A Secure Anti-Collusion Data Sharing Scheme for Dynamic Groups in the Cloud

S.S. Subashka Ramesh [1], M. Venkatesh Yadav [2], B. Sathya Narayana [3], T. Rohith [4], K. Revanth [5]
[1] Assistant Professor, Department of Computer Science and Technology, SRM Institute of Science and Technology, Chennai, Tmail Nadu, India.
[2,3,4,5] B.Tech (IV) Year Student , Department of Computer Science and Engineering, SRM Institute of Science and Technology, Chennai, India.

Abstract – The Benefited from Cloud Computing, clients can achieve a flourishing and moderate methodology for information sharing among gathering individuals in the cloud with the characters of low upkeep and little administration cost. Then, security certifications to the sharing information records will be given since they are outsourced. Horribly, attributable to the unending amendment of the enrollment, sharing data whereas protectively saving remains a testing issue, notably for associate degree untrusted cloud owing to the agreement attack. additionally, for existing plans, the protection of key dispersion depends on the safe line, then again, to possess such channel may be a solid feeling and is tough for apply. during this paper, we have a tendency to propose a secure data sharing arrange for part people. Firstly, we have a tendency to propose a secure route for key dispersion with no safe correspondence channels, and therefore the shoppers will safely acquire their personal keys from gathering administrator. Besides, the arrange will accomplish fine-grained access management, any consumer within the gathering will utilize the supply within the cloud and refused shoppers cannot get to the cloud once more once they're rejected. Thirdly, we can protect the plan from trickery attack, which implies that rejected clients can't get the first information record regardless of the possibility that they scheme with the untrusted cloud. In this methodology, by utilizing polynomial capacity, we can achieve a protected client denial plan. At long last, our plan can bring about fine productivity, which implies past clients need not to overhaul their private keys for the circumstance either another client joins in the gathering or a client is give up from the gathering.

Index Terms – Access control, Privacy-preserving, Key distribution, Cloud computing.

1. INTRODUCTION

In Cloud Computing, with the characteristics of natural information sharing and low support, gives a superior usage of resources. In Cloud Computing, cloud administration suppliers offer a reflection of boundless storage room for customers to host information [1]. It can offer customers some support with reducing their money related overhead of information administrations by moving the nearby administrations framework into cloud servers.

However, security concerns turn into the principle control as we now outsource the capacity of information, which is perhaps delicate, to cloud suppliers. To safeguard information security, a typical methodology is to encode information records before the customers transfer the scrambled information into the cloud [2]. Unfortunately, it is hard to outline a protected and productive information sharing plan, particularly for element groups in the cloud.

Kallahalla et al [3] displayed a cryptographic source framework that enables secure information sharing on untrusted servers taking in to consideration the processes that assimilate documents in to document collections and scrambling each document type with a listing square secret. Whatever the instance, the listing square foot keys should really be updated and circulated to get a client refusal, together the lines, the frame needed a broad important appropriation overhead. Different plans for information sharing on untrusted servers have been proposed. [4],[5]. As it might, the complexities of client interest and renouncement in these plans are straightly expanding with the quantity of information owner and the repudiated clients.

Yu et al [6] altered and joined procedures of key strategy trait based encryption [7], intermediary re-encryption and slow re-encryption to accomplish fine-grained information access control without presentation information substance. Be that as it may, the single-proprietor way might block the usage of uses, where any part in the gathering can utilize the cloud administration to store and impart information records to others.

Lu et al [8] suggested a secure source plan with the use of cluster marks and ciphertext-arrangement feature established encryption techniques [9]. Every customer receives 2 keys after the recruitment as the delegate key is useful to decipher the info that's scrambled by the caliber predicated encryption and also the collecting indicate key will be utilize for security protecting and trace ability. However,, the refusal isn't upheld within this strategy.

Liu et al [10] exhibited a protected multi-proprietor information sharing plan, named Mona. It is guaranteed that the plan can achieve fine-grained access control and renounced clients won't have the capacity to get to the sharing information

again once they are disavowed. In any case, the plan will naturally experience the ill effects of the plot attack by the repudiated client and the cloud [13]. The disavowed client can utilize his private key to decode the encoded information record and get the secrecy information after his denial by plotting with the cloud. At the time scale of record access, being an issue of primary value, the renounced client sends his solicitation into the cloud, after which your cloud reacts the concerning authenticated information document and refusal run-down into the repudiated client without tests. The renounced client will find out the partitioning key with the aid of the attack calculation. In the last, this attack may prompt the renounced customers obtaining the sharing advice along with discovering distinct secrecy of honest-to-goodness individuals.

