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

A Secure Role Based Encryption of Data Sharing for Dynamic Groups in the Cloud

Ajit N Pawar, Prof. Sonal Ftangare

M.E., Dept. of Computer, RMD Sinhgad School of Engineering, Pune, India

Assistant Professor, Dept. of Computer, RMD Sinhgad School of Engineering, Pune, India

ABSTRACT: Continuous changes in the membership of data sharing, giving security and privacy preservation are still challenging issues, especially for an untruth cloud due to the collusion attack. It is based on the secure key distribution without assuming any secure communication channel. We propose a secure role based encryption of data sharing scheme using secure communication channel for dynamic groups in the cloud .The system provides fine grained access control for any clients who wants to access the information from cloud .It also prevents access of clients after their revocation and protect from collusion attack. Proposed system provide guarantee for secure sharing of data files when they are outsourced with double encryption and particular security key distribution mechanism. Users can achieve an effective and economical way for data sharing among group members in the cloud with efficient manner and little management cost.

KEYWORDS: Access control, privacy-preserving, cloud computing key distribution.

I. INTRODUCTION

Cloud computing provides on demand service and processing resources to the Users or devices. It is dynamic computing style in which dynamically scalable and usually virtualization resources are provided as a service over the internet. Fundamental service offered by cloud providers is data storage. Cloud servers managed by cloud providers which are not fully trusted. Users may stored data files on cloud which may be sensitive and confidential, like business plans. To preserve data privacy, a basic solution is to encrypt data files, and then upload the encrypted data into the cloud.

One of the most significant difficulties is identity privacy for the wide deployment of cloud computing. Several security schemes for data sharing an untrusted servers have been proposed. In these approaches, data owners store the encrypted data files in entrusted storage and distribute the corresponding decryption. Users may not be willing to join in cloud computing systems without the guarantee of identity privacy, because their real identities could be easily disclosed to cloud providers and attackers. Identity privacy may incur the sabotage of privacy. For example, a misbehaved staff can deceive others in the company by sharing false files without being traceable. Therefore, traceability, which enables the group manager to track over the real identity of a user, is also highly desirable. Highly recommended for any member in a group should be able to fully access stored data and sharing services provided by the cloud, which could be defined as the multiple-owner manner. More broadly, each user in the group is able to not only read data, but also modify their part of data in the entire data file. Finally, groups are normally dynamic in practice. Changes in membership makes secure data sharing extremely difficult. On the other side, the various system challenges granted from new users to learn the content of data files stored before their participation, because it is impossible for new approved users to contact with anonymous data owners, and obtain the corresponding decryption keys. An appropriate membership revocation mechanism without updating the secret keys of the remaining users is also desired to minimize the complexity of key management.

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

II. RELATED WORK

In[1] author developedOn the security of public key protocol Proposes public key encryption protocol, describes the various techniques to encrypt the public key

In [2] author developed First complete group key management scheme which can supports all these functions yet preserves efficiency. The proposed scheme is based on the new concept of access control polynomial (ACP) that efficiently and effectively support full dynamics, flexible access control with fine-tuned granularity, and concealment .New scheme is protected from various attacks from both external and internal malicious parties.

In [3] author developed Achieving secure role based control on encrypted data in cloud achieved through RBAC. RBE scheme allows RBAC policies to be apply for the encrypted data stored in public clouds. RBE-based hybrid cloud storage architecture provides facility of an organization to store data securely in a public cloud, while maintaining the sensitive information related to the organization's structure in a private cloud.

In [4] author developedOne approach to encrypt documents satisfying different policies with different keys using a public key cryptosystem such as attribute-based encryption, and proxy re-encryption is called broadcast group key management (BGKM), and then give a secure construction of a BGKM scheme called ACV-BGKM. Major advantage of the BGKM scheme is that adding users/revoking users can be performed efficiently by updating only some public information. BGKM used for an efficient approach for fine-grained encryption-based access control for documents stored in an untrusted cloud file storage.

In [5] author developed MONA proposed a new secure multi-owner data sharing scheme, for multiple groups in the cloud. They applied the group signature and dynamic broadcast encryption techniques, any cloud user can secretly share data with others. The storage overhead and encryption computation cost of our scheme are independent with the number of revoked users. Also they analyze the security of scheme with difficult proofs, and demonstrate the efficiency of scheme in experiments.

