Anti Collusion Data Sharing Schema for Centralized Group in Cloud

Ankita Ajay Jadhav[1], Poonam Doshi(Lambhate) [2], Mohan V. Pawar [3]

[1]Department of Computer Engineering, JSCOE, Pune, Maharashtra, India, Email Id: ankitajadhav029@gmail.com

[2]Second PhD Scholar, Pascific University Udiapur. Email Id: pinu_poonam@yahoo.co.in

[3] JSCOE, Hadpsar, Pune, Maharashtra,India Email Id: mohanpawar2006@gmail.com

--***---

Abstract - *Data sharing among cluster members within the cloud with the characters of low maintenance and tiny management price. Meanwhile, we tend to offer security guarantees for the sharing information files since they're outsourced. To owing the frequent amendment of the membership, sharing information whereas providing privacy-preserving continues to be a difficult issue, particularly for an untrusted cloud owing to the collusion attack. Moreover, for existing schemes, the safety of key distribution is predicated on the secure channel, however, to own such channel may be a sturdy assumption and is troublesome for apply. We tend to propose a secure information sharing theme for dynamic members. First, we tend to propose a secure manner for key distribution with none secure communication channels, and therefore the users will firmly obtain their non-public keys from cluster manager. Secondly, we can do fine-grained access management; any user within the group of members will use the supply within the cloud and revoked users not able to access the cloud once more once they're revoked. Third, we are able to shield the theme from collusion attack, which suggests that revoked users cannot get the initial record though they conspire with the untrusted cloud. In our approach, by investing polynomial perform; we are able to attain a secure user revocation theme. Finally, we can provide the non-public key for security where the user needn't update, hence no need for a replacement of user joins within the cluster or a user is revoked from the cluster.*

Key Words: **Anti Collusion, Privacy Preserving, Revocation, Key Distribution, Data Confidentiality, Access Control**

1.INTRODUCTION

In Cloud Computing by consolidating an arrangement of existing and new procedures from research regions, for example, Service-Oriented Architectures (SOA) and virtualization, distributed computing is viewed all things considered a figuring worldview in which assets in the processing foundation are given as administrations over the Internet. One test in this setting is to accomplish fine grain, information privacy, and adaptability all the while, which is not given by current work. In this paper, we propose a plan to accomplish this objective by misusing KPABE and remarkably joining it with procedures of intermediary re-encryption and apathetic re-encryption. Besides, our proposed plan can empower the information proprietor to designate the majority of calculation overhead to capable cloud servers. Classification of client get to benefit and client mystery key responsibility can be accomplished. A standout amongst principal administration offered by cloud suppliers is information stockpiling. Give us a chance to consider handy information.

We can give secure and protection saving access control to clients, which will give certainty of any part in a gathering to secretly use the cloud asset. Also, the genuine characters of information proprietors can be uncovered by the gathering chief when question happen. In distributed computing, cloud servers give

an endless storage room to clients to store information [1]. It can help customers diminish their money related yield of information administrations by outsourcing the neighborhood stockpiling into the cloud. Be that as it may, as we now transfer information to the cloud, we lose the physical control of the information stockpiling. To accomplish security protecting, a typical approach is to utilize cryptography information records before the customers outsource the delicate information to the cloud [2]. Sadly, the ordinary way is insufficient in view of our itemized objectives, for example, fine-grained get to control. It is hard to plan a safe and productive information sharing plan, particularly for element individuals.

2. LITERATURE SURVEY

Ateniese et al. [1] proposed that quick and secure re-encryption will turn out to be progressively mainstream as a strategy for overseeing encoded document frameworks. Albeit effectively processable, the across the board reception of BBS re-encryption has been frustrated by extensive security dangers. Taking after late work of Dodis and Ivan, we show new re-encryption plots that understand a more grounded idea of security, and we exhibit the helpfulness of intermediary re-encryption as a technique for adding access control to a protected record framework.

Dan et al. [2] presented paper shows the testing open issue by one hand, characterizing and authorizing access arrangements in view of information features, and, then again, permitting the information proprietor to assign a large portion of the calculation undertakings required in fine-grained information get to control to untrusted cloud servers

without revealing the basic information substance. We accomplish this objective by abusing and exceptionally consolidating strategies of trait-based encryption (ABE), intermediary re-encryption, and apathetic re-encryption. Our proposed plot likewise has striking properties of client get to benefit classification and client mystery key responsibility.

