ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Self-Assured Security between Group Members for Data Stored In Cloud

Manthri Chinna Rao
Dept. of CSE,
Gokul College of Engineering,
Bobbili, AP, India.

P L Pradhan
Dept. of CSE,
Gokul College of Engineering,
Bobbili, AP, India.

Abstract:
Sharing group resource among cloud users is a noteworthy issue, so cloud computing gives a practical and productive organization. Because of regular change of enrollment, sharing data in a multi-owner way to an untrusted cloud is still a testing issue. In this proposition a protected multi-owner data sharing plan, for element group in the cloud. By giving AES encryption while transferring the data, any cloud user can safely impart data to others. Likewise, I investigate the security of this plan with thorough evidences. One-Time Password is one of the least demanding and most famous types of verification that can be utilized for securing access to accounts. One-Time Passwords are regularly used to as safe and more grounded types of verification, and permitting them to introduce over numerous machines. It gives different levels of security to share data among multi-owner way. Cloud computing now a day is expanding throughout the most recent couple of years because of its appealing elements like adaptability, adaptability, minimal effort and simple start up for the apprentices. It gives successful security of the data and data in the cloud storage. The data Distribution in numerous users getting to for element groups jelly data and its character and security from an untrusted cloud and allows access to incessant change of enrollment. The group manager can repudiate any number of users from the dynamic group. In any case, there is feasible for agreement when the repudiated user can attempt to get to the cloud data without the learning of the group manager. With a specific end goal to stop intrigue, this paper proposes an arrangement of mapping to make it conceivable. Fundamentally, a protected key circulation in a safe correspondence channel and the users can get the private key from the group manager.

Keywords: ***Cloud Computing, Access Control, Data owners, Cloud storage, group manager, group user.***

I. Introduction:

Cloud computing is one of the best stages which give storage of data in exceptionally lesser cost and accessible for unsurpassed over the web Cloud computing is Internet-based computing, whereby shared assets, programming and data are given to PCs and gadgets on request. In this few patterns are opening up the time of Cloud Computing, which are an Internet-based improvement and utilization of PC innovation. Cloud Computing implies more than basically saving money on Information Technology execution costs. Cloud Computing offers huge open door for new advancement, and even interruption of whole enterprises. So Cloud computing is the since a long time ago envisioned vision of computing as an utility, where data owners can remotely store their data in the cloud to appreciate on-request excellent applications and administrations from a mutual pool of configurable computing assets. Cloud computing is Internet-based computing, whereby shared assets, programming, and data are given to PCs and different gadgets on request. It depicts another supplement, utilization, and conveyance demonstrates for IT administrations taking into account the Internet. It has been imagined as the cutting edge data innovation (IT) engineering for undertakings, because of its extensive variety of phenomenal points of interest in the IT history: on-request self-benefit, omnipresent system get to, area autonomous asset pooling, quick asset versatility, utilization based valuing and transference of hazard. As a troublesome innovation with significant ramifications, Cloud Computing is changing the very way of how organizations utilize data innovation. One key part of this outlook changing is that data is being incorporated or outsourced to the Cloud. Cloud storage is one of its administrations which give a coherent pool to store the computerized data. It gives simple, savvy and dependable approach to deal with the data. With cloud storage and sharing administrations (e.g. Google Drive, Drop box) individuals can cooperate as a group and impart the data to each other. Cloud computing empowers its users to store the data and in addition impart the data to each other. At the point when user makes the mutual data, user gets to and alters the data as well as shares the data with different users. Since shared data got to and changed by different users, it confronts the difficulties of keeping up the uprightness of shared data. Different methods are proposed to check the trustworthiness of shared data [3], [4]. These methods prescribe to join the mark to every square of data and their respectability relies on upon the accuracy of the every one of the marks. These instruments permit open verifier or outsider reviewer (TPA) to check the honesty of shared data. The greater part of the work proposes methods to confirm the respectability of single owner shared data as opposed to multi-owner data. Multi-owner data is the data where every piece is marked by the different users. Multi-owner shared data can be found in numerous genuine circumstances, for example, checking accuracy of the money related records put away in cloud is legitimate just if all individuals from board advisory group are affirmed, patient's e-wellbeing records are further used just if both patient and his doctor(s) are endorsed and marked. In a group of users sharing the data, when user alters a piece, he/she needs to register the mark on that adjusted square. So with various owners pieces are marked by different owners in the group. At the point when any user leaves the group he/she should be repudiated from the group and squares marked by this denied user must be surrendered. The majority of the past work accepted that the cloud is semi-legitimate i.e. can't be plotted with any untrusted or renounced user. In agreement assault, cloud can take in the substance of the mutual data plotting with repudiated user.

