data in the entire data file shared by the company. Last but not least, groups are normally dynamic in practice, e.g., new staff participation and current staff revocation in a department. On the other hand, an efficient membership revocation mechanism without updating the secret keys of the remaining users is also desired to minimize the complexity of key management. Several security schemes for data sharing untrusted servers have been proposed [4], [5], [6]. In these approaches, data owners store the encrypted data files in untrusted storage and distribute the corresponding decryption keys only to authorized users. Thus, unauthorized users as well as storage servers cannot learn the content of the data files because they have no knowledge of the decryption keys.

1.2 Advantages and Disadvantages of CloudComputing:
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 this section system presenting the different methods those are presented to solve the problem cloud data security.

[1]"Mona: Secure Multi-Owner Data Sharing for Dynamic Groups in the Cloud" by Xuefeng Liu, Yuqing Zhang, Boyang Wang, and Jingbo Yan -
Extracting idea for Dissertation: -From this paper proposed system referred the concept of efficient user revocation and new user joining in groups. Also system referred the detailed concept of signature generation and revocation verification algorithm.

[2]"A View of Cloud Computing" by 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
Extracting idea for Dissertation: -From this paper proposed system referred the concept of public cloud, as it provide SaaS and utility computing.

[3]"Cryptographic Cloud Storage," by S. Kamara and K. Lauter
Extracting idea for Dissertation: - Fromthis paper proposed system referred concept of cryptography,as it beneficial for Customer and service Provider.

[4]"Achieving Secure, Scalable, and Fine-Grained Data Access Control in Cloud Computing," by S. Yu, C. Wang, K. Ren, and W. Lou
Extracting idea for Dissertation: -From this paper proposed system referred concept of SP scheme, as it provides trusted evidences for data forensics in cloud computing.

[5]"Sirius: Securing Remote Untrusted Storage," by E. Goh, H. Shacham, N. Modadugu, and D. Boneh
Extracting idea for Dissertation: -From this paper proposed system referred concept of SiRiUS, as it Secure for network file system and Key management and revocation is simple.

[6]"Secure Provenance: The Essential of Bread and Butter of Data Forensics in Cloud Computing," byR. Lu, X. Lin, X. Liang, and X. Shen
Extracting idea for Dissertation: -From this paper proposed system referred concept of SP scheme, as it provides trusted evidences for data forensics in cloud computing.

[7]"Ciphertext-Policy Attribute-Based Encryption: An Expressive, Efficient, and Provably Secure Realization," by B. Waters
Extracting idea for Dissertation: -From this paper proposed system referred concept of Cipher text-Policy ABE, as it efficient, expressive, and provably secure.

[8] "Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data," by V. Goyal, O. Pandey, A. Sahai, and B. Waters
Extracting idea for Dissertation: -From this paper proposed system referred concept of KP-ABE key policy attribute-based encryption, as it demonstrate sharing audit log information and broadcast encryption

[9] "Broadcast Encryption" byFiat and M. Naor
Extracting idea for Dissertation: -From this paper proposed system referred concept of broadcast Encryption, as it allow a central broadcast site to broadcast secure transmissions to an arbitrary set of recipients while minimizing key management related transmissions.

[10] "Knox: Privacy-Preserving Auditing for Shared Data with Large Groups in the Cloud" byB. Wang, B. Li, and H. Li
Extracting idea for Dissertation: -From this paper proposed system referred concept ofKnox, as it shared data with large groups in the cloud. Also utilize group signatures to compute verification information on shared data.

[11]"Security Arguments for Digital Signatures and Blind Signatures" by D. Pointcheval and J. Stern
Extracting idea for Dissertation: -From this paper proposed system referred concept of digital signatures, as it efficiently add new users to the group and disclose the identities of signers on all blocks.

[12]Three level security system for dynamics group in cloud" by V.Sathana, J.Shanthini
Extracting idea for Dissertation: -From this paper proposed system referred concept ofOne-Time Passwords, asit is secure and stronger forms of authentication and provide three level of security.

3. PROPOSED ARCHITECTURE

3.1 Problem Definition

In the literature study this paper have seen many methods for protective data sharing in cloud computing, although most methods failed to achieve the efficient as well as secure method for data sharing for groups. To afford the best solutions for the problems imposed by existing methods, recently the new method was presented called MONA [1]. This method presents the design of secure data sharing scheme, Mona, for dynamic groups in an untrusted cloud. However as per reliability and scalability concern this method needs to be exercises further as if the group manager stop working due to huge number of requests coming from different groups of owners, then entire security system of MONA failed down. In addition it is required to increase security of MONA, to prevent from Shoulder attack and Brute-force attack at the client side.

