A Safe Policy Based Data Sharing Scheme for Dynamic Groups in the Cloud

R.Aiswarya[1], M.Nikitha[2], N.Rama Kalpana [3]
[1,2] *Department of Computer Science and Engineering, Adithya Institute of Technology, Coimbatore, TamilNadu, India*
[3]*Assistant Professor, Department of Computer Science and Engineering, Adithya Institute of Technology, Coimbatore, TamilNadu, India*

Abstract *- In cloud providing securities, the users can achieve an effective and economical approach for data sharing among group members in the cloud with the characters of low maintenance and little management cost. Then, security certifications to the sharing information records will be given since they are outsourced. In addition, for the existing plans, the security of key distribution is based on secure communication channel.[1] In this paper we propose a safe information sharing plan for every individual in the group. Firstly, we propose a safe route for key distribution with no safe correspondence channels, and the group members can safely obtain their private key from group manager. Second, we use fine-grained access control, any user in the group can use the sources in the cloud and the revoked users cannot access the cloud again after they are revoked from the group. Third, we can protect the stored data files from collusion attack, so that the revoked users cannot access the original data files even if they have the plan with un-trusted cloud. In this we use polynomial function for secure user revocation and good efficiency. It means old user in the group need not renew their private keys when a new user is added into the group or a user is revoked from the group.*

Keywords —*Data Sharing, Cloud Computing, AES Algorithm, Ring Signature*

I. INTRODUCTION

Cloud is the latest and fast growing technology, it provides the resources to its users dynamically via the internet. It provides easy, cost effective and reliable way to store the data.[13] With cloud storage and sharing services (e.g. Google Drive, Drop-box) people can work together as a group and share the data with each other. Cloud computing enables its users to store the data as well as share the data with each other. When user creates the shared data, user not only accesses and modifies the data but also shares the data with other users. By storing the data in the cloud, the people can be relieved from the burden of data storage and maintenance. The cloud provides infinite storage space. In this paper the main contributions of schemes are,

1) We propose a secure data sharing scheme for dynamic members. we propose a secure way for key distribution without any secure communication channels, and the users can securely obtain their private keys from group manager.[16]
2) Our scheme can achieve fine grained accesscontrol, any user in the group can use the source in the cloud and revoked users cannot access the cloud.
3) Revoked users cannot get the original data file even if they have a plan with the un-trusted cloud.

II. EXISTING SYSTEM

In existing system, it will give the safe approach to key distribution with no protected correspondence channels.[2] The clients can acquire their private keys from the group manager with no certificate authorities because of the check for people in common key of the user. This can bring about fine grained access control, with the assistance of group users lists, any user in the group can utilize the source in the cloud. The rejected clients cannot access the old data files from the cloud once they are denied in spite of the plan that they have a plan with the un-trusted cloud.

A. Disadvantages

The disadvantages are as follows:

- It is difficult to design a secure and efficient data sharing scheme.
- The system had a heavy key distribution over head.
- The verification between entries are not concerned, the scheme easily suffer from attacks, for example, collusion attack.
- The scheme is not secure because of the weak protection commitment in the phase.

III.PROPOSED SYSTEM

A secure data sharing scheme can achieve secure key distribution and data sharing for dynamic group. The users can securely obtain their private keys from group manager Certificate Authorities and secure communication channels.

A. Advantages

- The users can securely obtain their private keys from group manager without any Certificate Authorities due to the verification for the public key of the user[15]
- Any user in the group can use the source in the cloud and revoked users cannot access the cloud again after they are revoked.
- Propose a secure data sharing scheme which can be protected from collusion attack.

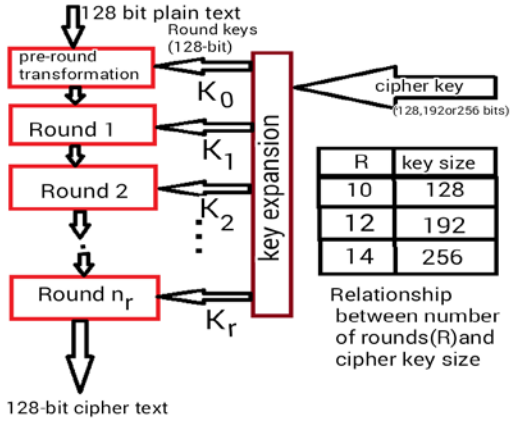
- This scheme can support and manage dynamic group effectively

IV. ALGORITHMS/TOOL USED

A. *AES Algorithm*

Advanced Encryption Standard (AES) algorithm is a symmetric encryption algorithm. This algorithm is used for both encryption and decryption process. It works by repeating the same steps multiple times

- AES is a secret key encryption algorithm[4]
- AES Encryption is used for uploading the data file in the cloud.
- AES Decryption is used for downloading the data file from the cloud.



