A Survey on Data Sharing Mechanism of Cloud Storage in Big Data

Sandhiya[1], Manohari[2]

[1]Research Scholar, Department of Computer Science Engineering, Theivanai Ammal College for Women, Villupuram, India

[2]Assistant Professor, Department of Computer Science Engineering, Theivanai Ammal College for Women, Villupuram, India

***Abstract*: Many users store the large amount of data in cloud. The Cloud Provider (CP) is semi trusted so that the Data Owner (DO) encrypt the file before uploading the file to the cloud. The Group Member(GM) seeking request from data owner to join in group. The Data Owner give permission to the group member then only they access the group. The Data Owner permit the group member to access the group in cloud and also distribute the key of the file which the legitimate users need. With the help of the key the user can view the file and download it.**

***Keywords*: Cloud provider, Data sharing, Cloud storage.**

1. Introduction

Cloud computing is an emerging technology in today's world. Cloud computing has an on demand process and also it has service and deployment models. Service models has four models Public Cloud, Private Cloud, Hybrid Cloud and community Cloud. Cloud computing has all resources in the form of internet in cloud resource pool and it allocates the different application services. By using cloud computing services many organization and enterprises maintain the grid computing environment can be very effectively. By the usage of Cloud computing, organizations and enterprises are very easy to access the cloud it is very efficient, scalability, effective, easy for doing their task.

Cloud Computing builds security mechanism for cloud storage is not easy work. Though it provides security to cloud it may hack by some adversaries or network hacker. Shared data on the cloud may use upon demand of the legitimate participants in the closed. Difficult to take proper access control because it involves increasing number of parties, devices and applications in the cloud with explosive growth of number of access points. Protecting shared data from unauthorized users on cloud is very difficult because shared data on cloud are vulnerable to lost or modify incorrectly by cloud provider or network hacker.

In Cloud there is an enormous amount of data available, cloud provider is a semi trusted due to profit CP may corrupt data or CP may fail to do their task correctly due to these drawbacks soo-young lee [1] proposed the data owner encrypt the data before uploading to the cloud. The file access by the legitimate user only. The cloud user should download the application of cloud or the user log on to the Google Cloud with help of web browser. One method for using Google Cloud is Console App.

In Big Data the cloud users are enterprises, organizations, hospitals etc. In hospital they maintain the health record of the patient's. The rapid development of cloud storage in service technology and explosive growth of information. Own cloud storage services are owned by many e-commerce enterprises.

2. Literature Survey

A. SAPDS: Self-healing attribute-based privacy aware data sharing in cloud [1]

The issue of this paper is storage of governing the data in the cloud system. The Cloud Contains the large volume data so that it occurs this type of issues.

Method: This Paper proposes "Self-healing Attribute-based Privacy aware Data Sharing" to gain fine grained access control over the outsourced data. This system done the key distribution and also this system helps to manage the cloud server for not seeping out any confidential information. The Data Owner only knows to whom the data want to be shared the data owner can restrict the illegal activities of the legitimate users. The user can change the particular information with the help of decryption policy, instead of modify the entire access control policy. Legitimate user can update their decryption keys by each participants revocation it makes self-healing without interact with the data owner. In Proposed system, the computation analysis shows data owner revoke the complexity of O(n) for n users and the decryption key can be update by the legitimate users with the Complexity O(1).

B. A new access control method based on multi-authority in cloud storage service [2]

Data has become an important asset in the arrival of the big data. In trending paid or unpaid data sharing in the usage of big data era and to maintain the security of data sharing it has a one of the key technique, in cloud storage services the access control plays an important role.

Method: “An Access Control method for revocation of user rights” in the cloud storage services is a proposed system in this paper. Two aspects involve to revoking user rights: revoking user and revoking attributes. In this paper the model is presented for Authority Attributes(AA), Data Owner(DO), user and cloud server. AA and DO generate a key component for each part which avoid the joint attack between the user and AA. The Analysis done for the scheme of the security by using the “Decisional Bilinear Diffie-Hellmen (DBDH)” theory. The Proposed Scheme has more efficiency in computation cost and in communication cost also this scheme is more effective in revoke the user rights when compared with other schemes.

Research Model:

1) Cloud Servers

It is a medium of semi trusted storage which has a strong computing power and capacity for storage. To gain benefits it acquire information as much as possible but it doesn’t perform any other operations in storing and re-encrypting the cipher text file.

1) Users

The user’s attributes satisfy the access policy the users can access the cipher text files which defined by the data owner. According to the attributes the key distributes to the user to prevent the joint attack among users, embed the random number into the private key which needed by data owner.

2) Authority Attribute

It distributes the relevant attributes and attribute keys to all the users and it can exchange some parameter with each other. The user can decrypt the file only if the property key available.

3) Data Owner

Data owner is responsible for providing access policies and attributes for legal users. Owner expects to access only the certain user also provide valid data. Also it proposes fuzzy identified-based encryption algorithm which describe the set of attributes to the user with the identity. They also proposed key policy attribute based encryption(KP-ABE). In KP-ABE part cipher text is associate with set of attributes the access control contains by the user key. The Linear Secret-Sharing Scheme (LSSS)is introduced in the encryption algorithm which reduces the time complexity and realize the encryption and decryption in polynomial time.

