International Journal of Advanced Research in Arts, Science, Engineering & Management (IJARASEM)

| ISSN: 2395-7852 | www.ijarasem.com | Bimonthly, Peer Reviewed & Referred Journal|

| Volume 6, Issue 1, January 2019 |

Role Based Approach for Secure Key Distribution and Data Sharing for Dynamic Groups

Smita S. Bhosale

ME Student, Department of Computer Engineering, TSSM'S BSCOER, Narhe, Pune, India

ABSTRACT: Today, use of cloud computing is rapidly growing for several purposes, mainly for large data storage and sharing data in clouds. Here, users can share data for dynamic groups with cost-effectively. Membership is frequently changing in a cloud. The Existing system is using the protected (secure) commutation channel for data sharing. This implementation is difficult for practice. Still, the existing system is suffering from collusion attack and insecure key distribution with a single cloud. There is no assurance of the data confidentiality and accessibility. In the proposed system, multiple cloud services are used to store data. The System is proposing a safe way for key distribution without using any protected communication channels, and the user can safely get their private keys from group administrators (managers).Any users in the gathering can use the source in the cloud and denied users cannot get to the cloud once more. The system provides fine-grained access control. Also, the system supports the anti-collusion attack with an untrustworthy cloud. Our system is proposing triple levels of encryption techniques and a file is stored in a split format on multiple clouds in different groups using a hybrid cloud. The system is providing secure revocation.

KEYWORDS: Collusion attack, key distribution, multiple clouds, AES, DSS, RSA

I. INTRODUCTION

In cloud computing, the cloud service providers offer single or multiple cloud services for storing and sharing data securely among users i.e. Amazon service S3. Cloud providers offers large storage space with abstraction for simplicity of the user [7]. The membership in the cloud is frequently changing and because of this, security preserving are turned into a challenging issue in the cloud. Company employees in the same department can share and store files in the cloud. However, here is a significant risk to the confidentiality of those stored files. For security purpose, it is necessary to encrypt data before uploading files in the cloud [8].These schemes do not support for secure data sharing for dynamic groups. Some systems have used techniques for securing data sharing called cryptography among multiple group members in an untrustworthy cloud [12].But these systems additionally experiences a cost overheads and security risks. These systems are not supported to dynamic group concept. In some systems, combined approaches of key policy attribute based encryption, proxy re-encryption, and lazy re-encryption are used to achieve fine-grained data access control without disclosing data contents.[9].Other system uses the group signatures and cipher text-policy attribute based encryption techniques[10][13].but these systems does not support to efficient user revocation. It breaches security. The multi-owner schemes [2] use the attribute-based techniques. If any owner revokes from an application, it leads to security issues. This approach is not safe for data sharing. Many approaches based on privacy-preserving policies in public clouds. These approaches are easily suffering due to collusion attack. The Existing approach supports secure data sharing scheme for dynamic groups in a single cloud. The scheme uses attribute-based techniques. It does not support protected/secure user revocation [1]. The proposed system uses role-based access control (RBAC) used for secure data sharing for dynamic groups by taking the advantage of multiple clouds. In RBAC, roles are considered to access permissions and users are mapped to appropriate roles [4]. In multiple clouds, storage space is again partitioned into groups. The files get partitioned and then store in multiple groups with triple level of encryption. The system Supports anti-collision attack and secure user revocation. Our system overcomes cost overhead. Here, the time and space constraints are applied. Our scheme achieves higher security.

1.1 Motivation:

The cloud storage is highly used for data sharing. Users share their confidential data in the cloud and providing security is essential factor in frequently changed membership. Storing data in single cloud creates a risk [1]. The proposed scheme achieves high security for data sharing by using multiple clouds with supporting anti-collusion attack and secure key distribution.

1.2 Goal:

a. Data sharing: To achieve secure data sharing among different users. It supports dynamic groups i.e. Any number of users can add or revoke from group at any time. It will not affect the security of data sharing.

b. key distribution: The Group Manager provides private keys to users securely without any certificate authority or communication channel.
c. Efficiency: Users can stores and shares data anywhere with any users in cloud. When user revokes the group in cloud, there is no need to update the keys of other users. This is single user system. Every user has separate private key.
d. Security: Unauthorized users can not capable to access the data which is stored in cloud. Files are fragmented and then stored in multiple clouds with achieving triple level of encryption.
e. User Revocation: One user revoked from group, he cannot access previous group again.

1.3 Objective:
1. To design a secure anti-collusion data sharing scheme for dynamic groups in the cloud.
2. The users can securely obtain their private keys from group manager without Certificate Authorities and secure communication channels.

