Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, Issue 6, June : 2023

A NOVEL APPROACH FOR EFFICIENT ENCRYPTION SCHEME IN CLOUD USING ABE ALGORITHM

KALAKATLA HARITHA, MCA, DCA, DVR & Dr.Hima Shekar MIC College of Technology, A.P., India.
MARESWARAMMA. P, Associate Professor, Dept.of AI & IT, DVR & Dr.Hima Shekar MIC college of Technology, A.P., India.

Abstract— The proposed system, the system put forward a CP-ABE with shared decryption (CP-ABE-SD) scheme to address the above problem. Besides the authorized user, multiple delegated users can also collaborate to recover the message in our solution. At the same time, we can verify the correctness of the decrypted results. To reduce the computation cost for encryption and decryption and save storage costs, an integrated access tree is used in our scheme as that in the scheme. CLOUD storage is a new storage technology based on network and cloud computing, which provides "unlimited" storage resources for data users. Users can easily access the data stored in the cloud from anywhere in the world. More personal and corporate data are being stored on cloud storage servers. These businesses and individuals can significantly reduce the cost of data storage and management by storing their data on the remote cloud storage servers. However, the cloud service provider, such as Google Cloud, IBM Cloud, and Microsoft Cloud, may be curious or profit-driven to leak users' sensitive data. In addition, these data stored on remote cloud storage servers may be attacked, modified, and disclosed by hackers. Therefore, users tend to encrypt their files before storing these files on an untrusted cloud storage server. In order to ensure the correctness of the files, some remote data integrity checking schemes were proposed.

INTRODUCTION

Cipher text-policy attribute-based encryption (CP-ABE) has been a preferred encryption technology to solve the challenging problem of secure data sharing in cloud computing. The shared data files generally have the characteristic of multilevel hierarchy, particularly in the area of healthcare and the military. However, the hierarchy structure of shared files has not been explored in CP-ABE. In this paper, an efficient file hierarchy attribute-based encryption scheme is proposed in cloud computing. The layered access structures are integrated into a single access structure, and then, the hierarchical files are encrypted with the integrated access Structure. The cipher text components related to attributes could be shared by the files. Therefore, both cipher text storage and

time cost of encryption is saved. Ciphertext -policy attribute based encryption is one of possible technique which has much more flexibility and is more suitable for general applications. In cloud computing, as illustrated in authority accepts the user enrollment and creates some parameters. Cloud service provider is the manager of cloud servers and provides multiple services for client. Data owner encrypts and uploads the generated ciphertext to CSP. Cloud gives number of advantages like better reliability, flexibility and security user do not have to keep the data as it is maintained by the cloud service provider, pay only that they used, portability user can access his data from everywhere with the help of internet and they do not need to transmit the physical data storage devices, enabling suitable, on-demand network access. Though these benefits make cloud storage a very economical option for storing data it has some drawbacks like the data loss incidents may take place. There are lots of inner and outer threats, for the payback of their ownership, CSP to behave disloyally like data loss occurrence may be kept secret from client to maintain position, and there may be viruses in the network path or in the software [1]. Security and privacy issues of cloud storage are verification, correctness of data, availability, data leakage, data loss. So, it requires an auditing service to check the reliability of outsourced data. As clients have limited capacity and they are only able to upload and download data from cloud storage. User downloads all data in order to check integrity of stored data. It is very costly and tedious task, particularly when the user is set with a low calculation device (e.g. smart phone) or is not for all time related to the Internet. Therefore, it is necessary to offer an efficient audit service to check the availability and integrity of the stored data. In the proposed system a Third Party Auditor (TPA) is introduced who will verify the data integrity of the client's data stored on cloud storage. TPA audit data when user needed. TPA has more prospective than user and advantageous for cloud provider too because audit result from TPA gives more values for Cloud base service platform and also they fulfill the cloud computing concerns [2]. Finally, this software/application provides the user with the ability to store the encrypted data in storage cloud and encryption/decryption keys in security cloud service, and no single cloud service contributor has access to both. Other benefit of delegating responsibility to trusted third party is that it reliefs the client from any kind of key administration or over head is maintainance of any key information related to data on it device, because it allows the client to use any browser enabled devices to access such service.

