

Integrity Auditing for Outsourced Dynamic Cloud Data with Group User Revocation

P.FARZANA, A.HARSHAVARDHAN

¹M.Tech (CSE), Priyadarshini Institute of Technology & Science for women's

²Assistant Professor (Dept.of CSE), Priyadarshini Institute of Technology & Science for women's

Abstract:- The imminent of the cloud computing makes storage outsourcing turns into a rising pattern, which advances the privacy for remote data auditing an intriguing issue that showed up in the literature. Recently a few researchers consider the issue of secure and productive public data respectability auditing for shared dynamic data. Be that as it may, these schemes are still not secure against the conspiracy of cloud storage server and revoked group users amid client denial reasonable cloud storage framework. In this paper, we make sense of the understanding attack in the presented system and give an adept public auditing scheme with secure group client repudiation in view of Asymmetric Group Key Agreement and group signature. Our Scheme supports effective dynamic user revocation with public auditing.

Keywords –Data Sharing, Dynamic Groups, user revocation, public auditing.

1. INTRODUCTION

Cloud computing, with the uniqueness of vital data sharing and low support, offers an improved misuse of assets. In cloud processing, cloud administration suppliers offer an idea of unending storage room for customers to host data [1]. It can help customers to diminish their monetary straightforwardness of data administrations by exchanging the neighborhood administration's framework into cloud servers. Then again, security worry turns into the fundamental disadvantage as we now outsource the capacity of data, which is potentially agreeable, to cloud suppliers. To take care of data privacy, a general move towards is to encrypt data documents before the customers transfer the encrypted data into the cloud [2]. Unfortunately, it is hard to outline a safe and effective data sharing plan, particularly for dynamic groups in the cloud.

Yu et al [6] oppressed and joined techniques of key policy attribute-based encryption [7], proxy re-encryption and lazy re-encryption to attain fine-grained data access control without revealing data

contents. On the other hand, the single-owner manner may delay the achievement of applications, where any member in the group can use the cloud service to store and divide data files with others.

Kallahalla et al [3] offered a cryptographic storage system that allow secure data sharing on unreliable servers based on the methods that dividing files into file groups and encrypting each file group with a file-block key. Conversely, the file-block keys need to be updated and distributed for a user revocation, so, the system had a heavy key distribution overhead. Additional schemes for data sharing on untrusted servers have been proposed in [4],[5]. Still, the difficulty of user participation and revocation in these schemes is linearly rising with the number of data owners and the revoked users.

Nabeel et al. [16] planned a privacy preserving policy-based content sharing scheme in public clouds. Yet, this scheme is not secure as the weak protection of assurance in the phase of identity token issue.

Zhou et al [14] offered a secure access control scheme on encrypted data in cloud storage by

invoking role-based encryption technique. It is maintained that the scheme can attain well-organized user revocation that merge role-based access control policies with encryption to secure large data storage in the cloud. Regrettably, the verifications between entities are not disturbed, the scheme easily suffer from attacks, for example, collusion attack. To conclude, this attack can lead to revealing sensitive data files.

Liu et al [10] proposed a secure multi-owner data sharing scheme, named Mona. It is claimed that the scheme can achieve fine-grained access control and revoked users will not be able to access the sharing data again once they are revoked. Conversely, the scheme will easily suffer from the collusion attack by the revoked user and the cloud [13]. The revoked user can use his private key to decrypt the encrypted data file and get the secret data after his revocation by combining with the cloud. In the stage of file access, first of all, the2. revoked user throws his request to the cloud, then the cloud act in response the corresponding encrypted data file and revocation list to the revoked user without verifications. Next, the revoked user can calculate the decryption key with the help of the attack algorithm. Lastly, this attack can guide to the revoked users receiving the sharing data and releasing other secrets of legal members.

Lu et al [8] anticipated a secure derivation scheme by leveraging group signatures and ciphertext-policy attribute-based encryption techniques [9]. Each user acquire two keys after the registration while the attribute key is used to decrypt the data which is encrypted by the attribute-based encryption and the group signature key is used for privacy-preserving and traceability. On the other hand, the revocation is not supported in this scheme.

Zou et al. [15] presented a sensible and flexible key management method for trusted joint computing. By leveraging access control polynomial, it is designed to achieve well-organized access control for dynamic groups. Regrettably, the secure way for sharing the private permanent portable secret between the user and the server is not sustain and the private key will be revealed once the personal everlasting portable secret is obtained by the invader/attackers.