AES Algorithm

B. *AES Encryption process:*

1) Sub Bytes:

The 16 input bytes are substituted by looking up a fixed table in design. The result is in the matrix of four rows and four columns.[5]

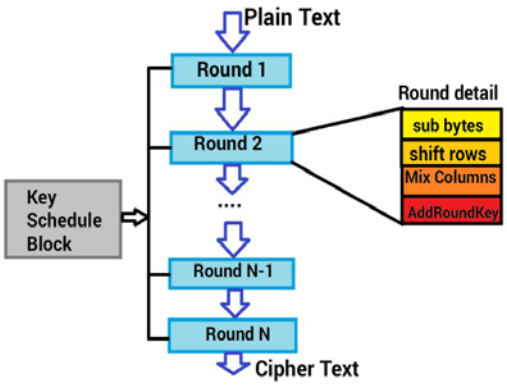
2) Shift rows:

Each of the four rows of the matrix is shifted to the left. Any entries that 'fall off' are re-inserted on the right side of row. Shift is carried out as follows-

- Second row is shifted one(byte) position to the left.
- Third row is shifted two positions to the left.
- Fourth row is shifted three positions to the left.
- The result is a new matrix consisting of the same 16 bytes but shifted but with respect to each other.

3) Mix Columns:

- Each column of four bytes is now transformed using a special mathematical function. This function takes as input the four bytes of one column. The result is another new matrix consisting of 16 new bytes. It should be noted that this step is not performed in last round.



AES Encryption

4) AddRoundKey:

- The 16 bytes of matrix are now considered as 128 bits and are XORed to the 128 bits of the round key. If this is the last round then the output is the ciphertext. The resulting 128 bits are interpreted as 16 bytes.

C. AES Decryption process:

- The process of decryption of an AES ciphertext is similar to the encryption process. Each round consist of four processes conducted in the reverse order- AddRoundKey , Mix columns, Shift rows, Byte substitution.
- The sub-process in each round are in reverse manner. The encryption and decryption algorithms are implemented separately, although they are very closely related.

D. Ring Signature Algorithm

- It is a secure key distribution algorithm, the group manager generates the secret key to the group user and the group user receives the encrypted key through the mail or through the message.[12]
- A ring signature algorithms a type of digital signature that can be performed by any member of the group users that each have keys.
- Therefore, a message signed with a ring signature is validated by someone in a particular group of people[6].
- Ring signatures are like group signatures yet contrast in two key routes: initially, individual signatures cannot be modified and a group can be formed by any number of persons.
- Ring signature is a promising candidate to construct an anonymous and authentic data sharing system for end user[10].

- It allows a data owner to secretly authenticate his data which can be put into the cloud for storage

E. Tool used

- The encrypted file is uploaded in the local disc and further it is stored in the drop box.
- When the user downloads the data it decrypts and sends the data to the user.

V.LITRATURE SURVEY

1) **Predicate Privacy in Encryption Systems:**

Methodology: A symmetric key predicate encryption scheme is used.

Advantages: The predicate privacy in the encryption systems are simple and slight efficiency ,supporting inner product queries, which are the most expressive queries supported by currently known schemes.

Disadvantages: The privacy in the encryption has no addresses from a high entropy distribution. computationally indistinguishable from our original construction.

2) Fully Secure Functional Encryption: Attribute-Based Encryption and (Hierarchical) Inner Product Encryption:

Methodology: A fully secure attribute-based encryption (ABE) scheme

Advantages: The attribute based encryption can achieve full security of systems and the users private keys cannot be combined.

Disadvantages: The cost of decryption grow with the complexity of the access structures and policies.

3) Enabling Secure and Efficient Ranked Keyword Search over Outsourced Cloud Data

Methodology: The secure ranked keyword search over encrypted cloud data and it is outsourced

Advantages: The ranked keyword search is a effective utilization and achieving of remotely stored encrypted data in Cloud Computing.

Disadvantages: The keyword search has little relevance score information leakage against keyword privacy

4) A Practical and Secure Multi-Keyword Search Method over Encrypted Cloud Data :

Methodology: The Secure Multi-Keyword Search Method over Encrypted Cloud Data.

Advantages: The multi-keyword search is proved to be privacy-preserving, efficient and effective. satisfies adaptive semantical security .

Disadvantages: The computation costs of pairing based solutions are significantly high and additional cost on the search due to decryption.

5) Dynamic Searchable Encryption in Very-Large Databases: Data Structures and Implementation :

Methodology: The Dynamic symmetric searchable encryption scheme .

Advantages: The dynamic searchable encryption can easily support additions to the data, as well as deletions via revocation lists.

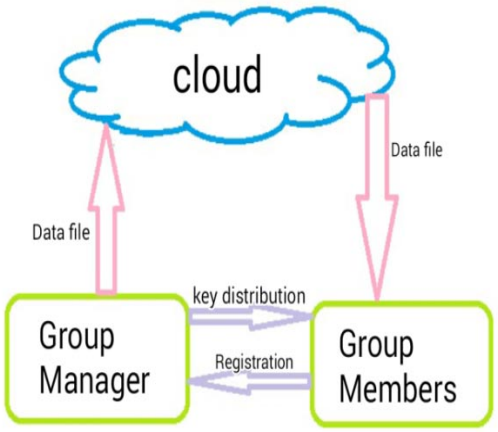
Disadvantages: The hard problem of how the syntactically-defined leakage can be captured in a semantic way such that for real world data sets and query distributions one.

