International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 07 Issue: 08 | Aug 2020 www.irjet.net p-ISSN: 2395-0072

Secure Data Group Sharing and Conditional Dissemination with Multi-Owner in Cloud Computing

Sahana C[1], Vyom Mishra[2], Arshad Makharani[3], Ritwick[4], Dr. M S Patel[5]

[1-4]*UG student*
[5]*Dr. M S Patel, Professor, Dept. of ISE, Sapthagiri college of Engineering, Karnataka, India*

Abstract - *Because of the exponential development in the cloud infrastructure, vast amounts of data are exchanged via cloud computing platforms. Cryptographic techniques are used to protect data privacy in cloud computing, but these techniques cannot handle privacy distress over multi-owner-related ciphertext, which prohibits co-owners from managing the dimension, whether data disseminators may actually disseminate their data. In this paper, we propose a secure data group sharing and conditional dissemination scheme in cloud computing with multi-owner, where the data owner can securely allocate the secured data to users who are part of the group via the cloud, and the data can be disseminated to a group of new users by the data disseminator if the ciphertext access policies are satisfied. We also provide a multi-party access control framework over the ciphertext which enables the ciphertext's co-owners to add new authorization policies to their protection preferences. In order to solve the disagreements in a state where data are not observed or disturbed, there are three policies of aggregation, which are fully enabled, owner priority and majority entitled. The protection analysis and test results demonstrate our approach to stable data sharing with multi-owners in cloud storage is practical and methodical. Through the rapid development of cloud administration, huge quantities of data are exchanged through cloud computing. While cryptographic methods have been used in cloud computing to provide data confidentiality, current instruments cannot allow multi-owner-related over ciphertext security issues, which makes it unfit for co-owners to properly monitor how data disseminators can actually disperse their data. In this paper, we suggest a stable data group sharing and restrictive dispersal conspire with multi-owner cloud computing in which data owner can securely distribute private data to a group of customers through the cloud, and data disseminator can distribute the data to another group of customers if the quality match the entry approaches in the ciphertext. We also present a multiparty method to monitor the scattered ciphertext in which the data co-owners are able to annex new access approaches to the ciphertext due to their security inclinations. However, three methodologies of agreement set, including full grant, owner need and lion 's share license, are provided to tackle the issue of security conflicts brought on by various access strategies. The technology analysis and test results show that our strategy is useful and successful for safe data offering in cloud computing to multi-owner.*

Key Words: Data sharing, cloud computing, conditional proxy re-encryption, attribute-based encryption, privacy conflict

1. INTRODUCTION

Cloud computing reverence is gained from the benefits of rich storage supplies and instantaneous feedback. Computer network assets are distributed, and on-demand support is delivered over the Internet. A number of businesses, such as Google, Alibaba and Amazon, have made public cloud services available. Individual users and business users upload data to the cloud service provider (CSP) with the aid of these service providers, which serves data accessibility purposes from anywhere at any time and data can also be exchanged with others. In order to strengthen users' privacy concerns, most cloud services maintain access control list (ACL) to achieve control of access. And so on, users can either choose to give access rights to certain approved persons, or can choose to open their data to anyone. The CSP stores the data in plaintext form, which raises concerns about security threats between users. When the data is released to the CSP, the owner of the data loses power. CSP implements an assigned protocol that makes it a semi-trusted server, where it may use the user's data for profit without the user's permission, this data is of significant interest to other users who would use the data to know the user's behavioural habits. The powerful findings are motivated by these protection and privacy issues surrounding data confidentiality. To achieve safe data sharing in cloud computing, it is important to implement access control mechanisms. Techniques such as attribute-based encryption (ABE), remote attestation and identity-based broadcast encryption (IBBE) are currently being used to resolve the security concerns. ABE is one of the tools used in cloud computing to share the data and to protect the data. ABE attributes a system for access control of the encrypted data using the access policies. Another tool used for cloud computing is IBBE where, for considering their specific I d or email, the data can be exchanged between multiple receivers at a time. IBBE is easier to assign data to individual users because it provides low-cost key management and comparatively smaller policy sizes. The owner of the data can securely share data using these mechanisms, thereby encouraging more users to share their data via cloud. These encryption mechanisms do not assist in cloud computing with data distribution but they may prevent unauthorized

