Secure Data Sharing In Multi-Owner for Dynamic Groups in Cloud

J. Pratheeka[1], Dr. M. Nagaratna[2]

JNTUH College of Engineering Hyderabad, JNTUH, Hyderabad, India

Abstract: ***The major aim of this technique is a secure multi-owner knowledge sharing theme. It indicates that any user within the cluster will firmly share knowledge with others by the world organization trust worthy cloud. This theme is ready to support dynamic teams. Efficiently, specifically, new granted users will directly rewrite knowledge files uploaded before their participation whereas not contacting with knowledge owners. User revocation square measure is just achieved through a very distinctive revocation list whereas not modification of the key. The keys of the remaining users then the size and computation overhead of cryptography square measure constant and freelance with the amount of revoked users. We've a bent to gift a secure and privacy-preserving access management to users that guarantee any member throughout a cluster to anonymously utilize the cloud resources. Moreover, the $64000 identities of information owners square measure disclosed by the cluster manager once disputes occur. We offer rigorous security analysis, and perform intensive simulations to demonstrate the potency of our theme in terms of storage and computation overhead. Cloud computing provides a cheap associated economical resolution for sharing cluster resource among cloud users sharing knowledge associate degree passing throughout a terribly multi-owner manner whereas protecting knowledge Associate in Nursing identity privacy from an world organization responsible cloud continues to be a issue, because of the frequent modification of the membership.***

Keywords: Multi owner, Cloud, resource, cluster manager, revocation, Key Distribution

1. Introduction

Cloud computing is recognized as another to ancient info technology as a results of its resource -sharing and low-maintenance characteristics. In cloud computing, the cloud service suppliers (CSPs), like Amazon, unit able to deliver numerous services to cloud users with the assistance of powerful knowledge centers. By migrating the native knowledge management systems into cloud servers, users will fancy high-quality services and save very important investments on their native infrastructures. One in each of the foremost basic services offered by cloud suppliers is knowledge storage. Allows us a to position confidence in a very sensible knowledge application. a corporation permits its staffs within identical cluster or department to store and share files within the cloud. By utilizing the cloud, the staffs area unit usually entirely discharged from the powerful native knowledge storage and maintenance. However, it additionally poses a big risk to the confidentiality of those hold on files. Specifically, the cloud servers managed by cloud suppliers don't seem to be all trustworthy by users whereas the information files hold on within the cloud could even be sensitive and confidential, like business plans. To preserve knowledge privacy, a basic resolution is to jot in code knowledge files and then transfer the encrypted knowledge into the cloud .Sadly, designing degree economical and secure knowledge sharing theme for groups within the cloud isn't a simple task as a results of the subsequent problems. However, the complications in user participation and revocation in these schemes area unit linearly increasing with the number of data householders and then the vary of revoked users, severally. By setting a bunch with one attribute level projected a secure origin theme supported the cipher text-policy attribute-based cryptography technique that permits any member throughout a cluster to share knowledge with others. However, the matter of user revocation isn't addressed in their theme given a climbable and fine-grained knowledge access management theme in cloud computing supported the key policy attribute-based cryptography (KP-ABE) technique. Sadly, the one owner manner [3]hinders the adoption of their theme into the case, wherever any user is permitted to store and share knowledge. Our contributions to resolve the challenges given more than, we've AN inclination to propose Mona, a secure multi-owner knowledge sharing theme for dynamic teams within the cloud

2. Related Work

2.1 Achieving Scalable, Secure and Fine-grained Data Retrieve Control in Cloud Computing

This details the challenging issue on one hand, describing and elaborating and imposing access policies based on data objects, and on the other hand, allow the data owner to point out and work on most of the computing tasks involved in fine grained data retrieval control to un trusted cloud servers without exposing the beneath data contents. We achieve this by exploiting and combining the techniques of attribute-based encryption (ABE) and proxy re-encryption, and lazy re-encryption [3]. The proposed technique also has unique features of user access rights confidentiality and user secret key accountability.