VI.SYSTEM ARCHITECHTURE

The system model consists of three different operations ,they are: the cloud, a group manager and the group members.

The cloud: The cloud is maintained by the cloud service providers, it provides space for storing the data's.[13]

Group manager: The group manager is the leader of the group. They takes charge of the user registration ,user revocation and the key distribution.



System Architecture

Group users: The group users is a set of registered users, they will store the data's in the cloud and share them with all group members.

Group creation: The group manager creates a group and add the members in the group. The group manager distributes the secret key to the group members. By using that secret key the user can access the cloud source.

User registration: The new user should register their valid details to join the group. The group manager accepts and generates he secret key. By using that secret key the user can access the cloud source.

File upload: Any user in the group can upload the data files in the cloud. By using AES algorithm the files will be encrypted and uploaded in the cloud storage.

File download: Any user in the group can download the uploaded files, if the secret key matches to the group the users are able to download and read the data's.

Revoke user: If any of the user in the group have the plan with the untrusted cloud, the group manager will

revoke that user from the group and the revoked user cannot access the original data's from the cloud.[8]

V. CONCLUSION

In this paper, this scheme designs the secured anti-collusion data sharing in the cloud. In this scheme the group uses can safely obtain their secret keys from the group manager with out safe communication channels and also this scheme supports the dynamic groups effectively, the group manager can add the new users in the group or revoke the users from the group. This scheme mainly accomplish a secure revocation, the revoked user cannot be able to access the group data's from the cloud once they are revoked from the group.

REFERENCES

[1] 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

[2] X.Liu,B.Wang,Y.Zhang and J.Yan, Mona: Secure Multi-Owner Data Sharing for Dynamic Groups in the Cloud,IEEE Computer Society, vol. 24,no. 6,June. 2013.

[3] Lan Zhou, Vijay Varadharajan, and Michael Hitchens, "Achieving Secure Role-Based Access Control on Encrypted Data in Cloud Storage, "IEEE Transactions on Information Forensics and Security, vol. 8, no. 12, pp. 1947-1960, December 2013.

[4] S. Kamara and K. Lauter, "Cryptographic cloud storage," in Proc. of FC, January 2010, pp. 136-149.

[5] T. Jiang, X. Chen, and J. Ma,"Public Integrity Auditing for shared Dynamic Cloud Data with Group User Revocation", IEEE Trans on Computers, 2015.

[6] G. Ateniese, K. Fu, M. Green, and S. Hohenberger, "Improved Proxy Re-Encryption Schemes with Applications to Secure Distributed Storage," Proc. Network and Distributed Systems Security Symp. (NDSS), pp. 29-43, 2005.

[7] Kishor Kumar E D, Dara Raju: Secured Anti-Collusion Data Sharing Scheme for Dynamic Groups in the Cloud, Vol. 4, Issue 9, September 2016

[8] C. Delerablee, P. Paillier, and D. Pointcheval, "Fully Collusion Secure Dynamic Broadcast Encryption with ConstantSizeCiphertexts or Decryption Keys," in Proc. of Pairing, 2007, pp.39-59

[9] J.Kar,"Low Cost Scalar Multiplication Algorithms for Constrained Devices", International Journal of Pure and Applied Mathematics, vol.102, no.3, pp.579-592.

[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. of AISIACCS, 2010, pp. 282-292.

[11] V.Sathana and J.Shanthini: Enhanced Security System for Dynamic Group in Cloud, Volume 4, Issue 3,March 2014.

[12] Smita S. Bhosale, Anil D.Gujar: Secure Key Distribution and Data Sharing for Dynamic Groups in Multiple Cloud, Vol. 4, Issue 12, December 2016,pp.21301-21303

[13] 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," Comm. ACM, vol. 53, no. 4, pp. 50-58, Apr.2010.

[14] 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.

[15] Shucheng Yu, Cong Wang, Kui Ren, and Weijing Lou, "Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing," Proc. ACM Symp. Information, Computer and Comm. Security, pp. 282-292, 2010.

BIOGRAPHIES

First Author: Ms. R.Aiswarya

She is currently a B.E student in Department of Computer Science and Engineering at Adithya Institute of Technology, Coimbatore Affiliated to Anna University. Her area of interest is Cloud Computing, Image Processing.

Second Author: Ms. M.Nikitha

She is currently a B.E student in Department of Computer Science and Engineering at Adithya Institute of Technology, Coimbatore Affiliated to Anna University. Her area of interest is Cloud Computing, Big Data Analytics.

Third Author:

Mrs. N.Rama Kalpana

She is currently working as an Assistant Professor Department of Computer Science and Engineering at Adithya Institute of Technology, Coimbatore Affiliated to Anna University. She received her B.E(CSE) degree in 2009 from Sasurie College of Engineering Affiliated to Anna University, M.E(CSE) from Karpagam University in 2014. Her research areas are Cloud Computing, Big Data Analytics and Image Processing.