



Data Sharing Scheme for Dynamic Groups in the Cloud

Using AES Model

V.PRIYANKA, K.SREENATH

P G Student, Dept. of CS., Qis College of Engineering and Technology, Ongole

Asst.Professor of IT, Qis College of Engineering and Technology, Ongole

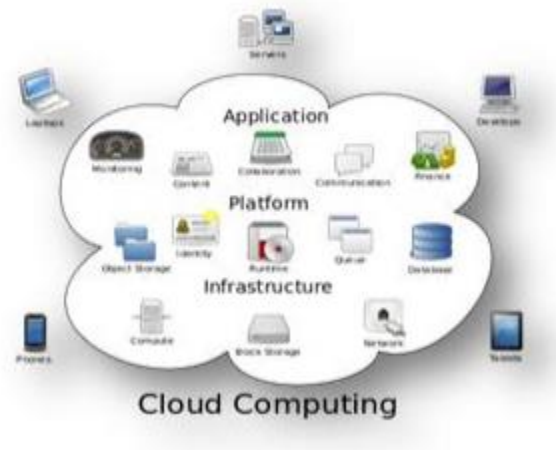
Abstract: Sharing gathering asset number of cloud clients is a noteworthy issue so distributed computing gives minimal effort and productive arrangement. Because of continuous difference in participation sharing information in a multi-proprietor way to an untrusted cloud is as yet a testing models. The sharing of information in assemble individuals to part information and furthermore gives security from untrusted clients by giving security from endowed clients. It will likewise allows take information from the cloud to aggregate individuals. In this suggestion a secured multi-proprietor information sharing arrangement for component bundle in the cloud by giving AES encryption while method the information any cloud customer can securely grant information to others. In the meantime the limit overhead and encryption estimation cost of the arrangement are free with the amount phrasings customers. We propose a protected information sharing technique for dynamic membersto give secure key conveyance with no safe correspondence approach and the clients safely get their security keys from assemble chief. It gives a different levels of security to share information number of multi-proprietor way. To begin with the client chooses the content based secret key is known as OTP is created consequently and sent to relating client email account. After consummation of confirmation and key age process it will encode the common information by utilizing security calculation is actualizing same ideas we can give adaptability and furthermore give greater adaptability of shared information in cloud.

Index Terms: Cloud computing, Broadcast encryption, cryptography, security, group key, verification.anti-collusion, group manager, group user.

1. INTRODUCTION

Cloud computing is Internet based improvement and utilization of PC introduce ages it is another figuring in which progressively versatile and security virtualization locations is provided as a service over the internet. A standout amongst the most significance administrations is offered by cloud suppliers are information stockpiling is thinking about a commonsense information application [1]. A company takes its staffs in the same group to store and destitutions files in the cloud. It also provide a significant risk to the confidentiality many stored files. Specifically the cloud servers is maintain by cloud providers is fully trusted by users while the data files stored in the cloud may be efficient and confidential such as business model. To preserve data security a basic solution is to encrypt data files and then upload the security data into the cloud.keys only to authorized users [2]. Thus unauthorized users as well to upload servers cannot learn the content of the data files because they have no knowledge of the decryption keys [3]. On the different hand an efficient member revocation without updating the secret key of remaining user to minimize the complexity of key management. Security receipt is caused after

every member revocation in group that minimizes multiple copy of encrypted file it can help to minimize computation cost [4]. The cloud computing privacy is a definite set of control based models and policies designed to changed and monitoring the data of rules and security the information and its data application and infrastructure linked with cloud computing to use [5]. Different procedures are proposed to check the new shared data[6]. The majority of the work proposes systems to confirm the honesty of single proprietor shared data as opposed to multi-proprietor information. Multi-proprietor data is information where every square is modify member of clients [7]