2.2 Plutus: Scalable secure file sharing on un trusted storage

The technique introduces novel cryptographic primitives applied to the secure data storage problems in the presence of un trusted servers and a aim for owner managed key distribution [4]. Excluding all requirements for server trust (servers are still required to protect the data) and allowing key distribution (and with access control) to the data owners who provides a secure storage system that protects and share data at very large and bulk scales across the trust boundaries.

2.3 Secure Provenance: The Necessity of Bread and Butter in Cloud Computing of Data Forensics

In this the proposed scheme is characterized by providing the information confidentiality on sensitive documents stored in cloud, anonymous authentication on user access ,and provenance tracking on disputed documents. With the provable security techniques, we formally demonstrate the proposed scheme is secure in the standard model.

Several security schemes for knowledge sharing on unsure servers are planned [4][5]. In these approaches, knowledge house owners store the encrypted knowledge files in unsure storage and distribute the corresponding decipherment keys solely to licensed users. Thus, unauthorized users in addition as storage servers does not know the content of the information files as a result of they need no information of the decipherment keys but, the complexities in user participating and revocation in these techniques square measure linearly increasing with variety of information house owners and therefore the number of revoked users, severally. By setting a gaggle with one attribute, Lu et al. planned a secure cradle theme supported the cipher text-policy attribute-based encoding technique that permits any member in a very cluster to share knowledge with others. However, the difficulty of user revocation isn't self-addressed in their theme. Given a scalable and fine-grained knowledge access management theme in cloud computing supported the key policy attribute-based encoding (KP-ABE) technique. Sadly, the one owner manner hinders the adoption of their theme into the case wherever any user is permitted to store and share knowledge.

3. Proposed Work

This paper, we have a tendency to propose a secure multi owner information sharing theme, named Mona, for dynamic teams within the cloud. By investment cluster signature and dynamic broadcast coding techniques, any cloud user will anonymously share information with others. Meanwhile, the storage overhead and coding computation price of our theme square measure freelance with the amount of revoked users. Additionally, we have a tendency to analyze the safety of our theme with rigorous proofs, and demonstrate the potency of our theme in experiments.

3.1 Proposed Algorithm

AES works on a principle known as Substitution and permutation network. Unlike DES its predecessor, AES does not follow Feistel network. AES is a block cipher with block size 128 bits and key length of 128,192 or 256 bits. Rijndael specified with block and key sizes in multiple of 32 bits, with minimum of 128 bits. The block size has a maximum of 256 bits, but the key size has no theoretical maximum.AES works with a 4×4 column major order matrix of bytes, called state. Most of AES calculations are done in a special finite filed. The AES cipher text is the number of repetitions and transformation rounds which converts the input plaintext into cipher text as final output. Each round is carried by several processing steps that depend on the encryption key. Reverse rounds are applied to transform block cipher text back to the original plaintext by making use of the same encryption key.

3.2 System Architecture

The system model details the group manager distribute the corresponding secret keys to the group members and hence the members get registered by the manager where in the group members perform the required operations on to the cloud and the user when required is revoked by the group manager. The Following Figure [1] shows that the architecture of our proposed work.