Liu et al. [3] In Mona, a client can impart information to others in the gathering without uncovering character security to the cloud. Also, Mona underpins effective client repudiation and new client joining. All the more uncommonly, effective client repudiation can be accomplished through an open renouncement list without redesigning the private keys of the rest of the clients, and new clients can specifically decode records put away in the cloud before their interest.

Zhu et al. [4] presented plan could address fine-grained get to control, which implies that not just the gathering individuals could utilize the sharing information asset whenever additionally the new clients could utilize the sharing information instantly after their disavowals and the denied clients won't be permitted to utilize the sharing information again after they are expelled from the gathering. Nonetheless, through our security examination, the Mona conspire still has some security vulnerabilities. It will effectively experience the ill effects of the intrigue assault, which can prompt to the renounced clients getting the sharing information and uncovering other honest to goodness individuals' insider facts. Moreover, there is another security lack in the client enrollment stage, which is the way to ensure the private key while circulating it in the unsecured correspondence channels.

3. SYSTEM MODEL

3.1 EXISTING SYSTEM

A security planning for information sharing on untrusted servers has been proposed. In these methodologies, information owner stores the encrypted or encoded information records in untrusted big data and disseminate the relating decoding secret key just to approved clients.

In this way, unapproved clients, and also stockpiling servers, can't take in the substance of the information documents since they have no learning of the unscrambling keys, However, the complexities of client support and denial in these plans are directly expanding the quantity of information proprietors and the quantity disavowed clients, separately.

By setting a gathering with a solitary quality, Lu et al. proposed a protected provenance conspire in light of the figure content arrangement trait based encryption strategy, which permits any individual from a gathering to impart information to others. Be that as it may, the issue of client renouncement is not tended to in their plan

They introduced a versatile and fine-grained information get to control plot in distributed computing in light of the key strategy property based encryption (KP-ABE) system. Tragically, the single proprietor way ruins the reception of their plan into the situation where any client is allowed to store and share information.

3.2 Proposed System

The System will keep up trustworthiness if renounce clients can't get an entrance of shared information once they have been disavowed. Be that as it may, this framework experiences a crash assault by the deny client and a cloud. the plan can accomplish fine effectiveness, which implies past clients require not to redesign their private keys for the circumstance either another client participates in the gathering or a client is renounced from the gathering. To Achieve a Secure Anti-Collusion Data Sharing Scheme, for element gathers in the cloud. we propose a safe information sharing plan for element individuals. In the first place, Group Manager wills distinctive deals with alternate gatherings and give an endorsement for Group individuals for enrollment. Client denial is performed by a gathering manager. Group Member will do enrollment first then transfer and download operation will be performed by the gathering part as it were.
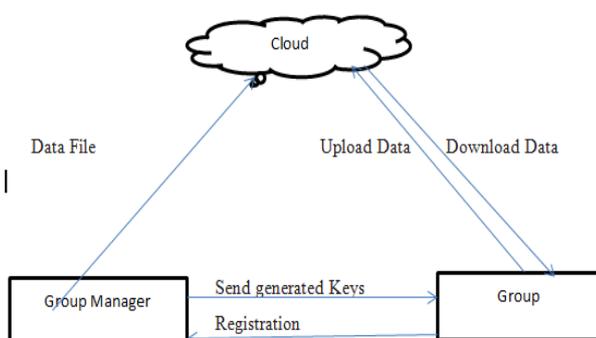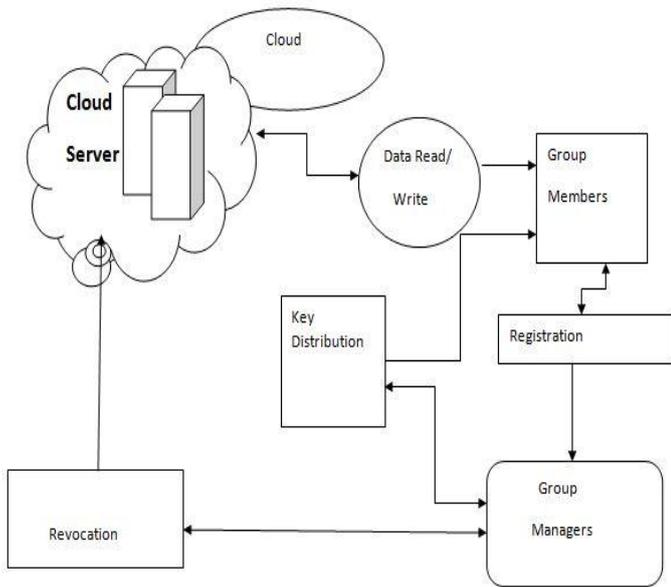

