ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 4, Issue 12, December 2016

Secure Key Distribution and Data Sharing for Dynamic Groups in Multiple Cloud

Smita S. Bhosale, Anil D.Gujar

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 two 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

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. But these systems additionally experience a cost overheads and security risks. These systems are not supported to dynamic group concept.re 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 displaying information[9].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 method. It does not support safe user denial or revocation [1].The proposed system uses role-based techniques for secure data sharing and key distribution for dynamic groups by taking the advantage of multiple clouds. In multiple clouds, storage space is again partitioned into groups. The files get partitioned and then store in multiple groups with two level of encryption. The system Supports anti-collision attack and secure user revocation. Our system overcomes cost and space overhead.

.

.

DOI: 10.15680/IJIRCCE.2016. 0412154

II. LITERATURE SURVEY

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.

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. 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.

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.

Z. Zhu and R. Jiang [3] introduced the scheme. 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 in storage of cloud. Use of cloud is rapidly growing for storing the large volume of data. 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.

III. PROPOSED SYSTEM ARCHITECTURE

One unimportant response for achieving secure data sharing in the cloud is for the data 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.

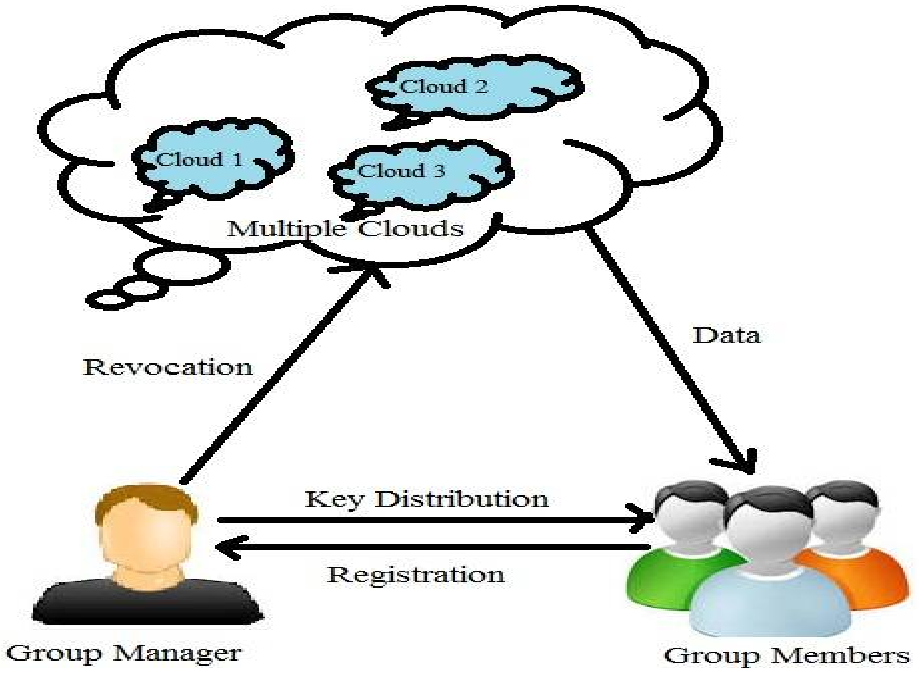

Fig.1 proposed system

Fig.1.shows the proposed architecture. This system proposes secure or protected data sharing and key distribution approach for dynamic groups. Users can get their private keys from group admin or manager in a safe way without using any Certificate Authorities because of the verification for the public key of the user. The multiple clouds are used to store data. The user uploads files with two level of encryption at user level and application level. Then files get split into pieces and then stored into groups in multiple clouds. The system is highly secure from hackers. Our system overcomes cost overhead. Our approach removes a space overhead by using the concept of the virtual storage server. Instead of public cloud, hybrid cloud is used for security and economical purpose. The System can support dynamic gatherings efficiently when new or another client joins the gathering (group) or client is revoked or renounced from the gathering or group, the private keys of alternate clients don't should be recomputed and redesigned. The system supports an anti-collusion attack. Authority of the group choice for storage purpose is of clients.

IV. ALGORITHM

In the System, four types of algorithms are used for different purposes.

1 AES algorithm:

This is symmetric encryption Algorithm which is called AES. It is iterative rather than Festal cipher. It depends on 'substitution–permutation arrange or network'. The algorithm is used for first level of encryption.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 4, Issue 12, December 2016

