IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 7, July 2016

A Protected Anti Collection Data Sharing and Secure user Revocation Scheme for Dynamic Groups in the Cloud

Dr.V.Goutham[1], Mrs. K. Srilatha[2], Ms. M. Swapna[3]

Professor, CSE, TKREC, Telangana, India [1]

Assistant Professor, CSE, TKREC, Telangana, India [2]

CSE, TKREC, Telangana, India [3]

Abstract: Endorsed from Cloud Computing, clients can achieve a thriving and modest practice for information sharing among gathering individuals in the cloud with the characters of low upkeep and slight administration cost. Then, security authorizations to the sharing information records will be given since they are outsourced. Extremely, due to the never-ending change of the enrolment, sharing information while giving protection saving is still a testing issue, predominantly for an untrusted cloud since of the agreement attack. In accumulation, for standing plans, the security of key dispersion be contingent on the harmless communication channel, then again, to have such channel is a solid feeling and is difficult for practice. A safe route for key dispersion with no safe correspondence channels, and the clients can safely acquire their private keys from gathering administrator is proposed. 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.

Keywords: Access control, Privacy-preserving, Key distribution, Cloud computing.

I. 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 un trust servers taking into account the procedures that isolating documents into file groups 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

DOI 10.17148/IJARCCE.2016.57142

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. Zuo 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.

II. 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 this plan 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 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.

III. 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

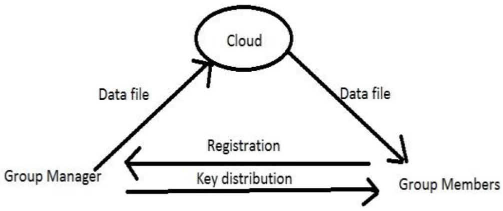


Figure 1: System model

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,

DOI 10.17148/IJARCCE.2016.57142

information secrecy, access control and effectiveness as takes after.

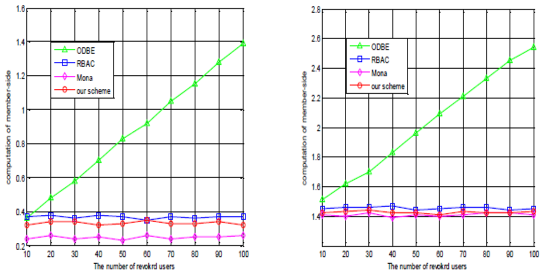
Key Distribution: The prerequisite of key transportation is that clients can safely get their private keys from the gathering director with no Certificate Authorities. In other existing plans, this purpose is skilful by expecting that the communication channel is secure, on the other hand, in our plan, 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.

IV. PERFORMANCE EVALUATION

We make the performance simulation with NS2 and compare with Mona in [10] and the original dynamic broadcast encryption (ODBE) scheme in [12]. Without loss of generality, we set and the elements in and to be 161 and 1,024 bits, respectively. In addition, we assume the size of the data identity is 16 bits, which yield a group capacity of data files. Similarly, the size of user and group identity are also set 16 bits. Both group members and group managers processes are conducted on a laptop with Core 2 T5800 2.0 GHz, DDR2 800 2G, Ubuntu 12.04 X86. The cloud process is implemented on a laptop with Core i7-3630 2.4 GHz, DDR3 1600 8G, Ubuntu 12.04 X64. We select an elliptic curve with 160 bits group order.



(a) Generating a 10 MB file (b) Generating a 100 MB file

Figure 2: Comparison on computation cost of members for file upload among ODBE, RBAC

As illustrated in figure 2, we list the comparison on computation cost of members for file upload among ODBE, RBAC, Mona and our scheme. It is obviously observed that the computation cost for members in our scheme is irrelevant to the number of revoked users. The reason is that in our scheme, we move the operation of user revocation to the group manager so that the legal clients can encrypt the data files alone without involving information of other clients, including both legal and revoked clients. On the contrary, the computation cost increases with the number of revoked users in ODBE. The reason is that several operations including point multiplications and exponentiations have to be performed by clients to compute the parameters in ODBE.

V. 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, KuiRen, 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.

DOI 10.17148/IJARCCE.2016.57142

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 Ciphertexts 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] XukaiZou, 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,"

BOIGRAPHIES

Dr V. Goutham is a Professor and Head of the Department of Computer Science and Engineering at Teegala Krishna Reddy Engineering College affiliated to J.N.T.U Hyderabad. He received Ph.d from Acharya Nagarjuna University and M.Tech from Andhra University. He worked for various MNC Companies in Software Testing and Quality as Senior Test Engineer. His research interests are Software Reliability Engineering, software testing, software Metrics, and cloud computing.

Mrs. K. Srilatha is working as a Assistant Professor in the Department of Computer Science and Engineering at Teegala Krishna Reddy Engineering College affiliated to J.N.T.U Hyderabad

Ms. M. Swapna Department of Computer Science and Engineering at Teegala Krishna Reddy Engineering College affiliated to J.N.T.U Hyderabad.

DOI 10.17148/IJARCCE.2016.57142