II. LITERATURE SURVEY

X. Liu [2] proposed Mona- A secure multi-owner data sharing for dynamic groups in the cloud. Membership in cloud computing is as often as possible changing, on account of this, information partaking in a multi-proprietor way to preserve information and identity privacy from an untrustworthy cloud is still a testing issue. The complexities of client investment and repudiation in these plans are directly expanding the quantity of information proprietors and the quantity of renounced clients, separately. To defeat these difficulties, Mona, a safe multi-proprietor information sharing plan for element gathers in the cloud has proposed. It exploits assemble signature and element communicate encryption procedures. It guaranteed that cloud client can namelessly impart information to others in the deceitful cloud. In this plan, there is no compelling reason to upgrade the client keys, when whatever other client is renounced from the cloud. Computation cost is independent of a number of denied users. Cost and storage overhead rises, easily suffer from collusion-attacks.

Z. Zhu and R. Jiang [3] introduced the attack on Mona. Secure multi-owner data sharing scheme was proposed which is called Mona, this approach introduces that any group member can share data without knowing to each other by using group signature technique. But Mona suffers from some security vulnerabilities. There is possibility of the denied users can sharing data and disclosing the secretes of other members and arises computation cost overheads. An attack on Mona is proposed to overcome the problem of user registration phase and other problems of Mona i.e. computation cost. But the approach is easily suffered from the collusion-attack by the denied user and the cloud.

Zhou, Varadharajan, and Hitchens [4] proposed the achieving secure role-based access control on encrypted data in storage of cloud. Use of cloud is rapidly growing for storing the large volume of data. This has raised security issue of how to control and prevent unapproved access to data put away in the cloud. In this approach, a role-based encryption method is utilized to a safe get to control scheme on encoded information in hybrid cloud storage for large data. This plan can accomplish efficient client denial that joins role-based get to control approaches with encryption that provides security to large data storage in the cloud. Here users only need to keep a single key for decryption.
It overcomes the complexity of members, but still it includes some issues.
1. Lack of secure key distribution.
2. Does not support secure user revocation.
3. Does not offer Anti-collusion attack.
4. Lack of Data confidentiality.

Nabeel [5] introduced a Privacy-preserving policy based content sharing in public clouds.
In this approach, The Public key cryptosystem, for example, attribute-based encryption (ABE) and proxy or intermediary re-encryption (PRE) are utilized for encryption reason.
In this approach, an important thing is it uses key management scheme called broadcast group key management (BGKM).In this scheme, just some public information should be upgraded for user addition or revocation. Yet at the same time, this approach is not secure as a result of the low insurance of responsibility or weak commitment.

Kamara [8] proposed the Cryptographic cloud storage. The cloud provider provides the best cloud services. One of them is data storage. But there are security problems related to data storage and data sharing among dynamic groups for an organization.

III. PROPOSED SYSTEM ARCHITECTURE

One inconsequential answer for accomplishing secure information partaking in the Cloud is for the information proprietor to encode his information before putting away into the Cloud, and later, the information remains data hypothetically secure against the Cloud supplier and different vindictive clients. At the point when the information proprietor needs to share his information with a group, he sends the key used for information encryption to every individual from the gathering or group. Any individual from the group can then get the encoded information from the Cloud and decode the information utilizing the key and thus does not require the intercession of the information proprietor.