Fin No 1 Cloud Computing Model

2. RELATED WORK



S. Kamara[9] is proposed a security for customers to store and share their security data in the cryptographic cloud storage. It provides a basic encryption and decryption for providing the security. The locations operation is main performance killer in the cryptographic access control system. E. Goh [8] presented a SiRiUS, a secure file system designed to be layered over insecure network and P2P file systems such as NFS, CIFS, Ocean Store, and Yahoo! Briefcase. SiRiUS assumes the network storage is untrusted and provides its own read-write cryptographic access control for file level sharing. Key modifications and remove the simple with minimal out-of-band communication.[10] Presented cryptographic storage system that enable secure data sharing. In this methods dividing file into the file group and security each file group with a file block key. In this method at the time of user revocation the file block key uses to be updated and shared to the user the system had a heavy key distribution overhead [11] Propose secure multiowner data sharing model named as Mona. He claimed his method achieve fine grained access control and revoked user is access the shared data again after he was revoked by the cloud and revoked user this model

should be suffer from the collusion attack. Revoked users use his security key to decrypt the encrypted data after his revocation. In 2003, Kallahalla[12] It enables the secure file sharing on the untrusted cloud servers uses the cryptographic storage system the files are divided into the file groups and security both groups with a unique file block key. Now the user to share the file groups with the others by delivering the matching lock box keys. The lock box key is used for modifying the file-block keys. But this changes heavy key dispersion for the enormous amounts of file sharing.

3. SYSTEM ARCHITECTURE

The main Objective of 2 Level Security system is same and an esoteric study of using OTP and implementation of extremely secured models employing 2 levels of security.

Level 1: Security at level 1 has been imposed by simple text based password.

Level 2: After the successful clearance of the above level the Level 2 Security System will then generate a one-time numeric password that would be valid just for that login session. The authentic user will be

informed of this one time password on his email id.

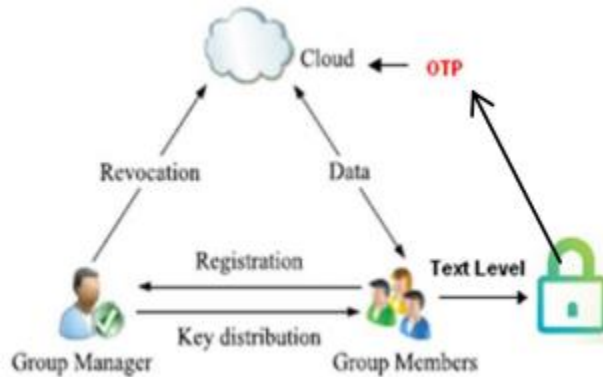


Fig. 3. System Architecture

Secure environments security their resources against unauthorized access by enforcing access control model. So it increasing security is an issue text based passwords is enough to counter such problems. Using the instant messaging service available in internet user will change the One Time Password (OTP) after image authentication. This OTP is used by user to access their personal accounts. In this paper one time password to achieve high level of security in authenticating the user over the internet.

4. PROPOSED SYSTEM

The gathering chief will keep up the renouncement rundown of the different ways. On the off chance that any of the part leavesto gathering the part detail to added

rundown and the client won't have the capacity to security login to that gathering. The new part is added to the gathering security key is given to the part. The documents which are transferred present in encoded structure and the records can be seen by gathering part as they have the authentic key.

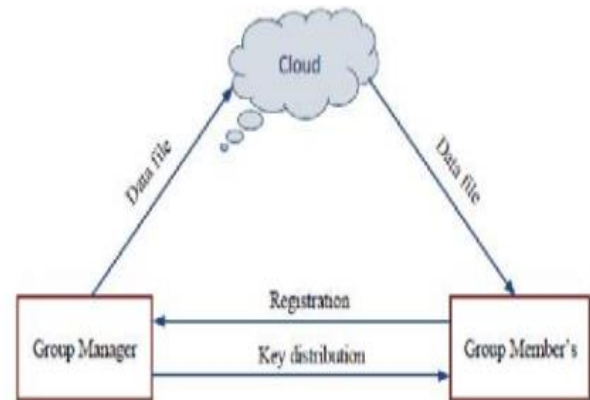


Fig No 4. Proposed system Architecture

AES Encryption

The information 16 byte Plain data can be changed over into 4×4 square lattice.