II. Related Work

S. Kamara et al.[9] proposed a security for users to store and share their touchy data in the cryptographic cloud storage. It gives a fundamental encryption and decoding for giving the security. HoIver, the repudiation operation is a certain execution executioner in the cryptographic get to control framework. To streamline the denial method, they display another effective renouncement plot which is proficient, secure, and unassisted. In this plan, the first data are initially partitioned into various cuts, and afterward distributed to the cloud storage. At the point when a renouncement happens, the data owner needs just to recover one cut, and re-scramble and re-distribute it. In this way, the denial procedure is quickened by influencing one and only cut rather than the entire data. They have connected the effective disavowal plan to the figure arrangement quality based encryption based cryptographic cloud storage. The security investigation demonstrates that the plan is computationally secure. E. Goh et al. [7] displayed a SiRiUS, a protected record framework intended to be layered over unreliable system and P2P document frameworks, for example, NFS, CIFS, Ocean Store,

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

and Yahoo! Folder case. SiRiUS expect the system storage is untrusted and gives its own read-compose cryptographic get to control for record level sharing. Key administration and renouncement is basic with negligible out-of-band correspondence. Record framework freshness certifications are bolstered by SiRiUS utilizing hash tree developments. SiRiUS contains a novel strategy for performing record irregular access in a cryptographic document framework without the utilization of a piece server. Augmentations to SiRiUS incorporate extensive scale group sharing utilizing the NNL key denial development. Our usage of SiRiUS performs Ill in respect to the basic document framework regardless of utilizing cryptographic operations. SiRiUS contains a novel strategy for performing document irregular access in a cryptographic record framework without the utilization of a piece server. Utilizing cryptographic operations are used and usage of Sirius additionally conceivable. It just uses the possess read compose cryptographic get to control. Record level sharing is just done by utilizing cryptographic get to. A.Fiat et al.[6] proposed a framework on multicast correspondence structure, different sorts of security danger happens. Therefore development of secure group correspondence that shields users from interruption and listening in are critical. In this paper, they propose an effective key circulation technique for a safe group correspondence over multicast correspondence structure. In this technique, they utilize IP multicast instrument to most brief rekeying time to minimize unfriendly impact on correspondence. What's more, they present intermediary system for answers from group individuals to the group manager to lessen activity produced by rekeying. They characterize another kind of clustering system for rekeying in which new key is created for both leaving and joining part. The rekeying suspicion sits tight for 30 sec so number time's key era will be diminished. M. Armbrust et al. [2] introduced a security a standout amongst the frequently referred to protests to cloud computing; examiners and distrustful organizations ask "who might believe their vital data „out there‟ some place?" There are likewise necessities for auditability, in the feeling of Sarbanes-Oxley azon keeping an eye on the substance of virtual machine memory; it's simple to envision a hard circle being discarded without being wiped, or consents bug making data obvious despicably. There's an undeniable protection, to be specific user level encryption of capacity. This is as of now basic for high-esteem data outside the cloud, and both apparatuses and aptitude are promptly accessible. This approach was effectively utilized by TC3, a human services organization with access to touchy patient records and social insurance claims, while moving their HIPAA-agreeable application to AWS [1]. Thus, auditability could be included as an extra layer past the range of the virtualized visitor OS, giving offices apparently more secure than those incorporated with the applications themselves and bringing together the product duties identified with co

III. Collusion Attack Scheme

Because additive embedding method [8] is widely used in watermarking, average attack is used as a main security analysis tool. This section describes collusion attack which extends average attack so as to enable *k* traitors to create a pirate image of good quality safely. For self-contained, the average attack is introduced in the following.