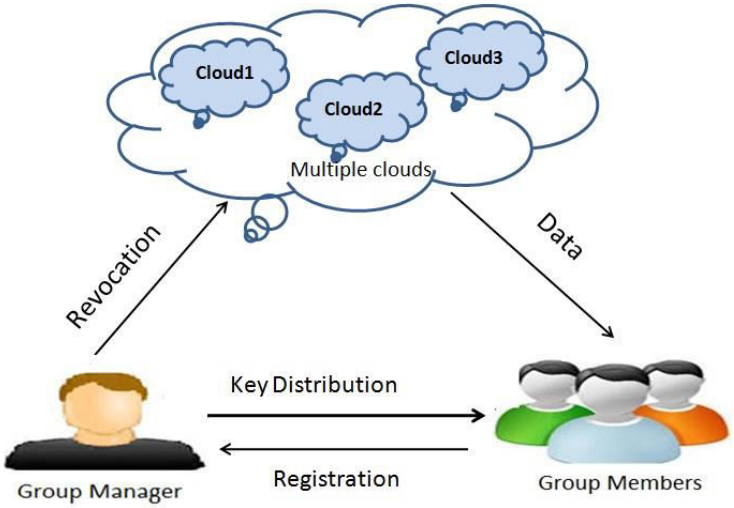


Fig.1 proposed system

- This system proposes secure data sharing and key distribution scheme for dynamic groups. In which, the key distribution is done without using any secure communication channels.
- Users can get their private keys from group manager in a secure way without using any Certificate Authorities due to the verification for the public key of the user.
- The system uses the group user list for the purpose of achieving fine-grained access control. The system allows any user to use the source in the cloud and revoked user can not access the group. And revoked user can not be able to get the original data files after they are revoked. The scheme can achieve secure user revocation with the help of polynomial function.
- The Proposed system uses multiple clouds, when the user uploads a file in the cloud, file contents are double encrypted and then file get fragmented and stored on different groups which are made in multiple clouds and third level of encryption are applied to file.
- Role based access control techniques are used for securing data.

| ISSN: 2395-7852 | www.ijarasem.com | Bimonthly, Peer Reviewed & Referred Journal|

| Volume 6, Issue 1, January 2019 |

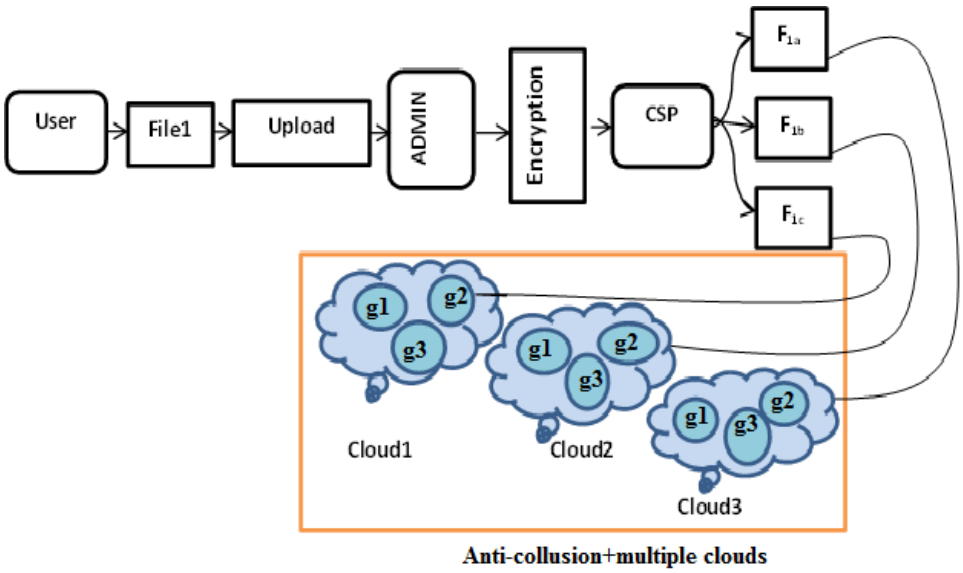


Fig 02 .Block diagram of proposed system

IV. ALGORITHM USED

1) AES Algorithm :

This symmetric encryption Algorithm which are AES is an iterative rather than Festal cipher. It is based on 'substitution–permutation network'. It comprises of a series of linked operations, some of which involve replacing inputs by specific outputs (substitutions) and others involve shuffling bits around (permutations).

2) Secure Key Distribution Algorithm DSS(Digital Signature Standard And Mail method)

Key are generated and given to particular user which are given to requested to key with mechanism of mail or SMS to that user.

3)Key Generation RSA (Ron Rivest,Adi Shamir and Leonard Adelman) :