organizations from accessing the data. And after the data is encrypted and disseminated, it is not possible to make any changes to the ciphertext that the data owner uploads. The proxy re-encoding scheme (PRE) is used to achieve safe data transmission in cloud computing by entrusting the CSP with a re-encoding key associated with the new receivers. Re-encryption key cannot meet some of the criteria, as the day owner can allow data disseminator to disseminate similar data only. Therefore, this problem is discussed in the definition called conditional PRE (CPRE). Where one can re-encrypt unique ciphertext. The conventional CPRE embraces only basic keywords, which is why they cannot address the dynamic scenarios that have arisen in cloud computing. Attribute-based CPRE is designed to support descriptive conditions, rather than keywords, which would enforce a ciphertext access policy. In this way the data owner will configure the fine-grained distribution condition for the shared data. Cloud computing 's popularity is born from the advantages of rich stockpiling assets and the time to come. This summarizes the computing platform properties and ultimately offers on-demand advantages over the Internet. Numerous esteemed companies, for example Amazon, Google, Alibaba, are currently offering transparent cloud administrations. Such administrations allow individual customers and undertaking customers to move data (e.g. images, records and reports) to cloud specialist organization (CSP), to access data anywhere, and to give data to others. Most cloud administrations maintain control by holding up to the control list (ACL) in order to ensure client security.

To alleviate the above-mentioned issues, we familiarize ourselves with a solution to accomplish ciphertext group sharing among multiple customers and catch the centre dimension of multiparty approval needs. Our Plan's obligations are as follows:

1. In cloud computing with trait-based CPRE, we achieve fine-grained, restrictive dispersal over the ciphertext. The ciphertext is transmitted right off the bat with an underlying access agreement changed by the data owner. Due to their security inclinations, our proposed multiparty get to control feature allows the data co-owners to add new access approaches to ciphertext. Henceforth, the data disseminator will re-scramble the ciphertext only if the traits satisfy adequate access approaches.
2. We offer three procedures including full license, owner requirement and larger grant to take care of the issue of security clashes. Exceptionally, the data disseminator must follow all the entry approaches defined by data owner and co-owners in full license methodology. Data owner can initially choose an opportunity for data co-owners with the dominant component grant process, and the ciphertext can be distributed if and only if the entire entry method accomplished by the characteristics of the data disseminator is more noteworthy than or equal to this fixed edge.
3. We demonstrate the accuracy of our strategy, and direct tests to assess the exhibition at each point to prove our strategy's adequacy.

2. PROBLEM STATEMENT

IBBE implements inexpensive key control and tiny constant regulation sizes that are more suited for the safe transfer of data to different cloud recipients. When you choose the choice of only one person to exchange this data with unauthorized users, that is a big and severe privacy issue. In addition to the need for conditions of data dissemination, multiparty access control for cloud computing data sharing, such as cloud cooperation and cloud-based social networks, allows the shared information to be managed jointly with the specific permission requirements of multiple associated users.

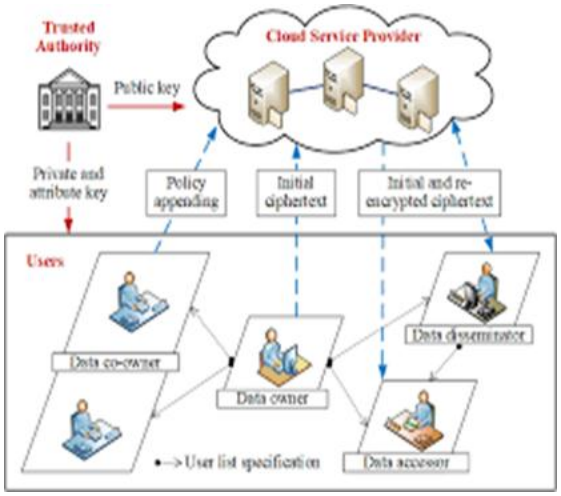

Fig -1: System model of proposed scheme. The user role is divided into the following categories: data owner, data co-owner, data disseminator and data accessor

The user function is divided into: data owner, data co-owner, data disseminator and data accessor.

