A Trustworthy Data Sharing Solution for Dynamic Groups in the Cloud, Ensuring Security and Preventing Collusion

Kondragunta Rama Krishnaiah, Professor, Department of Computer Science and Engineering, R K College of Engineering, Vijayawada - 521456, Andhra Pradesh, India, email: kondraguntark@gmail.com

Alahari Hanumant Prasad, Professor, Department of Computer Science and Engineering, R K College of Engineering, Vijayawada - 521456, Andhra Pradesh, India, email: hanuma.alahari@gmail.com

ABSTRACT

Utilizing the advantages of cloud computing, users can now easily and cost-effectively share data among group members within the cloud. This process comes with low maintenance and management costs, making it highly convenient. However, ensuring the security of shared data is crucial, especially when outsourcing it to an untrusted cloud where collusion attacks can be a threat due to the dynamic nature of group membership._Presently, existing schemes rely on secure communication channels for key distribution, which is not always practical as these channels are not always available. To address these challenges, we have developed a secure data sharing scheme for dynamic groups. Our approach allows for key allocation without the need for secure communication channels, making it more feasible for practical use. Group administrators can securely provide private keys to users._Moreover, our scheme offers fine-grained entrance control, granting any user in the group access to the cloud-based resources, while effectively revoking access for users who are no longer part of the group. This way, former members cannot regain access by collaborating with the untrusted cloud, protecting the shared data from potential collusion attacks._Additionally, our method employs AES encryption during data processing, ensuring secure data sharing among cloud users. The storage overhead and encryption costs are minimal and scalable according to the number of users in the group. This ensures a protected multi-owner data sharing plan for dynamic groups in the cloud, with each user having the ability to safely share data with others._Our approach offers multiple levels of security for sharing data, accommodating various scenarios and group compositions. It guarantees that previous users do not need to update their private keys when new users join or when a user is revoked from the group. This efficiency ensures a smooth and seamless data sharing experience for all members involved.

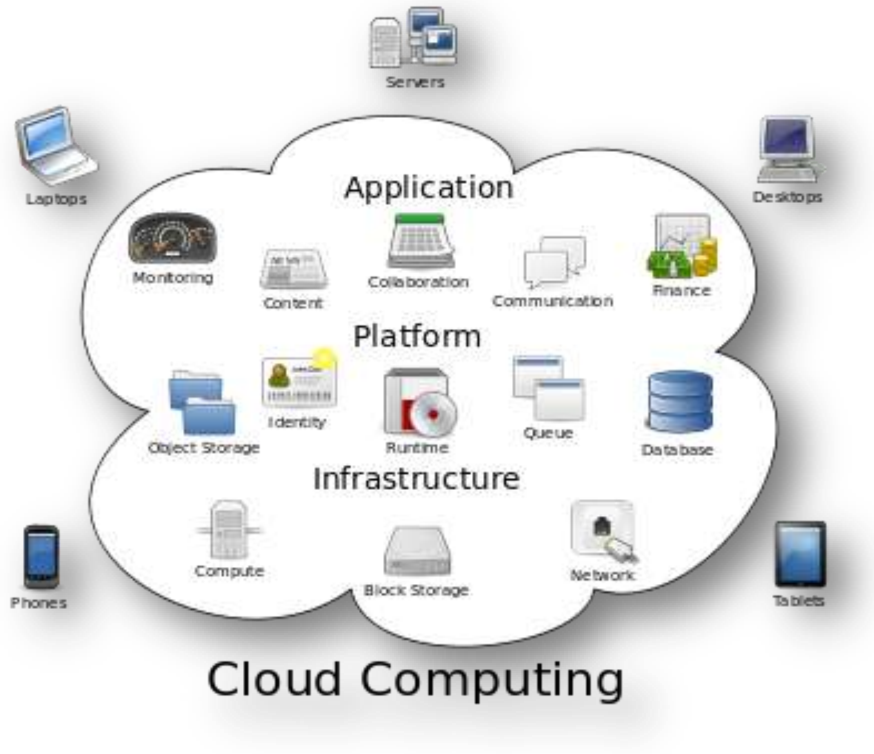
Keywords: cloud computing, data sharing, anti-collusion system, cloud security.

1. Introduction

Cloud computing is the use of computing resources (hardware and software) that are delivered as a service over a network (typically the Internet). The name comes from the common use of a cloud-shaped symbol as an abstraction for the complex infrastructure it contains in system diagrams. Cloud computing entrusts remote services with a user's data, software and computation. Cloud computing consists of hardware and software resources made available on the Internet as managed third-party services. These services typically provide access to advanced software applications and high-end networks of server computers.

How Cloud Computing Works?