Average Attack

Trappe *et al.* studied the security of AND-ACC fingerprinting based on the collusion attack model in [9] as

$$\begin{cases} \hat{\mathbf{Y}} = \sum_{i=1}^{k} \lambda_i \mathbf{Y}_i \\ \lambda_1 + \lambda_2 + \cdots + \lambda_k = 1 \\ 0 \le \lambda_i \le 1 \qquad\qquad i = 1, 2, \cdots, k \end{cases} (1)$$

where $\mathbf{Y}_i$ is the legal watermarked image of traitor P_i, i = 1,2,··· ,k = 2r+1. Trappe et al selected $\lambda_i = 1/k$, and they also noted: "there may exist cases in which the underlying fingerprints will not necessarily have the same energy, or be independent of each other, and that other choices for λ_i might be more appropriate." Although Trappe et al. noticed the existence of other

ISSN No: 2348-4845

International Journal & Magazine of Engineering, Technology, Management and Research

A Peer Reviewed Open Access International Journal

collusion attacks, they did not propose an effective collusion attack but average attack. Indeed, Su et al. [19] extended the average attack. They noted "more sophisticated linear temporal filters by allowing β_k (i.e., λ_i in [7]) to take on arbitrary values". Clearly, their collusion is not right. For example, if $\beta_k = 100$, the traitors will obtain nothing but noise according to Su's attack [9]. Thus, How to select λ_i is very important in the linear attack. In the following, a collusion attack model is addressed.

Linear Combination Collusion Attack

Collusion Attack extends the average collusion attack [9] [7] by removing the unnecessary restraint $0 \le \lambda_i \le 1$ from formula

(1), and the updated attack model is

½ Pk

$\mathbf{Y}\hat{}$ = i=1 $\lambda i\mathbf{Y}i$ (2) $\lambda_1 + \lambda_2 + \cdots + \lambda_k = 1$

Generally speaking, all the watermarks have almost the same energy. In order that each traitor has the same probability of escaping from being identified, the contribution to the pirated image from any traitor should be almost identical. That is to say, $| \lambda_1 | =| \lambda_2 |= \cdots =| \lambda_k |$. Hence, λ_i is selected to be 1 or -1 in the collusion attack of the present paper. Without loss of generality, the collusion attack model is

Xr 2Xr+1

$\mathbf{Y}\hat{} = -$ $\mathbf{Y}_i +$ $\mathbf{Y}_i$. (3)

i=1 i=r+1

Obviously, the challenge for collusion attacks how to achieve good fidelity of the pirated image. To quantitatively describe the similarity between the original image **X** and the pirated image **Y**ˆ, suppose the processing image is 8-bit gray images, and all the independent watermarks have the same energy, calculate the PSNR (peak signal-noise-ratio) as

$$\sigma^2 = \frac{1}{n^2} \| \hat{\mathbf{Y}} - \mathbf{X} \|^2 = \frac{1}{n^2} \| \sum_{i=1}^{k} \lambda_i \mathbf{Y}_i - \mathbf{X} \|^2$$

$$\begin{aligned} &= \frac{1}{n^2} \| \sum_{i=1}^{k} \alpha\lambda_i \mathbf{W}_i \|^2 = \frac{k}{n^2} \| \alpha \mathbf{W} \|^2 . \\ PSNR &= 10(\lg 255^2 - \lg \sigma^2) \\ &= 10(\lg 255^2 - \lg \frac{1}{n^2} \| \alpha \mathbf{W} \|^2) - 10 \lg k \\ &= PSNR_0 - 10 \lg k, \end{aligned}$$

Where$PSNR_0$ is the PSNR of the original watermarked image. Comparing with PSNR of the original watermarked images, the PSNR of the pirated image is decreased only 10lg$k$ dB.

For instance, if there are three traitors, the PSNR of pirated image is reduced 10lg3=4.7dB.

IV. Design Objectives of Authorized Method

The main design objectives of the schema include:

♦ A safe key dispersion is used with no secure communication channel. The user gets the private key from Certificate authorities with the public key.

♦ The group users can provide fine-grained access control of the group manager.

♦ The group user can revoke from the dynamic groups safely with the influence of the polynomial function.