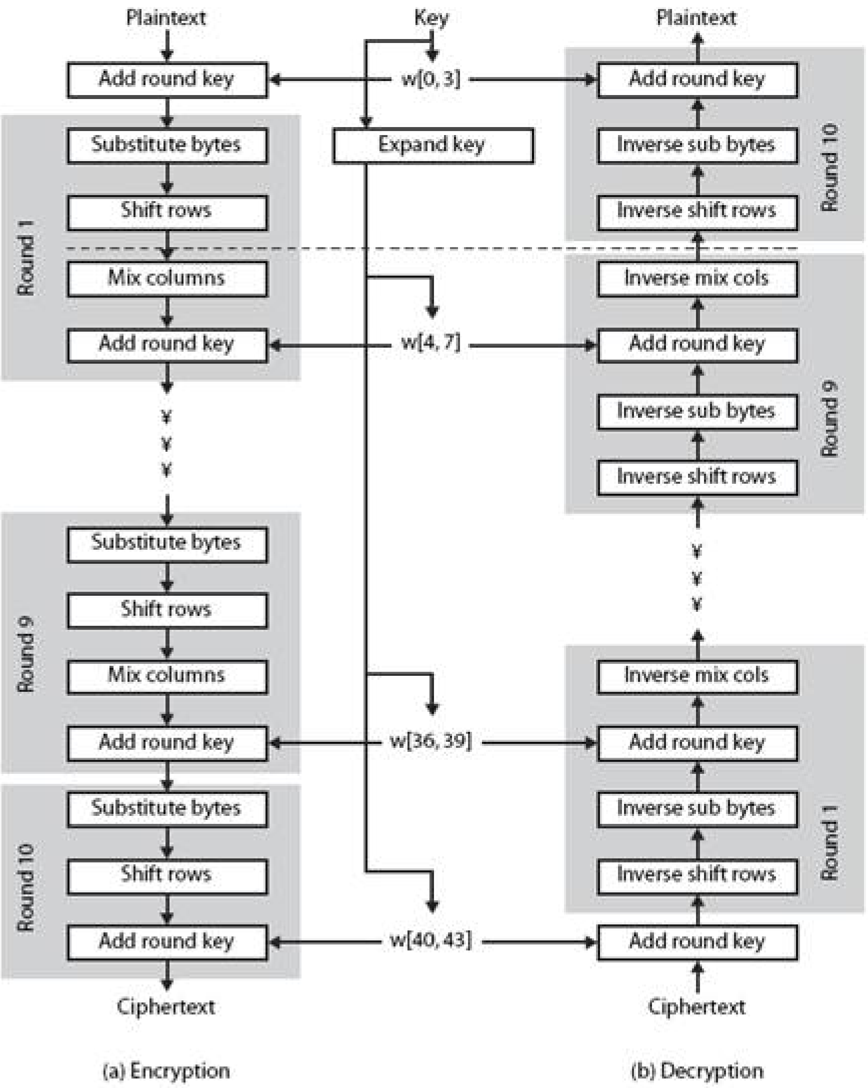

Fig. 2.AES algorithm flow

- **2.DSS algorithm** (Digital Signature Standard And Mail method): Secure key distribution algorithm. Key are generated and given to the particular user with the mechanism of mail or SMS to that user.

3.Key Generation RSA (Ron Rivest, Adi Shamir, and Leonard Adelman):
RSA algorithm is used to encrypt and decrypt messages. It is often used by modern computers for security purpose. It is an asymmetric cryptographic algorithm. Algorithm is used for level 2 encryption.

4.Fragment Algorithm: Splits the file into number of the block**.**
The below steps are included in this algorithms,

1. This system proposes secure or protected data sharing and key distribution approach for dynamic groups. In which, the key distribution is done without using any secure or protected communication channels.

2. Users can get their private keys from group admin or manager in a safe way without using any Certificate Authorities because of the verification for the public key of the user.
3. 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. Also, denied client cannot have the capacity to get the original data files after they are repudiated. The scheme can accomplish secure client denial with the assistance of polynomial function
4. 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 multiple clouds. The user can choose the group i.e. cloud at which he wants to store his file.
5.The System can support dynamic gatherings efficiently when new or another client joins the gathering (group) or client is renounced from the gathering, the private keys of alternate clients don't should be recomputed and redesigned. The system supports an anti-collusion attack

V. CONCLUSION

The system is designed for data sharing and key distribution securely for groups which are dynamic in an untruth cloud by storing data in multiple clouds. The user can share data with others in the group without revealing identity privacy to the cloud. The user is able to 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. All the more extraordinarily, the client denial or revocation can be accomplished efficiently through a public revocation list.

REFERENCES

[1] Zhongma Zhu and Rui Jiang, “Secure Anti-Collusion Data Sharing Scheme for Dynamic Groups in the Cloud”. IEEE Transaction Parallel Distribution System, Jan. 2016.

[2] X. Liu, Y. Zhang, B. Wang, and J. Yang, “Mona: A secure multi-owner data sharing for the dynamic groups in the cloud”. IEEE Transaction Parallel Distribution System, 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”, International Conference Inf. Sci. Cloud Compute 2013.

[4] L. Zhou, V. Varadharajan, and M. Hitchens, “Achieving a secure role-based access control on encrypted data in cloud storage”, IEEE Transaction. Inf. Forensics Security, Dec. 2013.

[5] M. Nabeel, N. Shang, and E. Bertino,”A Privacy preserving policy based content sharing in public clouds”. IEEE Transaction, Nov. 2013.

[6] Nesrine Kaaniche1, Aymen Boudguiga, Maryline Laurent1, “ID-Based Cryptography for a Secure Cloud Data Storage”, IEEE Cloud computing, 2013.

[7] M. Armbrust and M. Zaharia, “A view of cloud computing”, Communication ACM, April 2010.

[8] S. Kamara and Lauter, “Cryptographic cloud storage”,in International Conferenec, Financial Cryptography Data Security, Jan. 2010.

[9] S. Yu, C. Wang, K. Ren, and W. Lou, “Achieving a secure, scalable, and fine-grained data access control in cloud computing”,ACM Symp. 2010.

[10] R. Lu, X. Lin, X. Liang, and X. Shen, “A Secure provenance-The essential of bread and butter of a data forensics in cloud computing”, In ACM Symp. Inf. Compute. Communication and Security, 2010.

[11] B. Waters, “Ciphertext-policy attribute based encryption- An expressive, efficient and provably secure realization”, in International conference on public key cryptography .