3.2 Proposed Solution

The major function of the paper is to solve the challenges presented above, this paper propose a reliable, scalable and secure multi-owner data sharing scheme for dynamic group in the cloud. The main contributions of this paper include:

- To provide security for dynamic group system integrates Image based authentication and one time password to achieve high level of security.
- However existing system identified some limitations in the same approach in terms of reliability and scalability. Hence this paper furtherextends the basic MONA by adding the reliability as well as improving the scalability by taking backup of group managers dynamically.
- In addition, this paper analyzes the security with rigorous proofs. One-Time Password is one of the easiest and most popular forms of authentication that can be used for securing access to accounts. One-Time Passwords are often referred to as secure and stronger forms of authentication, and allowing them to install across multiple machines.
- This paper provides a multiple levels of security to share data among multi-owner manner. First the user selects the pre-selected image to login.Then

selects an image from the grid of images. Then OTP is generated automatically.

Following figure 2 are showing the proposed design and implementation flow respectively.

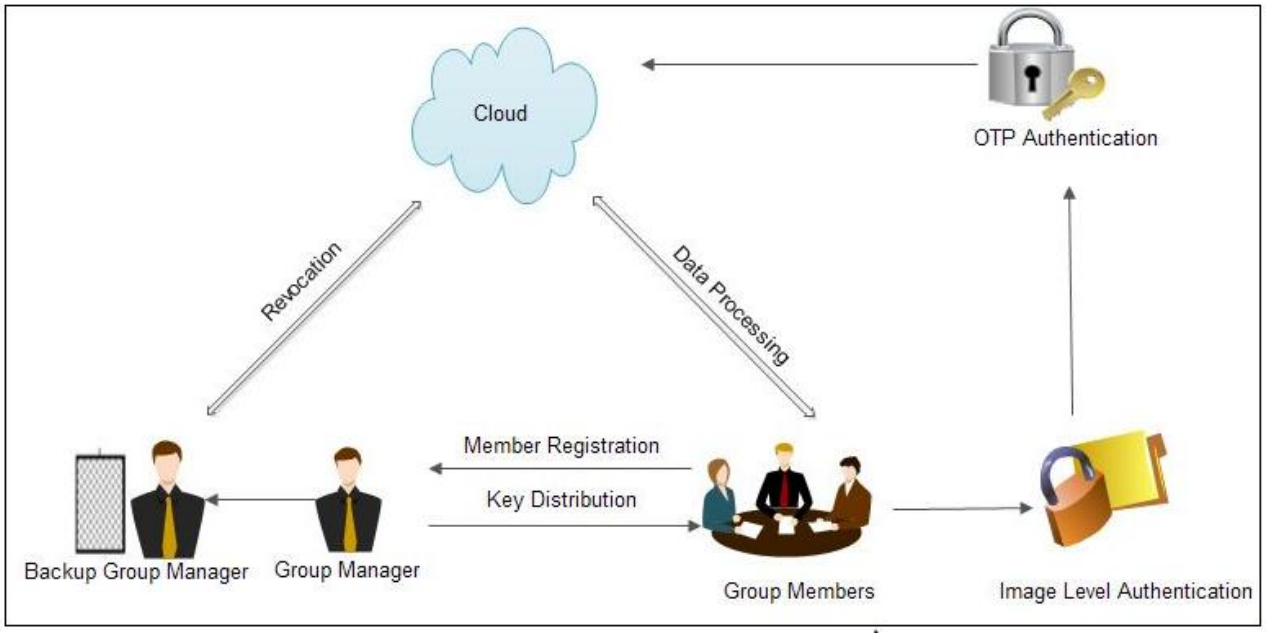

Fig 1: Proposed System Architecture

The system model consists of four different entities the backup group manager, a group manager (i.e., the Firm manager), cloud, and a large number of group members (i.e. the employee) .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 members are used three levels of security (Text Level, Image Level, and OTP) at the time of registration.

Level 1: Level 1 security provides a simple text based password.
Level 2: In this security level the user has to select an image from the set of images. It can reduce shoulder attack and Brute-Force attack.
Level 3: After the successful entry of the above two levels, The Level 3 Security System will then generate a one-time Password(OTP).
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.

4. ALGORITHMIC STRATEGY

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

- Algorithm 1: Signature Generation
- Algorithm 2: Signature Verification
- Algorithm 3: Revocation Verification

4.1 Signature Generation

Input: Private key(A,x), System parameter (P,U,V,H,W) anddata M.