The AES Encryption comprises of four distinct stages they are

Substitute Bytes: Uses a S-box to play out a byte-by- byte substitution of the square

Shift Rows: A Simple Permutation



Blend Columns: A substitution that makes utilization of number juggling

Include Round Key: A Simple Bitwise XOR of the present piece with the segment of the extended key (security key).

AES Decryption

The Decryption calculation makes utilization of the key in the opposite request. it may the decoding calculation is not indistinguishable to the encryption calculation.

Admin or Group Owner

1. **Group Creation** Groups are creating by admin. A company accesses its staffs in the same group to store and share files in the cloud. Any member in a group is able to fully enjoy the data storing and sharing produces provided by the cloud in the multiple-owner manner.

2. **User Registration** For the registration of user with security identity ID the group manager randomly selects a number and characters for generate random key is used for group signature generation and file decryption.

3. **Group Access Control** When a data shared occurs the tracing operation is performed by the group manager to find the real identity of the data owner. The requirement of access control is twofold. First group members is to use the cloud locations for data operations. Second unauthorized users cannot access the cloud resource at any time and removed users will be incapable of using the cloud again once they are removed.

4. **File Deletion** File stored in the cloud is deleted by either the group manager data owner. To delete a file ID data the group manager computes a signature ID data and sends the signature many ID data to the cloud.

5. **Revoke User** User revocation is performed by the group manager in a public available revocation list RL, based on which group members is encrypt their data files and security the confidentiality against the revoked users.

6. **OTP (One Time Password)** OTPs is removed number of shortcomings the associated with traditional passwords. The most important shortcoming that is

addressed by OTPs is that in contrast to static passwords is not vulnerable to replay attacks.

Generation of OTP Value The algorithm can be described in 3 steps:

Step 1: Generate the HMAC-SHA value Let $HMK = \text{HMAC-SHA}(\text{Key}, T)$ // HMK is a 20-byte string

Step 2: Generate a hex code of the HMK. $\text{HexHMK} = \text{ToHex}(HMK)$

Step 3: Extract the 8-digit OTP value from the string $\text{OTP} = \text{Truncate}(\text{HexHMK})$ the Truncate function in Step 3 does the dynamic truncation and reduces the OTP to 8-digit.

Repudiate client from the gathering user renouncement is performed by gathering chief by executing a polynomial capacity done by gathering director alone. Once the client is denied from the gathering, then the gathering part is capable access the cloud assets and its information

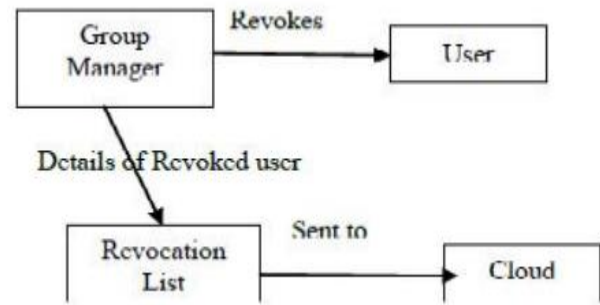


Fig No 5 Group Revocation in Cloud

5. RESULTS AND DISCUSSION

Number of group member is store and destitute data files with others in the group by the cloud . User revocation is achieved without involving the remaining users and signed receipts will be collected after secure content sharing. The remaining users is used to update security preserved data sharing for dynamic groups in the cloud the method combines the group signature and signed receipt and dynamic broadcast encryption method. Specially, the group signature and signed receipt scheme enables users to anonymously use the cloud location, and the dynamic broadcast encryption model access data owners to securely share their data files with other including new joining users.

