ISSN- 2394-5125 VOL 9, ISSUE 05, 2022

RESOLVING CONFLICTS AND PROVIDING SECURITY FOR THE DATA IN MULTI-OWNER CLOUD COMPUTING ENVIRONMENT

E Sai Kumar #1, Akuthota Sai Mukesh#2, Surabhi Lakshmi Manogna #3, Karicheti Madhusri #4, Kesineni Abhiram #5

#1 Asst. Professor, #2,3,4,5 B.Tech., Scholars
Department of Computer Science and Engineering,
QIS College of Engineering and Technology

Abstract:
Distributed computing can facilitate the massive data transfer required by the rapidly expanding cloud administrations. Existing infrastructure can't handle protecting ciphertext with many owners. Because of this, the creator loses some measure of control over whether or not useful knowledge is disseminated by information propagators. Classification of data has been made possible using cryptographic techniques thanks to distributed computing. In this research, we present a cloud-based method of encrypted group communication and conditional distribution with multiple data owners, where data is only distributed when specific criteria are met. If the owner's properties match the entry methods in the encrypted message, the information may be securely transferred into a group of consumers over the cloud. The content propagator will move the user-generated content to a new location. The researchers also provide a user-friendly design for distributed block cypher that allows for total user autonomy. With this setup, data co-owners may adjust the ciphertext to reflect their desired degree of security by using updated access methods. The multiple access arrangements also introduce a security conflicting concern, although this may be managed using one of three approach aggregation choices. Total grant, proprietor requirement, and major share licence are the applicable options. Our approach seems to be efficient and capable of securely transferring data to a number of different owners in distributed computing, as shown by the results of the security analysis and exploratory testing.

1. Introduction:

Large amounts of storage space and almost immediate access are two of the main reasons for cloud computing's stratospheric surge in popularity [1]. Individuals and businesses alike may take use of these services to store data (such as media files) with a cloud service provider (CSP) and then retrieve it at any time, from any location, and even share it with others. Most cloud services maintain an access control list as their method of implementing access control. This is done to protect the confidentiality of the users (ACL). Users have the option of making their information publicly available or restricting access to just those they have authorised in advance. Concerns have been voiced, however, because of security flaws stemming from the CSP's storage of the data in an unencrypted form. The owner of data loses all authority over its further processing after it has been posted to a CSP [2]. Unfortunately, the CSP is typically a partially

ISSN- 2394-5125 VOL 9, ISSUE 05, 2022

trusted server that follows the protocol as described but also has the ability to secretly collect and perhaps misuse user data.

The data, however, has substantial uses for a wide range of data consumers to gain understanding of user behaviour [3]. As a result of these vulnerabilities, effective methods of protecting data privacy have been developed and implemented. Access control mechanisms must be implemented in cloud computing environments for secure data transfer to take place [4]. Cryptographic methods are now being employed to solve these security and privacy concerns; such examples are attribute-based encryption (ABE) [5, identity-based broadcast encryption (IBBE) [6, and remote attestation [7]. [5] [6] [7] [8] [9] [10] [11] [12] [13] [14] [15] [16] [18] [19] [18] As a new generation of cryptographic algorithms, ABE is being used in cloud computing to provide private, granular data transfers [8]. It features a method for regulating who may see encrypted data and under what conditions, all thanks to the use of access rules and the assignment of properties to encryption keys and encrypted messages. Data encryption may still be subject to this kind of management.

If the attribute set can be proved to be compliant with the access rules, then the encryption text can be deciphered. The IBBE approach is another popular technique utilised in cloud computing [9, 10]. The public key of the recipient may be considered to be any acceptable string, such as their unique identity or email address, allowing users to transmit encrypted data with several recipients at once. Actually, IBBE may be seen as a concrete illustration of ABE for policies that have an OR gate. Because of its small fixed policy size and cheap key maintenance, IBBE is better suited for securely broadcasting data to predetermined receivers in the cloud. In ABE, both the secret key and the cypher text must correspond to a shared set of properties.