2. ASSOCIATED WORK

In this paper, we recommend a secure data sharing scheme, which can achieve secure key distribution and data sharing for dynamic group. The main contributions of our scheme include:

1. Our scheme is able to carry dynamic groups efficiently, when a new user joins in the group or a user is revoked from the group, the private keys of the other users do not need to be recomputed and altered.
2. We suggest a secure data sharing scheme which can be confined from collusion attack. The revoked users can not be capable to get the original data files once they are revoked even if they combine with the untrusted cloud. Our scheme can accomplish secure user revocation with the help of polynomial function.
3. We offer security examination to prove the security of our scheme. In addition, we also perform imitations to exhibit the competence of our scheme.
4. We provide a secure way for key distribution without any secure communication channels. The users can firmly obtain their private keys from group manager without any Certificate Authorities due to the verification for the public key of the user.
5. Our scheme can accomplish fine-grained access control, with the help of the group user list, any user in the group can use the source in the cloud and revoked users cannot access the cloud again after they are revoked.

3. 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

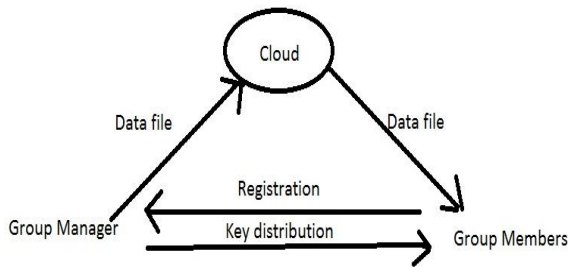


Figure 1: System model

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:

4. SECURITY ANALYSIS

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

4.1 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 $v \in \mathbb{Z}_q$ to the group manager with his identity IDE_i . Then the group manager computes corresponding value V, S .

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.

Furthermore, the user can confirm the identity of the group manager by the equation:

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

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.

$$\begin{aligned}
 S &= (v_1 \cdot f(qk \parallel ac \parallel IDE_i) \cdot Q, X) = e(Q, Q) \cdot e(v_1 \cdot f(qk \parallel ac \parallel IDE_i) \cdot Q, X) \\
 &= e(Q, Q) \cdot e(v_1 \cdot f(qk \parallel ac \parallel IDE_i) \cdot Q, \gamma Q) \\
 &= e(Q, Q) \cdot e(\gamma \cdot v_1 \cdot f(qk \parallel ac \parallel IDE_i) \cdot Q, Q) \\
 &= e(Q, Q) \cdot e(Q, Q)^{\gamma \cdot v_1 \cdot f(qk \parallel ac \parallel IDE_i)} \\
 &= e(Q, Q)^{\gamma \cdot v_1 \cdot f(qk \parallel ac \parallel IDE_i)} \\
 &= e((s + \gamma \cdot v_1 \cdot f(qk \parallel ac \parallel IDE_i))q, q) \\
 &= e \gamma, q \\
 e(X, f(UL)) &= e(P, sig(UL))
 \end{aligned} \tag{1}$$

When attacker wants to confirm the verification, they wants to compute $V = (r + \gamma \cdot v_1 \cdot f(qk \parallel ac \parallel IDE_i)) \cdot Q$ which means that q,s, needs to Compute $V = (r + \gamma \cdot v_1 \cdot f(qk \parallel ac \parallel IDE_i)) \cdot Q$

For unknown $\gamma \in X$. 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 $ASENC_{sk}(IDE_i, v1, ac)$ and obtains $IDE_i, v1$. Then he evaluates them with received IDE_i . Message and the random number V_1 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.

$$\begin{aligned}
 e((X, f_1(ULI))) &= e((\gamma P, f_1(ULI))) \\
 &= e(Q, f_1(ULI))^\gamma \\
 &= e(Q, \gamma f_1(ULI)) \\
 &= e(Q, sig(ULI))
 \end{aligned}$$

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 plot an ensured against understanding data sharing agreement for element group in the cloud. In our arrangement, the customers can securely gain their private keys from social affair executive Authentication Powers and secure correspondence channels. Moreover, our arrangement can support dynamic get-togethers capably, when another customer joins in the get-together or a customer is denied from the social occasion, the private keys of substitute customers ought not to be recomputed and upgraded. Likewise, our arrangement can finish secure customer renouncement; the repudiated customers can not have the ability to get the first data records once they are prevented in any case from claiming the likelihood 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 Computing," *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: Scalable Secure 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. Deleralee, 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] 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