The goal of cloud computing is to apply traditional supercomputing, or high-performance computing power, normally used by military and research facilities, to perform tens of trillions of computations per second, in consumer-oriented applications such as financial portfolios, to deliver personalized information, to provide data storage or to power large, immersive computer games. The cloud computing uses networks of large groups of servers typically running low-cost consumer PC technology with specialized connections to spread data-processing chores across them. This shared IT infrastructure contains large pools of systems that are linked together. Often, virtualization techniques are used to maximize the power of cloud computing.



Structure of cloud computing

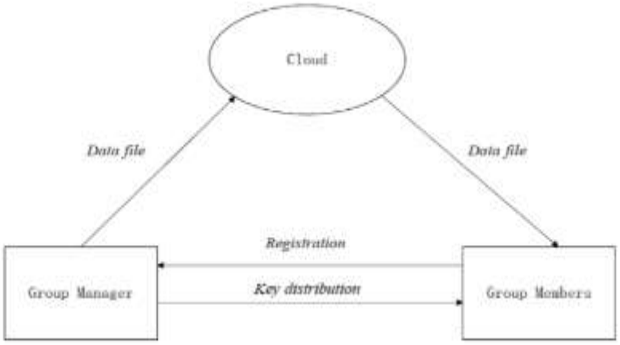
2. Related work

Cloud computing, with the characteristics of intrinsic data sharing and low maintenance, provides a better utilization of resources. In cloud computing, cloud service providers offer an abstraction of infinite storage space for clients to host data [1]. It can help clients reduce their financial overhead of data managements by migrating the local managements system into cloud servers. However, security concerns become the main constraint as we now outsource the storage of data, which is possibly sensitive, to cloud providers. To preserve data privacy, a common approach is to encrypt data files before the clients upload the encrypted data into the cloud [2]. Unfortunately, it is difficult to design a secure and efficient data sharing scheme, especially for dynamic groups in the cloud. Kallahalla et al [3] presented a cryptographic storage system that enables secure data sharing on untrustworthy servers based on the techniques that dividing files into file groups and encrypting each file_group with a file-block key. However, the file-block keys need to be updated and distributed for a user revocation, therefore, the system had a heavy key distribution overhead. Other schemes for data sharing on untrusted servers have been proposed in [4] and [5]. However, the complexities of user participation and revocation in these schemes are linearly increasing with the number of data owners and the revoked users. Yu et al [6] exploited and combined techniques of key policy attribute-based encryption [7], proxy re-encryption and lazy re-encryption to achieve fine-grained data access control without disclosing data contents. However, the single-owner manner may hinder the implementation of applications, where any member in the group can use the cloud service to store and share data files with others. Lu et al [8] proposed a secure provenance scheme by leveraging group signatures and cipher text-policy attribute-based encryption techniques [9]. Each user obtains two keys after 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. However, the revocation is not supported in this scheme. Liu et al [10] presented 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 shared data again once they are revoked. However, 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 conspiring with the cloud. In the phase of file access, first of all, the revoked user sends his request to the cloud, then the cloud responds the corresponding encrypted data file and revocation list to the revoked user without verifications. Next, the revoked user can compute the decryption key with the help of the attack algorithm. Finally, this attack can lead to the revoked users getting the sharing data and disclosing other secrets of legitimate members. Zhou et al [14] presented a secure access control scheme on encrypted data in cloud storage by invoking role-based encryption technique. It is claimed that the scheme can achieve efficient user revocation that combines role-based access control policies with encryption to secure large data storage in the cloud. Unfortunately, the verifications between entities are not concerned, the scheme easily suffers from attacks, for example, collusion attack. Finally, this attack can lead to disclosing sensitive data files. Zou et al. [15] presented a practical and flexible key management mechanism for trusted collaborative computing. By leveraging access control polynomial, it is designed to achieve efficient access control for dynamic groups. Unfortunately, the secure way for sharing the personal permanent portable secret between the user and the server is not supported and the private key will be disclosed once the personal permanent portable secret is obtained by the attackers. Nabeel et al. [16] proposed a privacy preservation policy-based content sharing scheme in public clouds. However, this scheme is not secure because of the weak protection of commitment in the phase of identity token issuance. Our scheme can achieve 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. We propose a secure data sharing scheme which can be protected from collusion attack. The revoked users can not be able to get the original data files once they are revoked even if they conspire with the untrusted cloud. Our scheme can achieve secure user revocation with the help of polynomial function. Our scheme is able to support dynamic groups efficiently. When a new user joins the group or a user is revoked from the group, the private keys of the other users do not need to be recomputed and updated. We provide security analysis to prove the security of our scheme.