Therefore, the content creator may safely and efficiently provide access to a set of users by virtue of their identities. Because of this, more consumers are likely to trust cloud storage with their sensitive information. While these encryption techniques may be effective at preventing unauthorised parties (such as semi-trusted CSPs and malicious users) from accessing the data, it is probable that they do not account for the widespread nature of data sharing in cloud computing. Data disseminators (such as editors and collaborators) may share documents with new users, including those who aren't linked with the firm, while using cloud-based collaboration tools like Box [11] and One Drive [12]. Not even the data distributors themselves can alter the cypher text that the data owners submit [13]. This is because it is impossible to decrypt data that has been encrypted using the methods outlined above. The CSP is given a re-encryption key that is specific to the new recipients as part of the proxy re-encryption (PRE) approach [14] used to guarantee the security of data transmission in cloud computing. This helps the CSP realise its objective of safe information sharing. The data disseminator, on the other hand, may give out the re-encryption key and let anybody access the data belonging to the data owner. Given that the

ISSN- 2394-5125 VOL 9, ISSUE 05, 2022

data owner may only provide authorization for the data disseminator to disseminate a certain document, this may or may not fulfil the practical need.

A more refined concept called conditional PRE (CPRE) [15, 16] may be able to help with this issue by allowing the data owner to restrict the re-encryption of the original cypher texts to just those that meet a certain criterion. However, the more complex situations that happen in the cloud render traditional CPRE schemes inadequate. These schemes only allow for simple keyword conditions. To implement an access policy inside the encrypted text, an attribute-based CPRE has been described [17]. In place of keywords, expressive conditions are being provided in this way. A proxy may only re-encrypt the cypher text if the re-encryption key is consistent with the access policy, since the re-encryption key is tied to a certain set of features. By doing so, the data's owner may fine-tune the terms under which the data is made public.

For instance, the data owner may provide permission for the company's project managers to share the status report through One Drive. Nonetheless, for a certain time frame, the project budget may only be shared on One Drive by senior directors in the finance department. The need of conditional data dissemination [18, 19] presents a multiparty access control dilemma for data sharing in cloud computing applications like cloud collaboration and cloud-based social networks. This allows for the coordinated satisfaction of the varied authorization needs of a network of interconnected users in order to exercise authority over their collective data. Take the case of three users, Alice, Bob, and Carol, who are utilising cloud computing to produce a coauthored paper or cophoto. Alice will be regarded to have shared ownership of the item if she uploads the co-authored document or co-photo to the CSP and lists Bob and Carol as co-owners. Alice may restrict access to this information by a select group of users, but Bob and Carol, as company co-owners, may have other privacy concerns. A major and serious privacy risk is raised if just one party is selected, since this raises the possibility that the data may be shared with unintended recipients. However, as privacy conflicts are inevitable when authorising many parties concurrently [20, 21], merging the privacy preferences of a data owner with those of numerous co-owners is not a straightforward job.

When two or more parties to an asset have rules that are at odds with one another, privacy conflicts emerge and the asset in issue becomes unavailable to outside parties [22]. Additional multiparty access control approaches, such as a vote procedure, have been made available to address this dilemma. But they are all based on data that was originally stored in plaintext. We provide a multi-owner cloud computing identity-based secure data group sharing and conditional dissemination technique. In order to address the issues mentioned above, we propose a method for enabling multi-user cypher text group sharing and recording the crucial characteristic of multi-party authorisation needs.

ISSN- 2394-5125 VOL 9, ISSUE 05, 2022

2. Related Work

In distributed computing, a variety of previously undiscovered safety with associated protection problems become key investigation subjects. In order to lessen the severity of these dangers, maintaining the confidentiality of sensitive information should make use of strong encryption technologies. In distributed computing, Huang et al., Patra Nabis et al., and Liu et al. [9] suggested a few different schemes for distributing a small amount of personal information. These researchers made use of the IBBE technique. The owner of the information reacquires ciphering from the CSP by providing a list of assignees. As a consequence of this design, only the recipients of the list are able to obtain the decryption key and decode the confidential information. ABE is yet another intriguing one-to-many cryptographic approach that can combine information encryption with granular access control in distributed computing. Since it conveys the ciphertext entry strategy in an efficient manner, the ciphertext-strategy ABE (CPABE) is an effective entry power approach that should be considered for practical applications.

The precautionary safety measure, as presented by Guo et al.