Encryption Scheme

The encryption scheme for the data security access control are,

1. Setup
2. Key Gen
3. Encrypt
4. Key Aggregation

Revocation Scheme:

1) Revoke User

The DO can revoke the user access to the public if the user exhibits any malicious or purchased expired service in the cloud storage of e-commerce. The DO has the rights to cancel the user that type of user cannot access the public resources. The Do generates the new Symmetric encryption key M for the user whenever they revoke and encrypts the file with new key.

2) Revoke Attributes

The large number of attribute keys and public keys are updated since the user properties has been revoked it is difficult to do Undo so this propose scheme revoke user attributes. Remaining user attributes are satisfy access to the structure tree.

C. Anonymous data sharing scheme in public cloud and its application in e-health record [4]

This paper is an example of data sharing used in Healthcare record. According to the healthcare record it stores vast amount of data regarding patient’s details along with their diseases. These data are uploaded in a public cloud server which is not trusted by users and most enterprises like to manage their data in the cloud servers. The challenge of security and privacy becomes immediate for broad deployment of the cloud systems when the data are outsourced to the cloud which is sensitive.

Method: The proposed system of this paper is “Secure Data Sharing Scheme” which provides flexible usage of data when solving the issues in security and privacy for data sharing. This scheme ensures security of the outsourced data and data owner’s privacy.

Data sharing done in the secret manner between the doctors about the patient details. It can be retrieved whenever they need. This Scheme is efficient and feasible for the e-health record users in the cloud. Cipher text policy implemented with the attribute based encryption (ABE). The Access Policy is declared by the hospital data owner.

3. Conclusion

This Paper conclude with the applications of cloud computing and also it involves in many schemes to safeguard the files or data in cloud also it provides privacy for the cloud users. The old detail can be retrieved using the cloud technology. This Paper helps to analyze about the schemes which used to keep the records very safe and secure.

References

[1] Zeeshan Pervez, Soo-young Lee,” SAPDS: Self-healing attribute-based privacy aware data sharing in cloud,” The Journal of Supercomputing, January 2017.

[2] Sheng Luo, Qiang Liu,” A new access control method based on multi-authority in cloud storage service” International Journal of Computational Intelligence Systems, Vol. 11. (2018). 483–495.

[3] J. Zhou et al., ‘‘Securing outsourced data in the multi-authority cloud with fine-grained access control and efficient attribute revocation,’’ Comput. J., vol. 60, no. 8, pp. 1210–1222, Aug. 2017.

[4] Huaqun Wang, “Anonymous Data Sharing Scheme in Public Cloud and its Application in E-Health Record,” IEEE Access pp. (99):1-1 · May 2018.

[5] Y. Tang, P. P. C. Lee, John C. S. Lui, and R. Perlman, ‘‘Secure overlay cloud storage with access control and assured deletion,’’ IEEE Trans. Dependable Secure Comput., vol. 9, no. 6, pp. 903–916, Nov./Dec. 2017.

[6] R. Ahuja, S. K. Mohanty, and K. Sakurai, ‘‘A scalable attribute-set-based access control with both sharing and full-fledged delegation of access privileges in cloud computing,’’ Comput. Elect. Eng., vol. 57, pp. 241–256, Jan. 2017.

[7] Y. S. Rao, ‘‘A secure and efficient ciphertext-policy attribute-based signcryption for personal health records sharing in cloud computing,’’ Future Gener. Comput. Syst., vol. 67, pp. 133–151 Feb. 2017.

[8] Q. Xu, C. Tan, Z. Fan, W. Zhu, Y. Xiao, and F. Cheng, ‘‘Secure multiauthority data access control scheme in cloud storage system based on attribute-based signcryption,’’ IEEE Access, vol. 6, pp. 34051–34074, 2018.

[9] V. Casola, A. Castiglione, K. K. Choo, and C. Esposito, ‘‘Health care related data in the cloud: Challenges and opportunities,’’ IEEE Cloud Comput., vol. 3, no. 6, pp. 10–14, Apr. 2016.

[10] L. Wu, Y. Zhang, K.-K. R. Choo, and D. He, ‘‘Efficient and secure identity based encryption scheme with equality test in cloud computing,’’ Future Gener. Comput. Syst., vol. 73, pp. 22–31, Aug. 2017.

[11] J. Luo, H. Wang, X. Gong and T. Li, A novel role-based access control model in cloud environments, International Journal of Computational Intelligence Systems 9 (2016), no. 1, 1-9.

[12] L. X. Xie, F. K. Bo, and B. B. Zhao, virtual group revocation policy-based cloud storage access control model. Computer Science, 43(2016),122-126.

[13] Z. Xu and K. M. Martin, Dynamic user revocation and key refreshing for attribute-based encryption in cloud storage, IEEE International Conference on Trust, Security and Privacy in Computing and Communications, 2017.

[14] M. Rezvani, A. Ignjatovic, E. Bertino, and S. Jha, ‘‘Secure data aggregation technique for wireless sensor networks in the presence of collusion attacks,’’ IEEE Trans. Dependable Secure Comput., vol. 12, no. 1, pp. 98– 110, Jan./Feb. 2016.

[15] K. Xue et al., ‘‘RAAC: Robust and auditable access control with multiple attribute authorities for public cloud storage,’’ IEEE Trans. Inf. Forensics Secur., vol. 12, no. 4, pp. 953–967, Apr. 2017.