In 2013 [6] author developed the collision attack prevent on MONA system.It proposed the secure multiowner data sharing in dynamic cloudes.Previous MONA system had some lack causes some security attacks.
In [7] author developed Data distribution in cloud infrastructure provides an effective approach called Secure-Split-Merge (SSM) is introduced for the security of data. The proposed SSM scheme was it uses unique mechanism for performing splitting of data using AES 128 bit encryption key. The chunks of encrypted splits are being maintained on various group servers of different types of cloud zones. The comparative analysis shows that the proposed system gives effective outcomes as compared to various existing and traditional security standards.
In [8] author developed Security achieves against chosen-plaintext attacks using the k-multilinear Decisional Diffie-Hellman assumption.

In [9]author developed Fine-grained two-factor authentication (2FA) access control system for cloud services.proposed2FA access control system, it was an attribute-based access control mechanism implemented with the necessity of both a user secret key and a lightweight security device

In [10] author developedEfficient and secure re-encryption scheme has been proposed for data sharing in unreliable cloud environment. This scheme is built on top of Ciphertext-Policy Attribute-Based Encryption (CPABE),fine-grained access control to share data. That scheme can achieve user revocation without whole ciphertexts re-encryption and key re-distributions also, re-encryption is not performed until a user requests for that data, which reduces overheads. Further, it does not need any clock synchronization.

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

III. GOALS AND OBJECTIVE

The main goals of the proposed scheme including access control, data confidentiality, anonymity and traceability and efficiency.Two requirement of access controls are first, group members are able to use the cloud resource for data operations another is unauthorized users cannot access the cloud resource at anytime, and revoked users will be incapable of using the cloud once again they are revoked.. A new type authentication system, which is highly secure, has been proposed in this system to design a secure data sharing scheme for dynamic groups in the cloud. The users can securely obtain their private keys from group manager Certificate Authorities and secure communication channels.

IV. PROPOSED SYSTEM ALGORITHMS

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).

Steps:

Step1: Select two Prime Numbers P and Q
Step 2: Compute N=p*q Compute φ(N)=(p-1)*(q-1)
Step 3: Choose e such that 1<e and e are Co-prime
Step 4: Computer a value for d such that (d *e) % φ(N)=1
Step 5: Public key is (e, N) Private Key is (d, N)

4)Horizontal Fragment:

Used for fragmentation of data file and groups.
Steps:
Step 1. File is to be split go to step 2
Step 2. Input source path, destination path, Source File, no of fragments
Step 3. N of= no of fragments
Size= size of source file
Step 4. Fragments=size/Nof
Step 5.End

V. PROPOSED SYSTEM ARCHITECTURE

This system propose a secure data sharing scheme, which can achieve through secure key distribution and data sharing for dynamic group along with secure way over secure communication channels. New role based encryption scheme is used for assigning the permissions data encryption. The users can securely obtain their private keys from group manager with Certificate Authorities for the verification of the public key of the user. The system can achieve fine-grained access control. Hybrid cloud is used for efficient use of cloud. Our system for Secure data sharing can be protected from collusion attack. The revoked users can not get the original data access once when they are revoked even if they tried with the untruth cloud. Proposed scheme achieve secure user revocation with the help of polynomial function .System is able to support dynamic groups efficiently, when a new user joins in the group or a user is revoked from the group, the private keys of the other users do not need to be recomputed and updated. System will provide security analysis to prove the security of our scheme. Data protection is also provided using double encryption mechanism.