Zhou et al [14] displayed a harmless entry control program on data that was authenticated in spread storage by summoning section-based encryption approach. It's ensured that the plan might reach creative client refusal which combines part predicated access control procedures with encryption to procure wide information supply from the cloud. Alas the confirmations between elements aren't worried, but the master plan effortlessly have the ill results of assaults, for example, conspiracy attack. In the last, this attack can prompt insightful touchy information records.

Zou et al. [15] displayed a down to earth and adaptable key administration system for trusted cooperative registering. By utilizing access control polynomial, it is intended to accomplish proficient access control for element bunches. unfortunately, the protected path for sharing the individual changeless flexible mystery between the client and the server is not encouraged and the private key will be revealed once the individual continuous convenient mystery is acquired by the attackers.

In this paper, we propose a protected information sharing plan, which can achieve secure key requisition and information sharing for element bunch. The principle commitments of our plan include:

1. We offer a safe way of key transport without a secure correspondence station. The customers may safely obtain their keys out of collecting chief without a Certificate Authorities on account of the affirmation for people generally key of their customer.
2. Our plan can accomplish fine-grained access control, with the assistance of the gathering client list, any client in the gathering can make use of the source in the cloud and disavowed clients can't get to the cloud again after they are denied.
3. We propose a safe information sharing plan which can be protected from agreement attack. The denied clients can not have the capacity to get the first information records once they are rejected regardless of the fact that they contrive with the untrusted cloud. Our plan can accomplish secure client rejection with the assistance of polynomial capacity.
4. Our plan might encourage lively parties efficiently, when still another client unites from the amassing or perhaps a client is profiting out of the collecting, the personal keys of alternative customers do not ought to be recomputed and reestablish.
5. Security investigation to demonstrate the security of our plan. In expansion, performance of reenactments to exhibit the effectiveness of our plan.

2. REALTED WORK

In segment 2, we demonstrate the framework model and configuration objectives. In this paper, we propose a safe information sharing plan, which can accomplish secure key appropriation and information sharing for element bunch. The primary commitments of this plan include:

1. We Offer a safe Method of key Dispersion without a secure correspondence station. The customers can safely Acquire their personal keys out of amassing director free of Certification Police due to the look for men and women generally secret of their customer.
2. This plan can bring about fine-grained access control, with the assistance of the gathering client list, any client in the gathering can utilize the source in the cloud and disclaim clients can't get to the cloud again after they are renounced.
3. We indicate a safe advice sharing plan that is often protected from storyline attack. Even the repudiated customers can't need the capability to find the very first information documents as soon as they're denied regardless of the simple fact they intend with the un-trusted cloud. Our plan might reach stable client renouncement with the guidance of polynomial capacity.
4. The proposed plan can support dynamic gatherings effectively, when another client joins in the gathering or a client is disavowed from the gathering, the private keys of alternate clients don't should be recomputed and upgraded.
5. Security examination to demonstrate the security of our plan. In extension, we additionally perform reenactments to exhibit the ability of our plan.

3. SYSTEM MODEL

THREAT MODEL, SYSTEM MODEL AND DESIGN

A. Threat Model:

In this paper, we propose our plan taking into account the Dolev-Yao model [17], in which the attacker can catch, capture and combination any message at the correspondence channels. With the Dolev-Yao model, the best way to protect the data from attack.

B. System Model

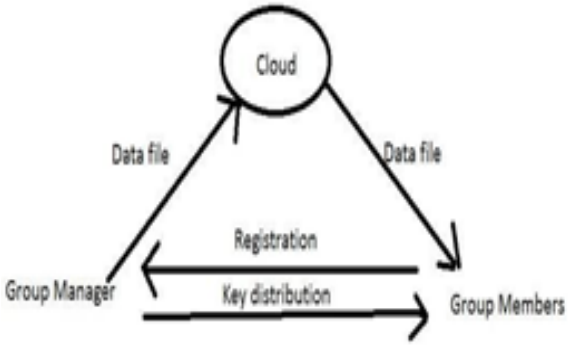

Figure 1: System model

Here the proposed model is illustrated in figure 1, the system model consists of three different entities: the cloud, a group manager and a large number of group members.

The cloud, even sustaining by the cloud hosting providers, provides space for storage for hosting datafiles at an payasyougo method. On the opposite side, the cloud will be un-trusted since the cloud providers are readily to eventually become untrusted. Hence, the cloud will take to to learn this content of their stored data.