Algorithm:

1.1 Begin
1.2 Select random numbers
1.3 Set $\delta 1 = x\alpha$ and $\delta 2 = x\beta$
1.4 Computes the following values
1.5 $T1 = \alpha .U$
1.6 $T2 = \beta .V$
1.7 $T3 = Ai + (\alpha+\beta).H$
1.8 $R1 = \gamma\alpha .U$
1.9 $R2 = \gamma\beta .V$
1.10 $R3 = e(T3,P)^{\gamma x} e(H,W)^{-\gamma\alpha-\gamma\beta} e(H,P)^{-\gamma\delta 1-\gamma\delta 2}$
1.11 $R4 = \gamma x .T1 - \gamma\delta 1.U$
1.12 $R5 = \gamma x .T2 - \gamma\delta 2.V$
1.13 Set c = f(M,T1, T2, T3, R1, R2, R3, R4, R5)
1.14 Construct the following numbers
1.15 $s\alpha = \gamma\alpha + c\alpha$
1.16 $s\beta = \gamma\beta + c\beta$
1.17 $sx = \gamma x + cx$
1.18 $s\delta 1 = \gamma\delta 1 + c\delta 1$
1.19 $s\delta 2 = \gamma\delta 2 + c\delta 2$
1.20 Return σ = (T1, T2, T3, c, $s\alpha$,, $s\beta$,,sx, $s\delta 1$, $s\delta 2$)
1.21 end

Output: Generate a valid group signature on M.

4.2 Signature Verification

Input: System Parameter (P, U, V, H, W),M And Signature

σ = (T1, T2, T3,c,$s\alpha$,,$s\beta$,,sx, $s\delta 1$, $s\delta 2$)

Algorithm:

1.1 Begin
1.2 Compute the following values
1.3 $R1 = s\alpha . U - c.T1$
1.4 $R2 = s\beta . V - c.T2$

1.5 R3 = (e(T3,W)/e(P,P))c e(T3,P)sx
e(H,W)-sα-sβ
1.6 R4= sx .T1 - sδ1 .U
1.7 R2 = sx .T2 - sδ2 .V
1.8 If c = f(M,T1, T2, T3,R1, R2, R3, R4, R5)
1.9 Return True
1.10 Else
1.11 Return False
1.12 End

Output: True or False.

4.3 Revocation Verification

Input: System Parameter (H0, H1, H2),a group signature σ,
And asset of revocation keys A1,……Ar

Algorithm:

1.1 Begin
1.2 Set temp = e(T1, H1) e(T2, H2)
1.3 for I = 1 to n
1.4 if e(T3 – Ai,H0) = temp
1.5 Return Valid
1.6 End if
1.7 End for
1.8 Return Invalid
1.9 End

Output : Valid or Invalid

5. SCHEME DESCRIPTION

In this proposed system consists following Moduleand techniques:

- System Setup
- User Registration
- User Revocation
- File Upload
- File Download
- File Deletion

5.1 System Setup

System setup can be done by creating a cloud assembler in which data owner creates an account with cloud server..

5.2 User Registration

After successful creation of cloud setup, users need to get registered with the system through user registration process. During registration process users need to fill their personal information such as user Name, Emailed etc. but the system guaranteesIdentity privacy. At same time user has to select image for Image based Authentication which is used 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.

5.3 User Revocation

For User revocation is the process of deletion of user from system user list which is performed by group manager or data owner. The system maintains Revocation List (RL) for each attributes. For the user to be revoked, his access structure is disconnected from RL, so that they can't have more access to cloud. Proposed system guarantee that revoked user can't access files on cloud

5.4 File Upload

User has to browse file for uploading. Before uploading files, Data Owner assign File IDto selected data files and then encrypts file using his public key Pk. In this way file successfully uploaded.

5.5 File Download

For downloading file Users must have valid secret key. First user has to submit file id, then cloud verify signature and revocation. In addition for security cloud verifies image based authentication and One Time Password. If it satisfies user's access structure and OTP, decrypted data file can be downloaded by user.

5.6 File Delete

For file deletion, Data Owner has to submit File Id. If owner's signature and revocation verification is verified successfully then cloud server positively deletes the file with specified identity.