Keeping the information distribution system running well in a variety of unofficial settings in consideration of CP-ABE Teng et al. developed a practical access control scheme that makes use of progressive CP-ABE with the intention of achieving security protection in networked storage systems. As a consequence of the usage of ABE in the plans to give access control of clinical reports during the delivery of health administrations via the cloud, the wellness record has to be decoded by authorised archive requesters who have equal credits. The demand for information capacity security in distributed computing places a significant emphasis on the importance of secure information delivery. The personality-based method might be used by information disseminators in order to transfer their encryption keys to the partly protected intermediate in order to alter the ciphertext used by the information owner for new customers. This encryption computation is very necessary in order to accomplish safe information dissemination in distant computing environments. Combining the ABE technique with property-based PRE [17] has also been used in distributed computing. Clients that use a newly developed access method will be able to get the raw text by having an intermediary replace the ciphertext with plaintext using the re-encryption key belonging to the information disseminator. The previously stated PRE plots, on the other hand, only allow for an all-or-nothing approach to the conveyance of the information. This issue is also addressed by the CPRE conspire algorithm, which, if the prerequisites are satisfied, makes it possible for the intermediate to encrypt the ciphertext without error. However, the constraints are only watchwords in prior plans for the CPRE, which limits flexibility when dealing with complicated appointments in distributed computing. To show a quality based CPRE methodology, Yang et al. sent an entry method as open-key encrypted ciphertext. This was done to protect the method's confidentiality. The encoded key is generated by combining the mystery key with a series of parameters in order to produce it. This allows the intermediate to encode the ciphertext, but only under the condition that specific entry strategy criteria are satisfied by the parameters. A pre-authentication technique was developed by Wang

ISSN- 2394-5125 VOL 9, ISSUE 05, 2022

et al. with the purpose of facilitating the transfer of cloud-based information. This mechanism checks the veracity of the beneficiary before to encryption. In distributed computing, co-owners and multiparty security control are both necessary components. As Thomas et al. [20] shown, the security model used by Facebook may be leveraged to provide protection for several parties simultaneously. Customers will be allowed to access the information if the owner and the openness policies of all linked groups are adhered to, which is made possible by this capability, which allows widely connected groups to establish openness rules for the information. Based on this multiparty security control paradigm, Xu et al. [19] built a system that allows each client inside an image to take part in deciding the access control states for the picture. This system was published as a research article.

However, the previous designs may have had protection concerns that were in contradiction with one another and may not have truly represented how customers would really arrive at a decision. Such et al. developed the major computational approach that has been used to find protection conflicts across multiparty systems (Arranging clients). Conduct an analysis of each item's responsiveness, relative importance, and level of preparation with regard to each competitive arranging consumer. Then, have the person who has less stringent criteria for security divide the difference. A systematic approach to dealing with the broadcast of information to several owners in order to enable cost savings in security was offered. This notion proposes three different approaches that may be used in democratic democracies in order to detect multiparty protection issues. Unfortunately, this solution is just concerned with establishing access control over unencrypted data, and it pays no attention to the privacy of information for CSPs or customers who intentionally do harm.

3. System Analysis

It is very necessary for there to be multiparty privacy control among co-owners when using cloud computing. Thomas et al. [20] shown how the privacy model used by Facebook may be modified to accommodate multiparty privacy requirements. It provides the ability for any and all related parties to define exposure rules for the data, making it possible for users to access the data provided that they fulfil the exposure policies of the owner as well as any and all associated parties. On the basis of this multiparty privacy control model, Xu et al. [19] designed a mechanism to enable each user in a photo to participate in the decision-making process regarding the access control conditions of the photo. [Citation needed] [Citation needed] [Citation needed] [Citation needed] [Citation needed] However, the aforementioned approaches could have an issue with privacy conflicts since they don't take into account how users would really reach a compromise [19]. The first computational mechanism was proposed by Such et al. [24] in an effort to resolve the privacy conflicts that arose among multiparty users who were negotiating. The fundamental concept is to determine the level of sensitivity, relative relevance, and willingness of each user involved in a contentious negotiation, and then to allow the user to compromise whose privacy requirements are the least rigorous. Hu et al. [23,25] offered a methodical strategy to permit data exchange with many owners while yet protecting individuals'

ISSN- 2394-5125 VOL 9, ISSUE 05, 2022

right to privacy. For the purpose of resolving the multiparty privacy conflicts, this plan proposes three different solutions that are based on a voting system. Regrettably, this technique is primarily concerned with the access control that co-owners have over unencrypted data. It pays no attention to the confidentiality of the data with respect to semi-trusted CSPs or malevolent users.

Disadvantages

In the work that has been done up to now, integrating the privacy preferences of a data owner with those of several co-owners is not a simple undertaking. This is because a privacy conflict is unavoidable in the implementation of multiparty permission. Due to the absence of conditional proxy re-encryption, the security of the system is highly compromised.