Group manager will gain control of system parameters creation, user enrollment, additionally, client repudiation. Bunch individuals (customers) are a comprehension of sign-up customers who may store their particular special advice in to the cloud and also impart them. From the design, the collecting registration is radically changed, on account of the brand new client callup and customer rejection.

C. Design Goals:

We depict the principle plan objectives of the proposed plan including key circulation, information secrecy, access control and effectiveness as takesafter:

Key Distribution: The prerequisite of key transportation is that clients can safely get their private keys from the gathering director with no Certificate Authorities. In other existing plans, this purpose is skilful by expecting that the communication channel is secure, on the other hand, in our plan, we can accomplish it without this solid thought.

Access control: First, collect individuals can make use of the cloud asset for information stockpiling and information sharing. Second, unapproved clients can't get to the cloud asset whenever, and disavowed clients will be unfitted for utilizing the cloud asset again once they are renounced.

4. THE PROPOSED SCHEME

A. Preliminaries

Biliner Maps:

Let H_1 and H_2 be additive cyclic groups of the same prime order r[18]. Let $e: H_1 \times H_1 \rightarrow H_2$ denote a bilinear map created with the following properties:

1. Bilinear: For all $b, c \in Z_r$ and $P, Q \in G$, $e(aP, bQ) = e(P, Q)$.
2. Nondegenerate: 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 $P, Q \in G$.

Definition 1(Basic Diffe-Hellman Problem (BDHP) Assumption:

Specified base point P and a value γ ∈ It is easy to calculate γ.P. However, given P,γ.P, it is infeasible to calculate γ since of the discrete algorithm problem.

Definition 2(Decisional Diffie-Hellman Problem (DDHP) Assumption):

Related to definition 1, given

Notation	Description
IDEi	the identity of user i
IDdatai	the identity of data i
qk	the public key of the user
tk	the corresponding private that Needs to be negotiated with the group manager
KEY=(x_i,A_i,B)	the private key which is Distributed to the user from the Group manger and used for data Sharing

base point Q and $aQ,(a+b)Q$, it is infeasible to compute b Q.

Definition 3(Weak Bilinear Diffie-Hellman Exponent):

For unknown e(X, P)a

Encpk()	symmetric encryption Algorithm used the encryption key k
ASENC()	asymmetric encryption Algorithm used the encryption key
ULI	group user list
DLI	data list

5. SECURITY ANALYSIS

Here, we show the security of our scheme in terms of key distribution, access control and data confidentiality.

A. Key Distribution Theorem 1:

Within this strategy, the communicating entities could safely consult with the people crucial qk and devote the private secret KEY = {xi , Ai , Bi} undefined for users with no Certificate Authorities and secure communication stations. Proof: During user enrollment, an individual sends his public key qk and also a arbitrary number v1€Zq into the band boss using his individuality IDEi. Afterward a group supervisor calculates corresponding value,S. Moreover, the consumer may verify the identity of this team supervisor by the equation:

$S \cdot e(v \cdot f(qk \,||\, ac \,||\, IDE)\, Q, X) = e(V, Q).$

The qk gets to be the negotiated public-key after powerful confirmation equation. Afterward your group manager can securely allocate the private key KEY, that will be useful for data sharing, for users together with the assistance of people key and with no Certificate Authorities and secure communication stations

$$
\begin{aligned}
S \cdot e(v_1 \cdot f(qk \,||\, ac \,||\, IDE_i) \cdot Q, X) &= e(Q, Q)^{s} \cdot e(v_1 \cdot f(qk \,||\, ac \,||\, IDE_i) \cdot Q, X) \\
&= e(Q, Q)^{s} \cdot e(v_1 \cdot f(qk \,||\, ac \,||\, IDE_i) \cdot Q, \gamma Q) \\
&= e(Q, Q)^{s} \cdot e(\gamma \cdot v_1 \cdot f(qk \,||\, ac \,||\, IDE_i) \cdot Q, Q) \\
&= e(Q, Q)^{s} \cdot e(Q, Q)^{\gamma v_1 \cdot f(qk \,||\, ac \,||\, IDE_i)} \qquad (1) \\
&= e(Q, Q)^{k \gamma \cdot v_1 \cdot f(qk \,||\, ac \,||\, IDE_i)} \\
&= e((s + \gamma \cdot v_1 \cdot f(qk \,||\, ac \,||\, IDE_i))q, q) \\
&= e\, v, q
\end{aligned}
$$

