Volume 2, Issue 12, December-2015, pp. 1113-1118 ISSN (O): 2349-7084

International Journal of Computer Engineering In Research Trends

Available online at: www.ijcert.org

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

[1]G.Mercy Vimala, [2]R.Vara Prasad ,[3]P.Rama Rao

[1]*Pursuing M.Tech, CSE Branch, Dept of CSE*
[2]*Assistant Professor, Department of Computer Science and Engineering*
[3]*Assistant Professor, Department of Computer Science and Engineering*
[1,2,3]*G.Pullaiah College of Engineering and Technology, Kurnool, Andhra Pradesh, 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, due to the never-ending change of the enrolment, sharing information while giving protection saving is still a testing issue, particularly for an untrusted cloud because of the agreement attack. In addition, for existing plans, the security of key dispersion depends on the safe communication channel, then again, to have such channel is a solid feeling and is difficult for practice. In this paper, we propose a safe information sharing plan for element individuals. Firstly, we propose a safe route for key dispersion with no safe correspondence channels, and the clients can safely acquire their private keys from gathering administrator. Besides, the plan can accomplish fine-grained access control, any client in the gathering can utilize the source in the cloud and refused clients can't get to the cloud again after they are 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.

Keywords— Access control, Privacy-preserving, Key distribution, Cloud computing

1. INTRODUCTION:

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 supply framework that empowers secure information sharing on untrust servers taking into

account the procedures that isolating documents into filegroups and scrambling each file_group with a record square key. In any case, the record square keys should be upgraded and circulated for a client denial, along these lines, the framework had a extensive key 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] proposed a protected origin plan by utilizing bunch marks and ciphertext-arrangement characteristic based encryption methods [9]. Every client gets two keys after the recruitment while the assign key is utilized to decode the information which is scrambled by the quality based encryption and the gathering mark key is make use for security protecting and traceability. Then again, the denial is not upheld in this plan.

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. In the period of document access, as a matter of first importance, the renounced client sends his solicitation to the cloud, then the cloud responds the relating scrambled information record and denial rundown to the repudiated client without checks. Next, the renounced client can figure the decoding key with the assistance of the assault calculation. At last, this assault can prompt the renounced clients getting the sharing information and uncovering different secrecy of honest to goodness individuals.

Zhou et al [14] displayed a safe access control plan on scrambled information in distributed storage by summoning part based encryption method. It is guaranteed that the plan can accomplish creative client denial that joins part based access control approaches with encryption to secure wide information supply in the cloud. unfortunately, the confirmations between elements are not concerned, the plan effortlessly experience the ill effects of assaults, for instance, conspiracy assault. At last, this assault can prompt enlightening touchy information documents.

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 give a safe approach to key transport with no protected correspondence channels. The clients can safely obtain their private keys from gathering chief with no Certificate Authorities because of the confirmation for people in general key of the client.

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 can encourage dynamic gatherings effectively, when another client joins in the gathering or a client is renounced from the gathering, the private keys of alternate clients don't should be recomputed and renovate.

5. security investigation to demonstrate the security of our plan. In expansion, performance of

reenactments to exhibit the effectiveness of our plan.

2. RELATED 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 thisplan include:

1.We give a safe approach to key dispersion with no protected correspondence channels. The clients can safely acquire their private keys from gathering director with no Certificate Authorities because of the check for people in general key of the client.

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 suggest a safe information sharing plan which can be protected from plot attack. The repudiated clients can not have the capacity to get the first information documents once they are denied in spite of of the fact that they plan with the untrusted cloud. Our plan can achieve secure client renouncement with the assistance 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 GOALS

3.1 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.