Symbols	Description
MK, PK	The master secret key and system public key
SK	The private key of user
AK	The attribute key of user
M	The data
U	The set of data accessors' identities
W	The set of data co-owners' identities
DK	The symmetric key
CT_0	The initial ciphertext
T_0	The access tree of CT_0
CT_i	The renew ciphertext generated by policy appending
T'_{i+1}	The access tree customized by data co-owner for CT_i
TK_i	The transformation key of data co-owner for CT_i
T_i	The access tree of CT_i
U'	The set of new accessors' identities
RK	The re-encryption key of data disseminator
CT'_i	The re-encrypted ciphertext

Table-1: Notations

3. PROPOSED SYSTEM

We gather our dataset from the Peking University First Hospital's Health Management Center (PUFH). To process the data and set up a prediction program, we use data cleaning approach, dimensionality reduction methods and several machine learning algorithms. Next, we apply word vector model to medical history and diagnostic results, transforming them into 0-1 characteristics. Second, we develop a reduction method of dimensionality to resolve the question of high dimensionality and raising the complexity of the computation. Instead we use machine learning approaches to discover the relationship between reports of physical exams and possible health risks. We set up our network of predictions using these techniques. The system provides a user-friendly interface for examiners to check their health risks after physical examination, as well as for doctors to get intervention-set examinations. In fact, the device provides a feedback mechanism for doctors to correct the inaccuracy of the forecast. These latest labeled data will trigger the day-to-day training step which will automatically improve system performance.
In our scheme, co-owners of data will recharge the ciphertexts by annexing their entry approaches as the conditions of spread. As shown in, we have the following procedures to satisfy multi-owner approval prerequisites, as shown in Fig.

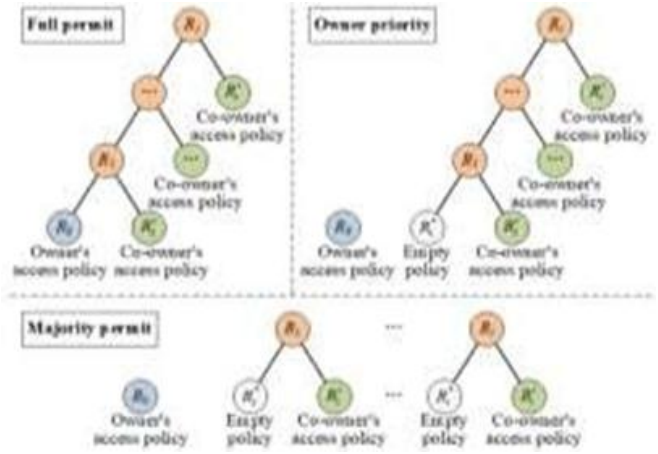

Fig-2: Three policy aggregation strategies with multi-owner

1. Full license: All owners (counting data owners and data co-owners) have a common right to pick the data dispersion states. The disseminator of the data will fulfill all the entry agreements defined by certain owners.
2. The owner needs: the option of the data owner has a great need, but it marks the co-owners. The data disseminator can disperse the data only when it fulfills the data owner's entry arrangement or all the data co-owner's entry strategies.
3. Majority grant: The data owner directly from the bat chooses an edge esteem, and the data can be disseminated if and only if the entire access strategies performed by the properties of the disseminator are more noteworthy than or equal to that fixed limit.

4. CONCLUSIONS

Data protection and confidentiality are of interest to cloud customers. In turn, it is a struggle to enforce numerous owners' privacy requirements and maintain confidentiality. This paper describes stable data community storage and dependable cloud infrastructure distribution scheme for multi-owners.

The data owner may, under our program, encrypt his or her private details and exchange them in a compatible manner with a community of IBBE based data accessors at once.

In the meantime, data owner will define a ciphertext-dependent fine-grained access policy based on the CPRE attribute and then the data provider may re-encrypt the ciphertext with the characteristics of the cyphertext access policy.

We often offer a multi-party access management system through the cipher text, which helps the data co-owners to implement their ciphertext access policies.

In fact, we have three regulation integration approaches that provide complete authorization, owner's preferences and majority authority to address privacy concerns.

The confidentiality and privacy of data is a problem for cloud computing clients. Specifically, how to allow multiple owners' security issues and ensure the classification of data becomes a test. Within this paper we present a safe exchange of data groups and a restrictive dispersal conspire within cloud computing with multi-owner. In our scheme, the data owner might scramble her or his private data and deliver it at once in a helpful way based on IBBE strategy, with a community of data accessors. Whereas, the data owner may determine fine-grained approach to the CPRE-based ciphertext, so the ciphertext has to be re-encoded by the data disseminator whose characteristics fulfill the ciphertext entry strategy. We also present a multiparty get to control the ciphertext variable, which allows the co-owners of the data to add their entry approaches to the ciphertext. However, we offer three strategy selection procedures like full license, owner's need and larger grant to deal with the issue of security clashes. Later we will strengthen our strategy by helping the hunt for catchphrases over the ciphertext.

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.

[3] 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.

[4] 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.