4. Proposed System

The suggested system presents a technique to enable cypher text group sharing across several users and capture the essential characteristic of multiparty permission needs. The following is a list of the contributions that our plan makes:

Through the use of attribute-based CPRE, the system is able to do fine-grained conditional dissemination over the encrypted text in cloud computing. First, the encrypted text is deployed with an initial access policy that has been personally crafted by the data owner. The multiparty access control technique that we have presented gives the data co-owners the ability to add new access rules to the cypher text so that they may meet their individual requirements for privacy. Therefore, in order for the data disseminator to be able to re-encrypt the cypher text, the characteristics must first comply with a sufficient number of access regulations. The system gives three solutions to the issue of privacy conflicts: full permit, owner priority, and majority permission. Full permit is the most comprehensive solution. In particular, when using the complete permission technique, the data disseminator is required to comply with all of the access regulations that have been set by the data owner and any co-owners. The data owner can first choose a threshold value for data co-owners when using the majority permit strategy. The cypher text can be disseminated if and only if the sum of the access policies satisfied by the data disseminator's attributes is greater than or equal to this fixed threshold. If the sum is less than this threshold, the cypher text cannot be disseminated.

The system demonstrates that our plan is sound, and it also allows us to carry out tests to assess how well our plan works at each stage. This demonstrates that our plan is successful.

Advantages

Since data co-owners may renew the cypher texts by appending their access rules as the dissemination conditions, the data's security has been increased significantly.

ISSN- 2394-5125 VOL 9, ISSUE 05, 2022

Continuous policy enforcement provides an additional layer of protection for the system by enforcing the data owner's access policy not only in the original cypher text but also in the renewed cypher text. This makes the system more resistant to intrusion.

5. Implementation

Data Requester/Receivers (DR)

DR will submit the decryption request to Cloud, where it will be obtained, and will get the ciphertexts from the internet. Plaintext access can only be granted if the individual's characteristics have been validated as complying with the ciphertext's access regulations. Requesters and recipients of data may confederate in order to obtain data that is in any other case inaccessible to them separately.

Servers in the cloud (CS)

The CS team is accountable for the storage of a vast amount of data. DO is unable to put their faith in them. As a result, it is essential that DO establish an access policy in order to safeguard the confidentiality of the data. It is presumed that CS did not conspire with DR.

Credible Source of Information (TA)

AA is in charge of enrolling individuals, assessing their characteristics, and producing their secret key SK in a manner that is appropriate for each individual user. It then issues each DO with a public key PK and a master key MK after running the Setup procedure. It is believed to be completely reliable.

6. Conclusion

Users of cloud computing are understandably concerned about the privacy and safety of their data. Specifically, finding a way to address the privacy concerns of numerous owners while still maintaining the secrecy of the data becomes a difficulty. In this article, we describe a secure data group sharing and conditional dissemination strategy for use in cloud computing that accommodates many owners. According to our plan, the owner of the data could encrypt it and then share it in a time- and labor-saving manner with several data accessors all at once using the IBBE method. This was all possible thanks to our system.

In the meanwhile, the owner of the data may establish a fine-grained access policy to the ciphertext using attribute-based CPRE. This means that the ciphertext can only be re-encrypted by a data disseminator whose attributes fulfil the access policy included in the ciphertext. In addition to this, we provide a multiparty access control technique over the ciphertext. This mechanism gives the data co-owners the ability to attach their own access rules to the ciphertext.

ISSN- 2394-5125 VOL 9, ISSUE 05, 2022

References

[1] Z. Yan, X. Li, M. Wang, and A. V. Vasilakos, "Flexible data access control based on trust and reputation in cloud computing," *IEEE Transactions on Cloud Computing*, vol. 5, no. 3, pp. 485-498, 2017.

[2] B. Lang, J. Wang, and Y. Liu, "Achieving flexible and self-contained data protection in cloud computing," *IEEE Access*, vol. 5, pp. 1510- 1523, 2017.

[3] Q. Zhang, L. T. Yang, and Z. Chen, "Privacy preserving deep computation model on cloud for big data feature learning," *IEEE Transactions on Computers*, vol. 65, no. 5, pp. 1351-1362, 2016.

[4] H. Cui, X. Yi, and S. Nepal, "Achieving scalable access control over encrypted data for edge computing networks," *IEEE Access*, vol. 6, pp. 30049–30059, 2018.

[5] K. Xue, W. Chen, W. Li, J. Hong, and P. Hong, "Combining data owner-side and cloud-side access control for encrypted cloud storage," *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 8, pp. 2062–2074, 2018.

[6] C. Delerablée, "Identity-based broadcast encryption with constant size ciphertexts and private keys," *Proc. International Conf. on the Theory and Application of Cryptology and Information Security (ASIACRYPT '2007)*, pp. 200-215, 2007.