3.2 System Model

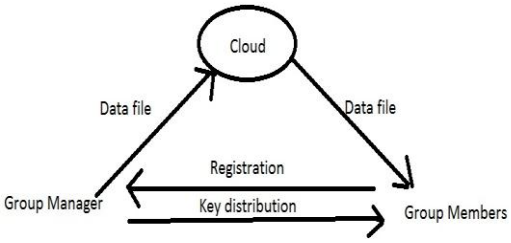

Figure 1: System model

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, sustaining by the cloud service providers, provides storage space for hosting data files in a pay-as-you-go manner. on the other hand, the cloud is untrusted since the cloud service providers are easily to become untrusted. Therefore, the cloud will try to learn the content of the stored data. Group manager will obtain charge of system parameters generation, user registration, also, client repudiation. Bunch individuals (clients) are an arrangement of sign up clients that will store their own particular information into the cloud and impart them to others. In the plan, the gathering enrollment is powerfully changed, because of the new client call-up and client denial.

3.3 Design Goals :

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

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.

Information classification: Data secrecy requires that unapproved clients including the cloud are unequipped for taking in the substance of the put away information. To keep up the accessibility of information secrecy for element gatherings is still an essential and testing issue. In particular, renounced clients can't unscramble the put away information document after the denial.

Effectiveness: Any gathering part can store and impart information records to others in the gathering by the cloud. Client repudiation can be accomplished without including the others, which implies that the remaining clients don't have to overhaul their private keys.

4.THE PROPOSED SCHEME

4.1 Preliminaries

4.1.1 Bilinear Maps

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

1. Bilinear: For all $b, c \in Z_r$ and $P, Q \in G_1$, $e(aP, bQ) = e(P, Q)$.
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 base point *Q* and *aQ,(a+b)Q*, it is infeasible to compute b *Q*.

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
Encp$_k$()	symmetric encryption algorithm used the encryption key k
ASENC()	asymmetric encryption Algorithm used the encryption key
ULI	group user list
DLI	data list

Definition 3(Weak Bilinear Diffie-Hellman Exponent) : For unknown $e(X, P)_a$

5. SECURITY ANALYSIS

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

5.1 Key Distribution Theorem 1. In this scheme, the communication entities can securely consult the public key qk and allocate the private key KEY = $\{x_i , A_i , B_i\}$to users without any Certificate Authorities and secure communication channels.

Proof: In user registration, the user sends his public key qk and a random number v1€Zq to the group manager with his identity IDE_i .Then the group manager computes corresponding value V,S. Furthermore, the user can confirm the identity of the group manager by the equation: $S \cdot e(v \cdot f(qk \| ac \| IDE) \cdot Q, X) = e(V, Q)$.The *qk becomes* the negotiated public key after successful verification equation. Then the group manager can firmly allocate the private key *KEY* , which is used for data sharing, to users with the help of public key and without any Certificate Authorities and secure communication channels.

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

$$e(X, f_i(UL)) = e(P, sig(ULI)).$$

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.

5.2 Access Control: Theorem 2: profit from the group user list, which is Produce by the group manager, our scheme can achieve capable access control. Proof. The access control is based on the security of the group user list, which is signed by the group Manager with his signature sig $(ULI) = \gamma\ f_1\ (ULI)$ and this process is generally carry out by the cloud. The cloud conforms the identity of the group manager by examining the equation The correctness of the above verification equation is based on the following equation.

$e\left(X, f_1(UL)\right) \quad = e\left(P, sig\ \ (ULI)\right)$.

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

$$e((X, f_{1}\ ULI)) = e((\quad \gamma P, f_{1}\ ULI))$$

1.1.2 $e\left(Q, f_1(ULI)\right)_{\gamma}$

1.1.3 $e\left(Q, \gamma f_1(ULI)\right)$

1.1.4 $e\left(Q, sig\ (ULI)\right)$

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.

5. CONCLUSION

In this paper, we outline a protected against agreement information sharing plan for element bunches in the cloud. In our plan, the clients can safely acquire their private keys from gathering director Certificate Authorities and secure correspondence channels. Likewise, our plan can bolster dynamic gatherings proficiently, when another client joins in the gathering or a client is denied from the gathering, the private keys of alternate clients don't should be recomputed and redesigned. In addition, our plan can accomplish secure client repudiation, the disavowed clients can not have the capacity to get the first information records once they are denied regardless of the possibility that they plot with the untrusted 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,"

Lecture Notes in Computer Science, vol. 2139 LNCS, pp. 213-229, 2001