LITERATURE REVIEW

Goyal et al. [10] gave a KP-ABE scheme in 2006. In this scheme, an access structure is related to the private key of a user. At the same time, an attribute set is related to the ciphertext. In 2007, Bethencourt et al. [11] provided a CP-ABE scheme. His scheme is more practical and more flexible than KP-ABE scheme. In a CP-ABE scheme, an attribute set is

related to the private key of the user, while an access structure is related to the cipher text. A user is able to decrypt the cipher text only if his/her attribute set satisfies the access policy. In 2016, Wang et al. [33] provided a file hierarchical cipher text-policy attribute based encryption (FH-CP-ABE) scheme, which greatly improved the efficiency of scheme [11] without sacrificing the security. In many cases, these stored data files in public cloud are characterized by multi-level hierarchy. Scheme [33] combines multiple different hierarchical access policy trees into a single one. As shown in the Fig. 1, file 1 *m* and file 2 *m* have a hierarchical relationship on access. Access tree 1 can be integrated with access tree 2 into a new access tree . Finally, file 1 *m* and file 2 *m* can be encrypted simultaneously by using the access tree , instead of encrypting it twice with two different access trees. Scheme [33] is efficient on both encryption and decryption, and the scheme also saves the storage overhead of the cipher text greatly. However, scheme [33] is not suitable for the case of multi-authority system, where the attributes belonging to a user are managed by different authorities. To solve the issue, Zhang et al. [34] improved above FH-CP-ABE scheme and provided a multi-authority hierarchical ABE scheme. There are multiple authorities in scheme [34] and an integrated access tree is used to encrypt these hierarchical files. However, there is a central authority in scheme [34], which is not sufficient for distributed systems. To overcome this issue, based on the hierarchical structure of personal health record (PHR) files, Guo et al. [35] provided a unique ABE scheme with multiple authorities. In addition, Li et al. [36] gave a more practical file hierarchical CP-ABE scheme to overcome the disadvantage that FH-CP-ABE scheme [33] cannot encrypt more than one file in the same level. For those big companies or institutions, scheme [36] can securely and efficiently store their data in the cloud, which is more flexible and practical than scheme [33]. However, if the stored files have not the characteristic of multiple hierarchical structures, above schemes [33-36] will fail due to the lack of the integrated access trees. In order to solve this issue, Fu et al. [37] proposed an attribute based hierarchy encryption scheme (ABHE) to encrypt a collection of documents.

RELATED WORK

The cloud can perform the following operations.

UPDATE OPERATION

In cloud data storage, sometimes the user may need to modify some data block(s) stored in the cloud, this refer this operation as data update. In other words, for all the unused tokens, the user needs to exclude every occurrence of the old data block and replace it with the new one.

DELETE OPERATION

Sometimes, after being stored in the cloud, certain data blocks may need to be deleted. The delete operation this are considering is a general one, in which user replaces the data block with zero or

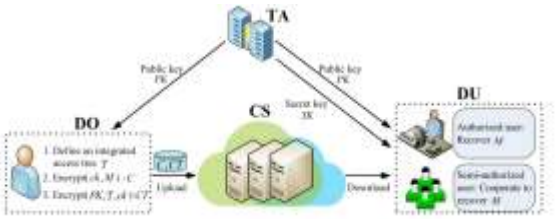
some special reserved data symbol. From this point of view, the delete operation is actually a special case of the data update operation, where the original data blocks can be replaced with zeros or some predetermined special blocks.

APPEND OPERATION

In some cases, the user may want to increase the size of his stored data by adding blocks at the end of the data file, which this refer as data append.I anticipate that the most frequent append operation in cloud data storage is bulk append, in which the user needs to upload a large number of blocks (not a single block) at one time.