$e(X, f1(UL)) \quad = e(P, sig \quad (ULI)).$

When attacker wants to confirm the verification, for unknown γ € X. on the other hand this oppose with the DDHP assumption. As a result, the user can authenticate the identity of the group manager by the confirmation equation above and they can firmly negotiate the public key without any Certificate Authorities and secure communication channels. In addition to this, the scheme can assurance the user and the group manager to attain the accurate message which is sent by the legal Communication entity. in the third step of user registration, the group manager carry out calculations after receiving the message from the user. First of all, he decrypts ASENC sk(IDEi ,v1, ac) and obtains IDEi ,v1 . Then he evaluates them with received IDEi. Message and the random number V1 in the first step .If either of them are not equal the manager stops the registration and informs the user to send new request in the third step. Furthermore, the user transmits a random number v2 to the manager and the manager encrypts it with the public key qk. so, the attacker cannot deceive the Legal users and our scheme can be protected from repeat attack.

B. Access Control:

Theorem : Make money from the category user list, that will be Create by the category manager, our strategy may gain competent access control. Proof. The access controller is predicated upon the security of this category user list, that will be signed with the group Supervisor with his trademark sig (ULI) = gram finch (ULI) which procedure is normally carried from the cloud system. The cloud contrasts the individuality of this team supervisor by analyzing the equation. The correctness of the above verification equation is based on the following equation.

$e(X, f1(UL)) \quad = e(P, sig \quad (ULI)).$

The correctness of the above verification equation is based on the following equation.

$e(X, f1(UL)) \quad = e(\gamma P, (ULI)).$

Assume that an attacker can fail to remember the signature, which means that given Q, needs to compute γ, where $\gamma \in Z_q^*$. Thus, there is no one except the group manager that can alter and update the group user list to make sure that the resources in the cloud is available for the legal users and engaged for the revoked users and attackers.

6. CONCLUSION

Within this paper we now summarize a secure against agreement information-sharing arrange to get element bunches from the cloud. Within our plan, the customers may safely acquire their own keys out of amassing director Certificate Authorities and protected spam stations. Likewise our plan might reinforce dynamic parties efficiently, when still another client unites from the gathering or perhaps a customer is refused by the collecting, the personal keys of alternative customers do not should be recomputed as well as re designed. Additionally, ours plan might reach stable client repudiation, the disavowed customers can't have the capacity to acquire the very first information records as soon as they're denied whatever chance they scheme with the un-trusted cloud.

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 omputing,” Comm. ACM, vol. 53, no. 4, pp. 50-58, Apr.2010.

[2] S. Kamara and K. Lauter, “Cryptographic Cloud Storage,” Proc. Int’l Conf.Financial Cryptography and Data Security (FC), pp.136- 149, Jan. 2010.

[3] M. Kallahalla, E. Riedel, R. Swaminathan, Q.Wang, and K. Fu, “Plutus: ScalableSecure File Sharing on Untrusted Storage,” Proc. USENIX Conf. File and Storage Technologies, pp. 29-42, 2003.

[4] 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.

[5] 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.

[6] 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.

[7] 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

[8] 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.

[9] B. Waters, "Ciphertext-Policy Attribute-Based Encryption: An Expressive, Efficient, and Provably Secure Realization," Proc. Int'l Conf.http://eprint.iacr.org/2008/290.pdf, 2008

[10] 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.

[11] 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.

[12] C. Delerablee, P. Paillier, and D. Pointcheval, "Fully Collusion Secure Dynamic Broadcast Encryption with Constant-Size Ci-phertexts or Decryption Keys," Proc.First Int'l Conf. Pairing-Based Cryptography, pp. 39-59, 2007.

[13] Zhongma Zhu, Zemin Jiang, Rui Jiang, "The Attack on Mona: Secure Multi-Owner Data Sharing for Dynamic Groups in the Cloud," Proceedings of 2013 International Conference on Information Science and Cloud Computing (ISCC 2013), Guangzhou, Dec.7, 2013, pp. 185-189.

[14] 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.

[15] Xukai Zou, Yuan-shun Dai, and Elisa Bertino, "A practical and flexible key management mechanism for trusted collaborative computing," INFOCOM 2008, pp. 1211-1219.

[16] M. Nabeel, N. Shang, and E. Bertino, "Privacy preserving policy based content sharing in public clouds," IEEE Trans. on Know. and Data Eng., vol. 25, no. 11, pp. 2602-2614, 2013.

[17] Dolev, D., Yao A. C., "On the security of public key protocols", IEEE trans. on Information Theory, vol. IT-29, no. 2, pp. 198–208, 1983

[18] Boneh Dan, Franklin Matt, "Identity- based encryption from the weil pairing,"