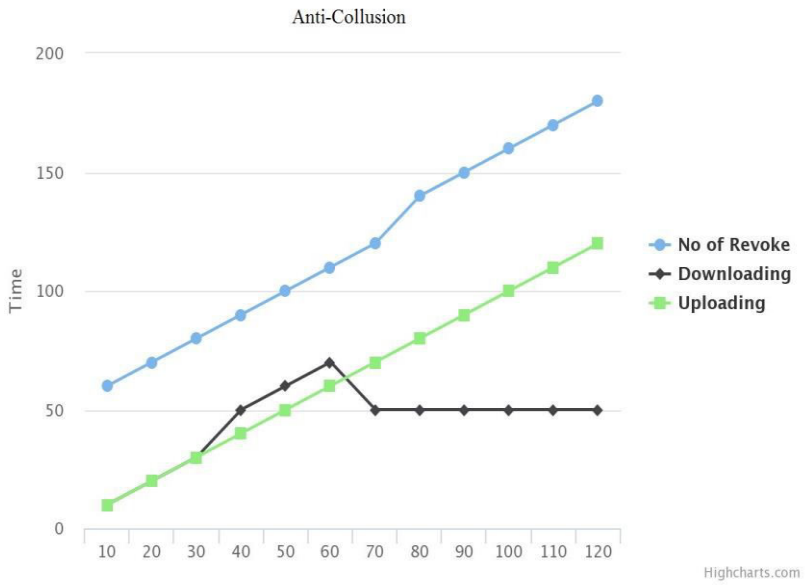
RSA is the algorithm used by modern computers to encrypt and decrypt messages. It is an asymmetric cryptographic algorithm. Asymmetric means that there are two different keys. This is also called public key cryptography, because one of them can be given to everyone. Key generation has two phases. The first phase is a choice of algorithm parameters which may be shared between different users of the system, while the second phase computes public and private keys for a single user.

4. **Fragment:**

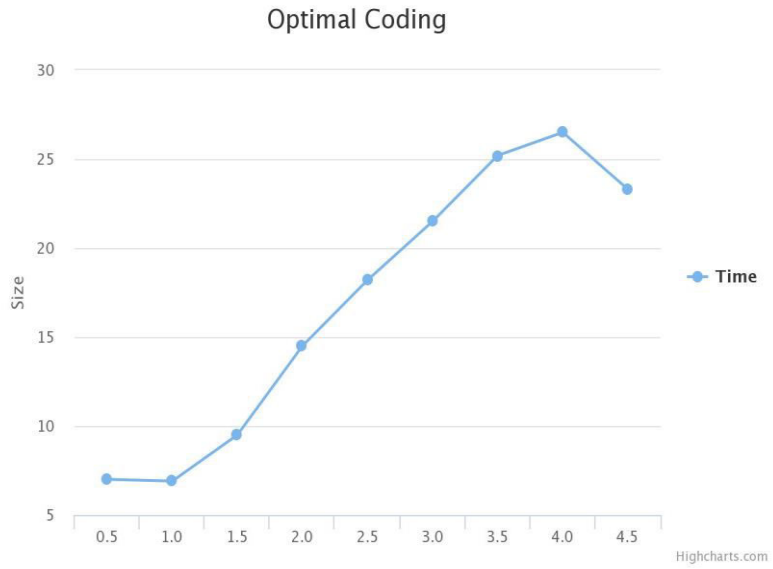
Splits the file into number of the block**.**

V. EXPERIMENTAL SET UP

1. Graph



Graph 1: No. of Uploading and Downloading Time analysis



Graph 2: File size and time variance

Graph 1 shows time for no.of revoke users from groups and time for download and upload files.

Graph 2 shows the time variance with file size.