♦ The number of the user revoked is independent of the existing user in dynamic groups getting the private key.

A. Scheme Representation

The System model consists of the Group Manager, Group user, and the Cloud [6]. The Group member or group users can divide as creator, reader and writer. The system setup is as follows

Step1: Set up the Cloud Server

Step2: Confirm the Group Manager

Step3: Select Group Member with privileges

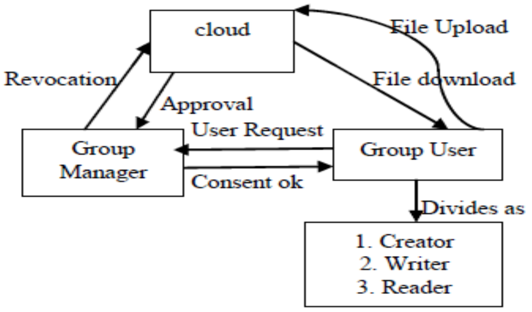
Step4: Group Member Registration

Step5: Key Distribution for Group Member & Group Manager

Step 6: Data Read/Write/Create

Step 7: Revocation procedures

The work flow of the system model is



B. Methodology

Preliminaries:

[1] Bilinear Maps: Let G1 and G2 are additive cyclic groups of the same prime order q. Let e: G1 x G2 →G2 denote a bilinear map constructed with the following properties:

1. Bilinear: $\forall$ a, b $\in$ Z*q and P,Q $\in$G1, e(aP,bQ) = e(P,Q)ah

• 2. Non generate: There exists a point Q such that e(Q.Q)$\neq$ 1.

• 3. Computable: There is an efficient algorithm to compute e (P, Q) for any P, Q $\in$ G1.

C. Asymmetric Encryption Algorithm

Step 1: 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<φ (N) and e and N are Co prime

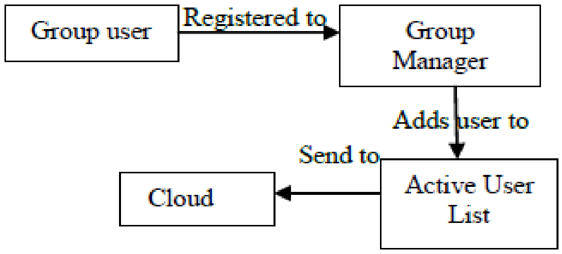
Step 4: Computer a value for d such that (d *e) % φ (N) =1

Step 5: Public key is (e, N) Private Key is (d, N)

The asymmetric Encryption techniques enable the group manager to dynamically increase fresh user and at the same time reserves the earlier calculated information. So, newly joined users can straightly decrypt data files without contacting with the owners. So that there will be no need to change user decryption keys.

D. System Entities Work

1. User Registration For user registration of user member has an ID. The group manager adds the user ID into the group user list, which will be used in tracking. After registration, user obtains a private key, with will be used for group signature and file decryption. While during registration itself, the user differentiates themselves as a creator or a writer or a reader.

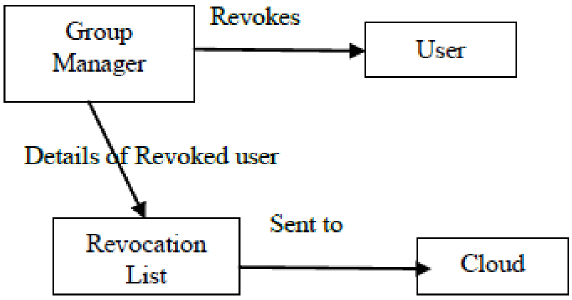


2. Upload Files the File upload is done only by the group Manager or an admin.

3. Files Update Moreover, the creator and writer only can do editing of the data with the consent of the group manager. The reader can only use the data content with authorization.

4. File Deletion The file or data stored in the cloud are deleted by either the group manager or the member who uploaded the file into the server.

5. Revoke user from the group User revocation is performed by group manager by executing a polynomial function done by group manager alone. Once the user is revoked from the group, then the group member r cannot be able access the cloud resources and its data.



V. Proposed System

The group manager will maintain the revocation list of the members. If any of the members leave the group then the member detail is added to that list and the user will not be able to further login to that group. When the new member is added to the group then group key is provided to the member. To remove identity privacy problem, the group manager will have the list of the uploaded files along with the member ID from which the file is uploaded.