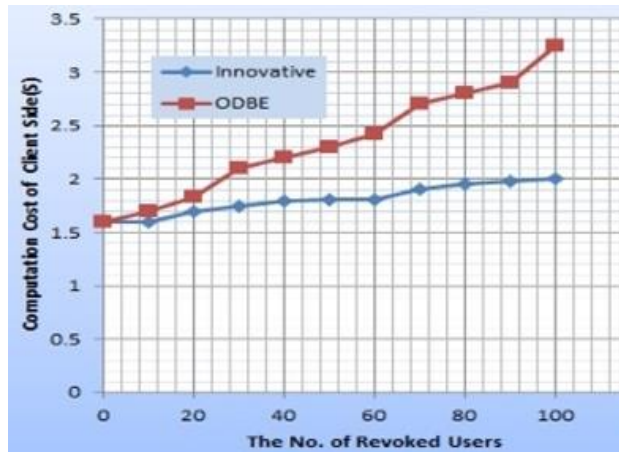


Fig No 6 ODBE Represent Model

6. CONCLUSION

It underpins proficient client repudiation and new client joining. All the more exceptionally, productive client repudiation is accomplished through an open renouncement list without refreshing the security keys of the rest of the clients and new clients can specifically decode documents put away in the cloud before their cooperation. Our plan is bolster dynamic gatherings effectively new client participates in the gathering or a client is denied from the gathering the security keys of alternate clients don't should be recomputed and refreshed. The cloud server contains all data inside arrangement of figure and if any gathering part needs the specific record recovers. We can provide more security of shared data and low cost

this system is users friendly. Tempest attack and Brute-force attack at the client side though 3-Level Security system is a time consuming models it will take to strong security where we need to store and maintain crucial and confidential data secure Such systems provide a secure channel of communication between the communicating entities

7. FUTURE WORK

In our plan we uses two sorts of calculations to scramble and unscramble the data put away in the cloud for more security is utilized to make more troublesome framework for assault. In this plan we uses sending instrument in which transferring client has power to forward his information to the next client and asked for client downloading client will take for data to the transferring client..

8. REFERENCES

- [1] 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



- [2] M. Armbrust, A. Fox, R. Griffith, A.D. Joseph, R.H. Katz, A. Konwinski, G. Lee, D.A. 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] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, "Deduplication in cloud storage using side channels in cloud services," Oct 2008.
- [4]. Jun Zheng and Abbas Jamalipour, "Wireless Sensor Networks: A Networking Perspective", a book published by A John & Sons, Inc, and IEEE, 2009.
- [5]. 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
- [6] A. Fiat and M. Naor, "Broadcast Encryption," *Proc. Int'l Cryptology Conf. Advances in Cryptology (CRYPTO)*, pp. 480-491, 1993.
- [7] E. Goh, H. Shacham, N. Modadugu, and D. Boneh, "Sirius: Securing Remote Untrusted Storage," *Proc. Network and Distributed Systems Security Symp. (NDSS)*, pp. 131-145, 2003.
- [8] 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.
- [9] S. Kamara and K. Lauter, "Cryptographic Cloud Storage," *Proc. Int'l Conf. Financial Cryptography and Data Security (FC)*, pp. 136-149, Jan. 2010.
- [10]. 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.
- [11] Varun and VamseeMohan.B," An Efficient Secure Multi Owner Data Sharing for Dynamic Groups in Cloud Computing", *International Journal of Computer Science and Mobile Computing*, Vol.3 Issue.6, June-2014, pg. 730-734
- [12]. Jun Zheng and Abbas Jamalipour, "Wireless Sensor Networks: A Networking Perspective", a book published by A John & Sons, Inc, and IEEE, 2009.

About Authors:



V.PRIYANKA is current pursuing M.Tech in CS. dept., Qis College of Engineering and Technology, Ongole, Prakasam (Dist.)-523001, AP.



K.SREENATH, Asst.Professor in IT, Qis College of Engineering and Technology, Ongole, Prakasam (Dist.)-523001, AP.