3. PROPOSED SYSTEM

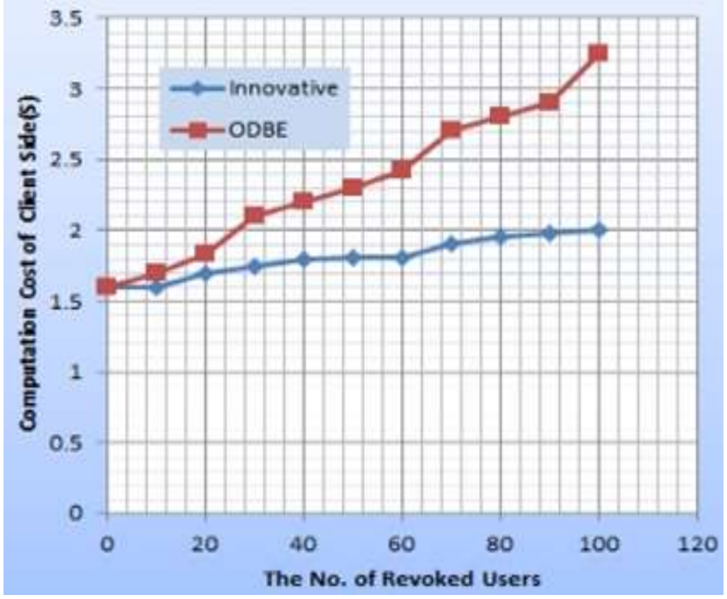
- ✓ The computation cost is irrelevant to the number of revoked users in the RBAC scheme. The reason is that no matter how many users are revoked, the operations for members to decrypt the data files almost remain the same.
- ✓ The cost is irrelevant to the number of the revoked users. The reason is that the computation cost of the cloud for file upload in our scheme consists of two verifications for signature, which is irrelevant to the number of the revoked users. The reason for the small computation cost of the cloud in the phase of file upload in RBAC scheme is that the verifications between communication entities are not concerned in this scheme.
- ✓ In our scheme, the users can securely obtain their private keys from group manager Certificate Authorities and secure communication channels. Also, our scheme is able to support 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 updated.

We offer a secure data sharing scheme for vibrant members. Firstly, we propose a secure way for key allocation without any secure communication channels and the users can securely obtain their private keys from group administrator. Secondly, our scheme can achieve fine-grained entrance control, any user in the group can use the basis in the cloud and revoked users cannot entrée the cloud another time after they are revoked. Thirdly we can protect the scheme from collusion hit, which means that revoked users cannot get the unique data file even if they work together with the entrusted cloud. It will also grant data from the cloud to group members. In this proposition a protected multi- proprietor data sharing plan for element bunch in the cloud by giving AES encryption while procedure the data any cloud client can safely impart data to others. In the interim the capacity overhead and encryption calculation expense of the plan are free with the quantity dictions clients. We propose a secure data sharing method for dynamic members to provide secure key distribution without any secure communication approach and the users securely obtain their security keys from group manager. It provides multiple levels of security to share data number of multi-owner manner. First the user selects the text-based password is known as OTP is generated automatically and sent to corresponding user e-mail account. The new part is added to the gathering security key is given to the part. The documents which are transferred present in encoded structure and the records can be seen by gathering part as they have the authentic key. The cloud maintained by the cloud service providers provides storage space for hosting data files in a pay-as-you-go manner. However, the cloud is entrusted since the cloud service providers are easily to become entrusted. Therefore, the cloud will try to learn the content of the stored data. Group manager takes charge of system parameters generation, user registration, and user revocation.



Advantages of Proposed System:

Our scheme is able to support dynamic groups efficiently. When a new user joins the group or a user is revoked from the group, the private keys of the other users do not need to be recomputed and updated. We provide security analysis to prove the security of our scheme. The cost is irrelevant to the number of the revoked users. The reason is that the computation cost of the cloud for file upload in our scheme consists of two verifications for signature, which is irrelevant to the number of the revoked users. The remaining users are used to update security preserved data sharing for dynamic groups in the cloud the method combines the group signature and signed receipt and dynamic broadcast encryption method. Specially, the group signature and signed receipt scheme enables users to anonymously use the cloud location, and the dynamic broadcast encryption model access data owners to securely share their data files with others including new joining users.



4. CONCLUSION

In this paper, we design a secure anti-collusion data sharing scheme for dynamic groups in the cloud. In our scheme, the users can securely obtain their private keys from group manager Certificate Authorities and secure communication channels. Also, our scheme is able to support 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 updated. Moreover, our scheme can achieve secure user revocation, the revoked users can not be able to get the original data files once they are revoked even if they conspire 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, andM.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 DistributedSystems 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 SecuritySymp. (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. Practice and Theory in Public Key Cryptography Conf. Public Key Cryptography, 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 IdentityBasedEncryption 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, "FullyCollusionSecure Dynamic Broadcast Encryption with Constant-SizeCi-phertexts or Decryption Keys," Proc.First Int'l Conf. Pairing-BasedCryptography, 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 of2013 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-shunDai, and ElisaBertino, "A practical and flexible keymanagement mechanism for trusted collaborative computing,"INFOCOM 2008, pp. 1211-1219.

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