Fig 1. System Model

Fig 2. System Architecture Design

Hostile to plot data sharing plan for element organizations inside the cloud, the clients can safely get their private keys from group supervisor testaments Authorities and secure correspondence channels. Likewise, our plan is prepared to help dynamic companies productively, when a fresh out of the plastic new client joins inside the workforce or a purchaser is denied from the gathering, the classified keys of the inverse clients don't need to be recomputed and redesigned. In addition, our plan can harvest calm client disavowal; the denied clients can't be prepared to get the standard information reports when they are repudiated despite the fact that they scheme with the untrusted cloud.

4. SYSTEM ANALYSIS

AES is based on a design principle known as a substitution-permutation network, combination of both substitution and permutation, and is fast in both software and hardware. Unlike its predecessor DES,

AES does not use a Feistel network. AES is a variant of Rijndael which has a fixed block size of 128 bits, and a key size of 128, 192, or 256 bits. By contrast, the Rijndael specification *per se* is specified with block and key sizes that may be any multiple of 32 bits, both with a minimum of 128 and a maximum of 256 bits.

AES operates on a 4 × 4 column-major order matrix of bytes, termed the *state*, although some versions of Rijndael have a larger block size and have additional columns in the state. Most AES calculations are done in a special finite field.

For instance, if there are 16 bytes, b0, b1, b2....b15 , these bytes are represented as this matrix:

The key size used for an AES cipher specifies the number of repetitions of transformation rounds that convert the input, called the plaintext, into the final output, called the ciphertext. The number of cycles of repetition is as follows:

- 10 cycles of repetition for 128-bit keys.
- 12 cycles of repetition for 192-bit keys.
- 14 cycles of repetition for 256-bit keys.

Each round consists of several processing steps, each containing four similar but different stages, including one that depends on the encryption key itself. A set of reverse rounds are applied to transform ciphertext back into the original plaintext using the same encryption key.

High-level description of the algorithm:

1.   KeyExpansions—round keys are derived from the cipher key using Rijndael's key schedule. AES requires a separate 128-bit round key block for each round plus one more.

2. InitialRound

1. AddRoundKey—each byte of the state is combined with a block of the round key using bitwise xor.

3. Rounds

1. SubBytes—a non-linear substitution step where each byte is replaced with another according to a lookup table.

2. ShiftRows—a transposition step where the last three rows of the state are shifted cyclically a certain number of steps.

3. MixColumns—a mixing operation which operates on the columns of the state, combining the four bytes in each column.

4. AddRoundKey

4. Final Round (no MixColumns)

1. SubBytes

2. ShiftRows

3. AddRoundKey.

5. SECURITY ANALYSIS

In general, this scheme can achieve secure key distribution, fine access control, and secure user revocation. For clearly seeing the advantages of security of our proposed scheme, as illustrated in Table 1, we list a table compared with Mona[3], which is Liu et al.'s scheme, the RBAC[10] scheme, which is Zhou et al.'s scheme and ODBE[9] scheme, which is Delerablee et al.'s scheme. The 'Yes' in the blank means the scheme can achieve the corresponding goal.

Table -1: Security Analysis Comparison

	Secure key	Access control	Secure user revocation	confid-entia-lity	Anti collusion attack
Mona	-	Yes	-	-	-
RABC	-	Yes	-	-	-
ODBE	-	Yes	Yes	Yes	-
Our schema	Yes	Yes	Yes	Yes	Yes

The graphical representation between two schemas.
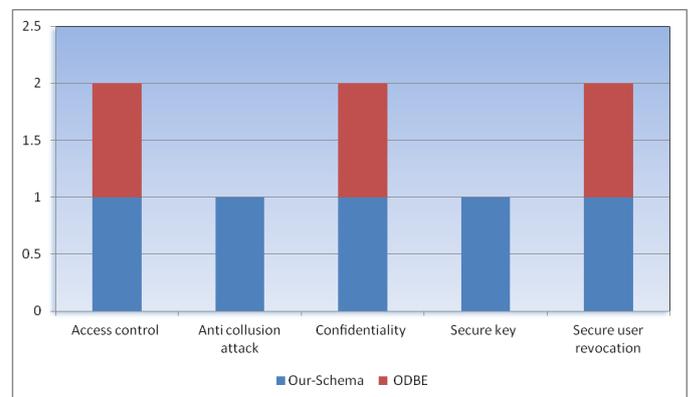
Chart -1: Graphical comparison of (ODBE & Our schema)