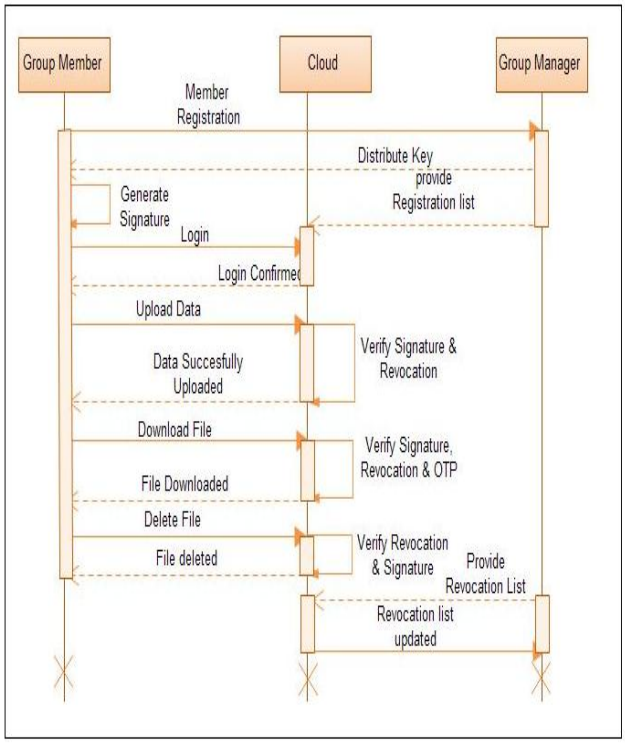

Fig 2: Sequence diagram for proposed system

6. ADVANTAGES OF SYSTEM

- Thwarting Shoulder attack and Brute-force attack at the client side.
- Provide 3-Level Security to system.
- Provide strong security where the need to store and maintain crucial and confidential data secure.
- System is more users friendly
- Provide a secure channel of communication between the communicating entities.
- Ease of using & remembering images as a password also support the scope of these systems.
- Provides reliability and scalability
- Backup group manager will remains available
- Satisfaction of the perfect forward secrecy
- Security against the OTP reveal
- Privacy protection

7. CONCLUSION

Cloud computing is very glowing environment for corporation world in term of providing essential facilities in a very cost effective way. This paper hazards are manage like failure of group manager by growing backup group manager, sagging of group manager in case number of requests more by sharing

the workload in group managers. This system will definitely help thwarting Shoulder attack and Brute-force attack at the client side. The main Objective of 3 Level Security system is aexcellent and an mysterious study of using images as password and implementation of an tremendously secured system. Additionally, It supports efficient user revocation and new user joining. More specially, efficient user revocation can be achieved through a public revocation list (RL) without updating the private keys of the remaining users. Extensive studies show that proposed scheme satisfies the desired security necessities and assurances efficiency, security and scalability as well.

8. ACKNOWLEDGMENTS

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. Sandeep Kadam whose help, stimulating suggestion and encouragement helped me in the all-time.

9. REFERENCES

[1] Xuefeng Liu, Yuqing Zhang, Boyang Wang, and Jingbo Yan. 2013, Mona: Secure Multi-Owner Data Sharing for Dynamic Groups in the Cloud, IEEE Transactions On Parallel And Distributed Systems, Vol. 24, No. 6.

[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, 2010, A View of Cloud Computing, Comm. ACM, vol. 53, no. 4, pp. 50-58.

[3] S. Kamara and K. Lauter, 2010, Cryptographic Cloud Storage, Proc. Int'l Conf. Financial Cryptography and data Security (FC), pp. 136- 149.S. Yu, C. Wang, K.Ren,and W. Lou,2010 ,Achieving Secure, Scalable, and Fine-Grained Data Access Control in Cloud Computing, Proc. IEEE INFOCOM, pp. 534-542.

[4] E. Goh, H. Shacham, N. Modadugu, and D. Boneh, 2003,Sirius: Securing Remote Untrusted Storage, Proc. Network and Distributed Systems Security Symp. (NDSS), pp. 131-145.

[5] R. Lu, X. Lin, X. Liang, and X. Shen, 2010, 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.

[6] B. Waters, 2008 ,Ciphertext-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.

[7] V. Goyal,O. Pandey, A. Sahai, and B. Waters,2006 ,Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data, Proc. ACM Conf. Computer and Comm. Security (CCS), pp. 89-98.

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

[9] Wang, B. Li, and H. Li, 2012, 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.

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

[11] V.Sathana, J.Shanthini, 2013 Three level security system for dynamics group in cloud (IJCST)- Volume1 Issue2.

[12] Mrs. Sunita R. Patil, Prof Sandeep Kadam 2014, Reliable and Scalable approach to Store and Share Sensitive Data for Dynamic Groups in the Cloud, International Journal of Advanced Research in Computer Science and Software Engineering(IJARCSSE), Volume 4, Issue 5,ISSN: 2277

[13] D. Naor, M. Naor, and J.B. Lotspiech, 2001, Revocation and TracingSchemes for Stateless Receivers, Proc. Ann. Int'l Cryptology Conf.Advances in Cryptology (CRYPTO), pp. 41-62.