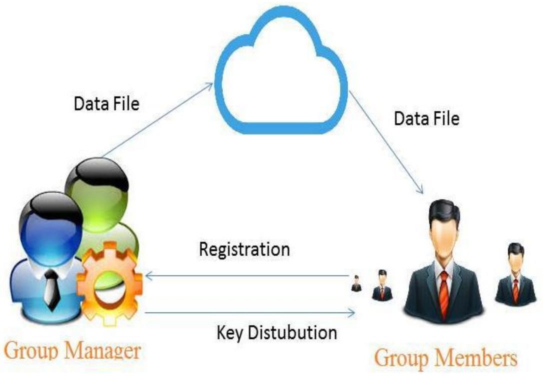


Fig. Proposed system Architecture

By this privacy is kept secure and no one will misuse as it is traceable by the group manager. And as it is multi-owner then any member can not only read data but also modify their own data along with the group manager. The files which are uploaded present in encrypted form and the files can be viewed by group member as they have the group key on which he or she belongs.

AES Encryption

The input 16 byte Plain text can be converted into 4×4 square matrix.

The AES Encryption consists of four different stages they are

Substitute Bytes: Uses an S-box to perform a byte-by-byte substitution of the block

Shift Rows: A Simple Permutation

Mix Columns: A substitution that makes use of arithmetic overGF(9)

Add Round Key: A Simple Bitwise XOR of the current block with the portion of the expanded key

AES Decryption

The Decryption algorithm makes use of the key in the reverse order. However, the decryption algorithm is not identical to the encryption algorithm

VI. Conclusion

In this paper, we design anti-collusion data sharing scheme for dynamic group in the cloud. In our scheme we use two types of algorithms to encrypt and decrypt the data stored in the cloud for more security that is used to make more difficult system for attack. In this scheme we use forwarding mechanism in which uploading user has authority to forward his data to the other user and requested user i.e. downloading user will request for data to the uploading user. All the activity can be manage by the manager.

References

[1] Zhongma Zhu, Rui Jiang, “A Secure Anti-Collusion Data Sharing Scheme for Dynamic Groups in the Cloud” 10.1109/TPDS.2015.2388446, IEEE Transactions on Parallel and Distributed Systems

[2] 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.

[3] M. Kallahalla, E. Riedel, R. Swaminathan, Q. Wang, and K. Fu, “Plutus: Scalable Secure File Sharing on Untrusted Storage,” Proc. USENIX Conf. File and Storage Technologies, pp. 29-42, 2003.Tavel, P. 2007 Modeling and Simulation Design. AK Peters Ltd.

[4] 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.

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

[6] Xuefeng Liu, Yuqing Zhang, Boyang Wang, and Jingbo Yang, "Mona: Secure Multi-Owner Data Sharing for Dynamic Groups in the Cloud," IEEE Transactions on Parallel and Distributed Systems, vol. 24, no. 6, pp. 1182-1191, June 2013.

[7] D. Boneh, X. Boyen, and E. Goh, "Hierarchical Identity Based Encryption with Constant Size Ciphertext," Proc. Ann. Int'l Conf. Theory and Applications of Cryptographic Techniques (EUROCRYPT), pp. 440-456, 2005.

[8] 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.

[9] M. Nabeel, N. Shang, and E. Bertino, "Privacy preserving policy based content.

Author Details

Manthri Chinna Rao, pursuing his M.Tech in the department of Computer Science and Engineering, Gokul college of Engineering, Bobbili, A.P, India. Affiliated to Jawaharlal Nehru Technological University, Kakinada. Approved by AICTE, NEW DELHI. He obtained his B.Tech(CSE) from Gokul college of Engineering, Bobbili

P L Pradhan, M.Tech, working as Associate Professor in the department of Computer Science and Engineering, Gokul college of Engineering, Bobbili, A.P. Affiliated to Jawaharlal Nehru Technological University, Kakinada. Approved by AICTE, NEW DELHI. India. Affiliated to Jawaharlal Nehru Technological University, Kakinada. Approved by AICTE, NEW DELHI.