3. CONCLUSIONS

The system proposes a Secure Anti-Collusion Data Sharing Scheme, for dynamic groups in the cloud. By member group signature and dynamic broadcast encryption techniques, any cloud user can unidentified share data with others. Meanwhile, the storage expenses and encryption estimation cost of our scheme are independent with the number of officially cancelled

users. The system mainly concentrates on the user official cancellation which should solve the problems of efficiency and storage. In addition, we examine the security system of our scheme with harsh proofs and demonstrate the efficiency of our scheme in expected results.

ACKNOWLEDGEMENT

REFERENCES

[1] G. Ateniese, K. Fu, M. Green, and S. Hohenberger, "Improved proxy re-encryption schemes with applications to secure distributed storage," in Proc. Netw. Distrib. Syst. Security Symp., 2005, pp. 29–43.

[2] B. Dan and F. Matt, "Identity-based encryption from theweil pairing in Proc. 21st Annu. Int. Cryptol. Conf. Adv Cryptol., 2001, vol. 2139, pp. 213–229.

[3] X. Liu, Y. Zhang, B. Wang, and J. Yang, "Mona: Secure multiowner data sharing for dynamic groups in the cloud," IEEE Trans.

[4] 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.

[5] 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," Commun. ACM, vol. 53, no. 4.

[6] D. Boneh, X. Boyen, and H. Shacham, "Short group signature," in Proc. Int. Cryptology Conf. Adv. Cryptology, 2004, pp. 41–55.

[7] B. Waters, "Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization," in Proc. Int. Conf. Practice Theory Public Key Cryptography Conf. Public Key Cryptography, 2008, pp. 53–70.

[8] S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving secure, scalable, and fine-grained data access control in cloud computing," in Proc. ACM Symp. Inf., Comput. Commun. Security, 2010, pp. 282–292.

[9] C. Delerablee, P. Paillier, and D. Pointcheval, "Fully collusion secure dynamic broadcast encryption with constant-size Ci-phertexts or decryption keys," in Proc. 1st Int. Conf. Pairing-Based Cryptography, 2007, pp. 39–59(ODBE original dynamic broadcast encryption (ODBE) scheme)

[10] 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. (RBAC)

[11] 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.

[12] 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.

[13] 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.

[14] B. Den Boer, "Diffie–Hellman is as strong as discrete log for certain primes," in Proc. Adv. Cryptol., 1988, p. 530.

[15] D. Boneh, X. Boyen, and E. Goh, "Hierarchical identity based encryption with constant size ciphertext," in Proc. Annu. Int. Conf. Theory Appl. Cryptographic Techn., 2005, pp. 440–456.

[16] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in Proc. ACM Conf. Comput. Commun. Security, 2006, pp. 89–98.

[17] 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. ACM Symp. Inf., Comput. Commun. Security, 2010, pp. 282–292.

[18] A. Fiat and M. Naor, "Broadcast Encryption," Proc. Int'l Cryptology Conf. Advances in Cryptology (CRYPTO), pp. 480-491, 1993

[19] B. Sheng and Q. Li, "Verifiable Privacy-Preserving Range Query in Two-Tiered Sensor Networks," Proc. IEEE INFOCOM, pp. 4650, 2008.

[20] D. Boneh, B. Lynn, and H. Shacham, "Short Signature from the Weil Pairing," Proc. Int'l Conf. Theory and Application of Cryptology and Information Security: Advances in Cryptology, pp. 514-532, 2001.

BIOGRAPHIES

Miss. Ankita Ajay Jadhav

Student in Department of Computer Engineering, Jayawantrao Sawant College of Engineering, Pune, Mah, India. She pursued her **BE (Comp)** from Pune University, Mah, India in 2012 and Pursuing **ME (Comp)** from Jayawantrao Sawant College of Engineering, Pune, Mah, India. Her research interests include Cloud Computing Security.