[7] N. Paladi, C. Gehrmann, and A. Michalas, "Providing user security guarantees in public infrastructure clouds," *IEEE Transactions on Cloud Computing*, vol. 5, no. 3, pp. 405-419, 2017.

[8] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute based encryption," *Proc. IEEE Symposium on Security and Privacy (SP '07)*, pp. 321-334, 2007.

[9] L. Liu, Y. Zhang, and X. Li, "KeyD: secure key-deduplication with identity-based broadcast encryption," *IEEE Transactions on Cloud Computing*, 2018, https://ieeexplore.ieee.org/document/8458136.

[10] Q. Huang, Y. Yang, and J. Fu, "Secure data group sharing and dissemination with attribute and time conditions in Public Clouds," *IEEE Transactions on Services Computing*, 2018, https://ieeexplore.ieee. org/document/8395392.

[11] Box, "Understanding collaborator permission levels", https://community. box.com/t5/Collaborate-By-Inviting-Others/Understanding- Collaborator-Permission-Levels/ta-p/144.

[12] Microsoft OneDrive, "Document collaboration and co-authoring", https://support.office.com/en-us/article/document-collaborationand- co-authoring-ee1509b4-1f6e-401e-b04a-782d26f564a4.

[13] H. He, R. Li, X. Dong, and Z. Zhang, "Secure, efficient and finegrained data access control mechanism for P2P storage cloud," *IEEE Transactions on Cloud Computing*, vol. 2, no. 4, pp. 471-484, 2014.

[14] Z. Qin, H. Xiong, S. Wu, and J. Batamuliza, "A survey of proxy reencryption for secure data sharing in cloud computing," *IEEE Transactions on Services Computing*, 2018, https://ieeexplore.ieee.org/document/7448446.

ISSN- 2394-5125 VOL 9, ISSUE 05, 2022

[15] J. Son, D. Kim, R. Hussain, and H. Oh, "Conditional proxy reencryption for secure big data group sharing in cloud environment," *Proc.* of *2014 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, pp. 541–546, 2014.
[16] L. Jiang, and D. Guo "Dynamic encrypted data sharing scheme based on conditional proxy broadcast re-encryption for cloud storage," *IEEE Access*, vol. 5, pp. 13336 – 13345, 2017.
[17] K. Liang, M. H. Au, J. K. Liu, W. Susilo, D. S. Wong, G. Yang, Y. Yu, and A. Yang, "A secure and efficient ciphertext-policy attribute-based proxy re-encryption for cloud data sharing," *Future Generation Computer Systems*, vol. 52, pp. 95-108, 2015.
[18] X. Li, Y. Zhang, B. Wang, and J. Yan, "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, 2013.
[19] K. Xu, Y. Guo, L. Guo, Y. Fang, and X. Li, "My privacy my decision: control of photo sharing on online social networks," *IEEE Trans. On Dependable and Secure Computing*, vol. 14, no. 2, pp. 199-210, 2017.
[20] K. Thomas, C. Grier, and D. M. Nicol, "UnFriendly: multi-party privacy risks in social networks," *Proc. International Symposium on Privacy Enhancing Technologies Symp. (PETS '2010)*, pp. 236-252, 2010.
[21] L. Fang, L. Yin, Y. Guo, Z. Wang, and Fenzhua Li, "Resolving access conflicts: an auction-based incentive approach," *Proc. IEEE Military Communications Conference (MILCOM)*, pp. 1-6, 2018.
[22] L. Xu, C. Jiang, N. He, Z. Han, and A. Benslimane, "Trust-based collaborative privacy management in online social networks," *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 1, pp. 48- 60, 2019.
[23] C. Gentry and B. Waters, "Adaptive security in broadcast encryption systems (with short ciphertexts)," *Proc. 28th Ann. International Conf. on Advances in Cryptology: the Theory and Applications of Cryptographic (EUROCRYPT '09),* pp. 171-188, 2009.
[24] Q. Huang, W. Yue, Y. He, and Y. Yang, "Secure identity-based data sharing and profile matching for mobile healthcare social networks in cloud computing," *IEEE Access*, vol. 6, pp. 36584–36594, 2018.
[25] S. Patranabis, Y. Shrivastava, and D. Mukhopadhyay, "Provably secure key-aggregate cryptosystems with broadcast aggregate keys for online data sharing on the cloud," *IEEE Transactions on Computers*, vol. 66, no. 5, pp. 891–904, 2017.