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

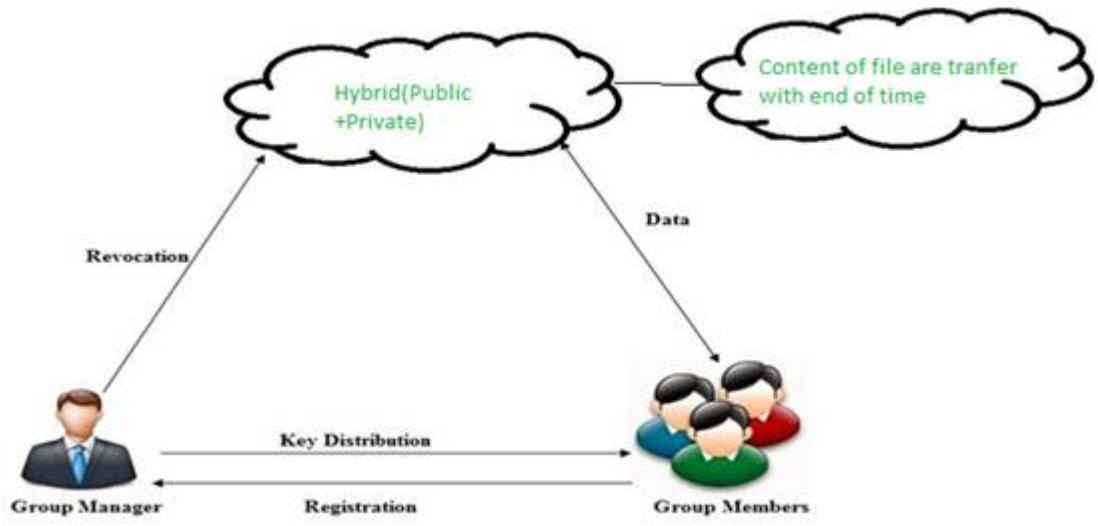

Fig proposed System Architecture

VI. ADVANTAGES OF PROPOSED SYSTEM

1)The computation cost is irrelevant to the number of revoked users in RBE scheme. Because it does not affected by how many users are revoked, the operations for members to decrypt the data files almost remain the same.

2)New approach called RBE provides role based encryption permissions. The cost is irrelevant to the number of the revoked users.

3)Users can securely obtain private keys from group manager Certificate Authorities and secure communication channels.Also, our scheme is able to support dynamic groups efficiently,when a new user registered they can store data in one of chosen group. User can efficiently use the private and public cloud storage

VII. CONCLUSION

This system is design for secure data sharing scheme, for dynamic groups in an untruth cloud. A new type authentication system, which is highly secure, has been proposed in this system. User is able to share data with others in the group without disclose identity privacy to the cloud. It also supports efficient user revocation and new user joining. User revocation can be done through a public revocation list without updating the private keys of the remaining users, and new usersvcan directly decrypt files stored in the cloud before their participation. System also provides the new double encryption technique for data security. New role based encryption provides tight authentication.

REFERENCES

[1] D. Dolev and A. C. Yao, "On the security of public key protocols,"IEEE Trans. Inf. Theory, vol. IT-29, no. 2, pp. 198–208, Mar. 1983.
[2]X. Zou, Y.-S. Dai, and E. Bertino, "*A practical and flexible key management mechanism for trusted collaborative computing*,"in Proc. IEEE Conf. Comput.Commun., 2008, pp. 1211–1219.
[3] 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.
[4]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.
[5]X. Liu, Y. Zhang, B. Wang, and J. Yang, "*Mona: Secure multiowner data sharing for dynamic groups in the cloud*," IEEE Trans. Parallel Distrib. Syst., vol. 24, no. 6, pp. 1182–1191, Jun. 2013.

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

[6]Z. Zhu, Z. Jiang, and R. Jiang, "*The attack on mona: Secure multiowner data sharing for dynamic groups in the cloud*," in Proc. Int.Conf. Inf. Sci. Cloud Comput., Dec. 7, 2013, pp. 185–189.
[7]BurhanUl Islam Khan,Rashidah F. Olanrewaju"SSM: Secure-Split-Merge Data Distribution in Cloud Infrastructure",in2015 IEEE Conference on Open Systems (ICOS), August 24-26, 2015, Melaka, Malaysia
[8]JieXu, Qiaoyan Wen, Wenmin Li, and Zhengping Jin, "*Circuit Ciphertext-Policy Attribute-Based Hybrid Encryption with Verifiable Delegation in Cloud Computing*" IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 27, NO. 1, JANUARY 2016
[9]Joseph K. Liu, Member, IEEE, Man Ho Au, Member, IEEE, Xinyi Huang,
Rongxing Lu, Senior Member, IEEE, and Jin Li, "*Fine-Grained Two-Factor Access Control for Web-Based Cloud Computing Services*", IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 11, NO. 3, MARCH 2016
[10] NazatulHaque Sultan &Ferdous Ahmed Barbhuiya, "*A Secure Re-Encryption Scheme for Data Sharing in Unreliable Cloud Environment*,"978-1-5090-2616-6/16 © 2016 IEEE
DOI 10.1109/SERVICES.2016.16
11] Zhongma Zhu and Rui Jiang "*A Secure Anti-Collusion Data Sharing Scheme for Dynamic Groups in the Cloud*", IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 27, NO. 1, JANUARY 2016.