2. Comparative analysis

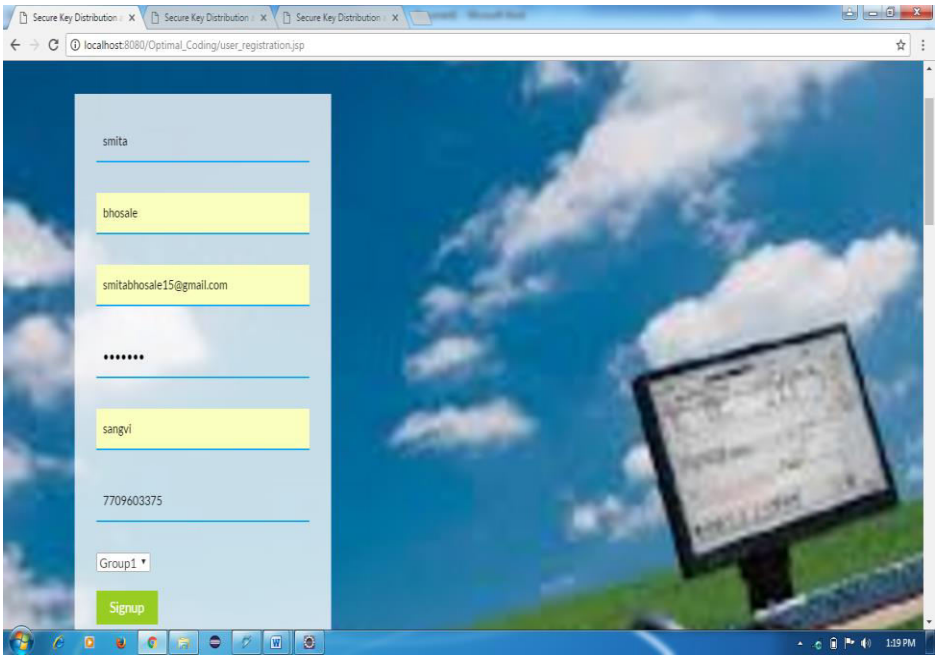
Table1 :Comparative analysis

Parameter	MONA	RBAC	ODBE	Proposed
Secure Key Distribution	No	No	No	Yes
Data Confidentiality	Low	Low	Low	High
Anti-collusion attack Support	No	No	No	Yes
File upload	Complete file stores	Complete file stores	Complete file stores	File get fragment and store in multiple clouds
Data Availability	No	No	No	Yes

Table:2 Comparative analysis

Parameter	Data Sharing using single cloud	Data Sharing using Multiple clouds(Proposed)
Cloud used	Single **cloud**	Multiple clouds
Encryption Levels	Single level	Two level
Access control Techniques	Attribute Base(ABAC)	Role based (RBAC)
Data Confidentiality	Low	High
File upload	Complete file stores in the cloud	File get fragment and store in multiple clouds

User Registration:



VI.CONCLUSION

In this system, multiple clouds are used for secure data sharing and key distribution for groups (users) which are dynamic in nature. The user can share data with others in the group without revealing identity privacy to the cloud. Also, the system supports efficient denial and the addition of user. There is not necessary to update the private keys of the rest of the clients when user revocation occurs. Also, we investigate the minimization of storage cost when the user stores its data in multiple unreliable clouds. Hence, this system achieves higher security.

VII.FUTURE SCOPE

In future, we can use hybrid access control i.e. Combination of RBAC and ABAC for providing more security to multiple clouds. More recovery options can use to recover data. Also, audio and video can share in future work.

REFERENCES

1. Zhongma Zhu and Rui Jiang ,"Secure Anti-Collusion Data Sharing Scheme for Dynamic Groups in the Cloud," IEEE Trans. Parallel Distrib. Syst, vol. 27, no. 1, Jan. 2016.
2. X. Liu, Y. Zhang, B. Wang, and J. Yang, "Mona: Secure multi-owner data sharing for dynamic groups in the cloud," IEEE Trans. Parallel Distrib. Syst., vol. 24, no. 6, pp. 1182–1191, Jun. 2013
3. Z. Zhu, Z. Jiang, and R. Jiang, "The attack on Mona: Secure multi-owner data sharing for dynamic groups in the cloud," in Proc. Int.
   Conf. Inf. Sci. Cloud Compute., Dec. 7, 2013, pp. 185–189.
4. L. Zhou, V. Varadharajan, and M. Hitchens, "Achieving secure role-based access control on encrypted data in cloud storage,"IEEE Trans. Inf. Forensics Security, vol. 8, no. 12, pp. 1947–1960,Dec. 2013.
5. M. Nabeel, N. Shang, and E. Bertino, "Privacy preserving policy based content sharing in public clouds," IEEE Trans. Know. Data Eng., vol. 25, no. 11, pp. 2602–2614, Nov. 2013.
6. Nesrine Kaaniche1, Aymen Boudguiga, Maryline Laurent1, "ID-Base Cryptography for Secure Cloud Data Storage," IEEE Cloud computing, Dec. 2013.

7. M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, "A view of cloud computing," Commun. ACM, vol. 53, no. 4, pp. 50–58, Apr. 2010.
8. S. Kamara and K. Lauter, "Cryptographic cloud storage," in Proc.Int. Conf. Financial Cryptography Data Security, Jan. 2010, pp. 136–149
9. S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving secure, scalable, and fine-grained data access control in cloud computing," in Proc.ACM Symp. Inf., Comput. Commun. Security, 2010, pp. 282–292.
10. R. Lu, X. Lin, X. Liang, and X. Shen, "Secure provenance: The essential of bread and butter of data forensics in cloud computing," in Proc. ACM Symp. Inf., Compute. Commun. Security, 2010, pp. 282–292.
11. B. Waters, "Cipher text-policy attribute-based encryption: An expressive, efficient, and provably secure realization," in Proc. Int. Conf. Practice Theory Public Key Cryptography Conf. Public Key Cryptography, 2008, pp. 53–70.
12. M. Kallahalla, E. Riedel, R. Swaminathan, Q. Wang, and K. Fu, "Plutus: Scalable secure file sharing on untrusted storage," in Proc. USENIX Conf. File Storage Technol., 2003, pp. 29–42.