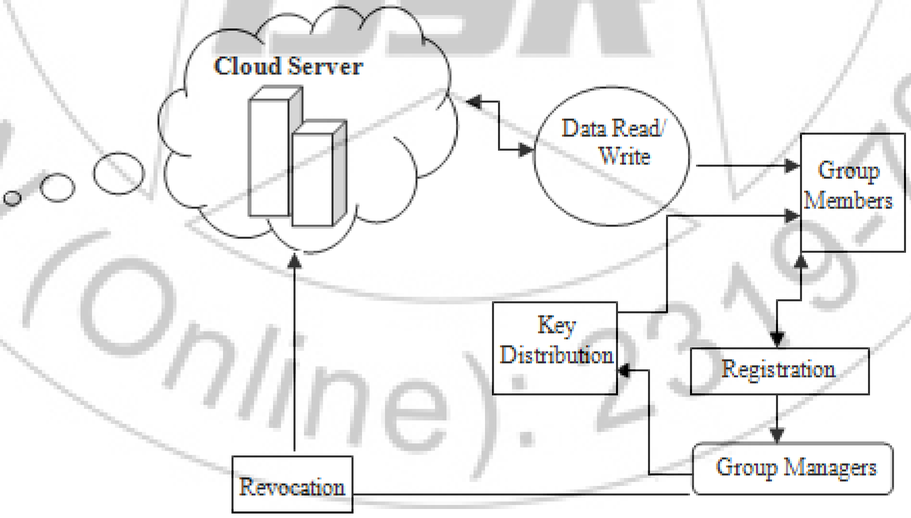

Figure 1: System Architecture for Proposed Work

4. System Implementation

Our proposed system implementation can be divided into four modules as follows
1. User Registration
2. User Revocation
3. File Uploading and Deletion
4. File Access and Traceability

4.1 User Registration:

For the registration of user with identity ID the group manager randomly selects a number. Then the group manager adds into the group user list which will be used in the traceability phase. After the registration, user obtains a private key which will be used for group signature generation and file decryption.

4.2 User Revocation

The group manager performs the user revocation via a public available. Revocation list based on which the group members can encrypt their data files and ensure the confidentiality against the revoked users. Group manger update the revocation list each day even no user has being revoked in the day. In other words, the others can be verified the freshness of the revocation list from the contained current date.

4.3 File Uploading and Deletion:

To store and share a data file in the cloud, a group member performs to getting the revocation list from the cloud. In this step, the member sends the group identity ID group as a request to the cloud. Verifying the validity of the received revocation list and can delete the stored files in the cloud by either the group manager or the data owner. For file uploading and deleting we apply AES algorithm to provide security for the data.

4.4 File Access and Traceability:

To access the cloud, a user needs to compute a group signature for his/her authentication. The employee group signature scheme can be regarded as a variant of the short group signature which inherits the inherent enforceability property, anonymous authentication, and tracking capability. When a data dispute occurs, the tracing operation is performed by the group manager to identify the real identity of the data owner.

5. Experimental Results

The Computation cost under various operations including the request for file generation, file access, file deletion. The sizes of requested file are 200 and 20MB the test results are given below. The computation cost is acceptable even when the revoke users are large. It's important to note that computation cost is independent with the size of the request to file access or delete operations.

Table 1: Computational Cost

Request	The Number Of Revoked Users		
	0	100	200
File Generation (200MB) File	0.110	0.221	0.404
File Generation (20MB)File	0.480	0.204	0.385
File Access (200MB) File	0.075	0.205	0.355
File Access (20MB) File	0.075	0.207	0.361
File Delete (200MB) File	0.065	0.205	0.357
File Deletion (20MB) File	0.069	0.210	0.356

6. Conclusion

In this paper, we've an inclination to vogue a secure data sharing theme, for dynamic groups in associate world organization trustworthy cloud. In this a user during a position can share data with others at intervals in the cluster whereas not revealing identity privacy to the cloud. Additionally, Lots of specially, economical user revocation are achieved through a public revocation list whereas not modification of the remaining users private keys, and new users can directly decipher files keep at intervals the cloud before their participation. Moreover, the storage overhead and additionally the coding computation value are constant.

The future work of Intensive analysis makes this scheme satisfy the desired security requirements and hence guarantees efficiency.

References

[1] M. Armbrust, A. Fox, R. Griffith, A.D. Joseph, R.H. Katz, A.Konwinski, G. Lee, D.A. 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] S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving Secure, Scalable, and Fine-Grained Data Access Control in Cloud Computing," Proc. IEEE INFOCOM, pp. 534-542, 2010.

[4] 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.

[5] 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.

[6] 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.

[7] 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.

[8] B. Waters, "Ciphertext-Policy Attribute-Based Encryption: An Expressive, Efficient, and Provably Secure Realization," Proc. Int'lConf. Practice and Theory in Public Key Cryptography Conf. Public Key Cryptography, http://eprint.iacr.org/2008/290.pdf, 2008.

[9] 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.

[10]D. Naor, M. Naor, and J.B. Lotspiech, "Revocation and Tracing Schemes for Stateless Receivers," Proc. Ann. Int'l Cryptology Conf. Advances in Cryptology (CRYPTO), pp. 41-62, 2001.