INSERT OPERATION

An insert operation to the data file refers to an append operation at the desired index position while maintaining the same data block structure for the whole data file, i.e., inserting a block F[j] corresponds to shifting all blocks starting with index j + 1 by one slot.



PROPOSED WORK

attribute based hierarchy encryption scheme (ABHE) to encrypt a collection of documents. Based on the access attributes of these files in the document collection, an integrated access tree is constructed with a greedy algorithm in scheme [37]. Finally, the document collection is encrypted with the integrated access tree, just like the above scheme [33-36].

DISADVANTAGES OF EXISTING SYSTEM

The system is not implemented CP-ABE-SD Scheme method.

The system is implemented FH-CP-ABE in which the scheme cannot encrypt more than one file in the same level

PROPOSED SYSTEM:

The proposed system, the system put forward a CP-ABE with shared decryption (CP-ABE-SD) scheme to address the above problem. Besides the authorized user, multiple delegated users can also collaborate to recover the message in our solution. At the same time, we can verify the correctness of the decrypted results. To reduce the computation cost for encryption and decryption and save storage costs, an integrated access tree is used in our scheme as that in the scheme .

Finally, the plaintext is encrypted with the integrated access tree. Frequent data encryption and decryption operations make cloud storage very inefficient. In our scheme, the shared message is encrypted only once and size of the ciphertext is small. Our solution improves the efficiency of cloud storage.

Advantages:

- The security of the proposed CP-ABE-SD scheme is reduced to the DBDH assumption.
- In order to ensure the correctness of the files, some remote data integrity checking schemes have been proposed.

CONCLUSION

In this paper, we propose a two cipher text-policy attribute based encryption schemes with shared decryption. There are two kinds of data users in our schemes. For an authorized user, he/she can recover the message independently. When the authorized user cannot decrypt the cipher text in time for some reason, these semi-authorized users can cooperate to decrypt the cipher text to replace the authorized user. An integrated access tree is used in proposed schemes to improve the efficiency of the schemes. The security for our schemes is proved under the DBDH assumption. The experimental result shows that CP-ABE-SD scheme is better than scheme [11,33,36] in terms of storage cost and computational overhead.

REFERENCES

[1] S. Abolfazli, Z. Sanaei, E. Ahmed, A. Gani, and R. Buyya, "Cloud-based augmentation for mobile devices: motivation, taxonomies, and open challenges," *IEEE Communications Surveys & Tutorials*, vol. 16, no. 1, pp. 337–368, 2014.

[2] J. Aikat et al., "Rethinking security in the era of cloud computing," *IEEE Security Privacy*, vol. 15, no. 3, pp. 60-69, Jun. 2017. [3] J. Li, H. Yan, and Y. Zhang, "Efficient identity-based provable multi-copy data possession in multi-cloud storage,"*IEEE Transactions on Cloud Computing*, DOI: 10.1109/TCC.2019.2929045.

[4] J. Li, H. Yan, and Y. Zhang, "Certificateless public integrity checking of group shared data on cloud storage," *IEEE Transactions on Services Computing*, to be published. DOI 10.1109/TSC.2018.2789893.

[5] H. Yan, J. Li, and J. Han, "A novel efficient remote data possession checking protocol in cloud storage," *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 1, pp. 78-88, Jan. 2017.

[6] H. Yan, J. Li, and Y Zhang, "Remote data checking with designated verifier in cloud storage," *IEEE Systems Journal*, vol. 14, no. 2, pp. 1788-1797, 2020.

[7] J. Li, H. Yan, and Y. Zhang, "Identity-based privacy preserving remote data integrity checking for cloud storage," *IEEE Systems Journal*. DOI:10.1109/JSYST.2020.2978146.

[8] L. Zhang, H. Xiong, Q. Huang, J. Li, K. K. Raymond Choo, and J. Li, "Cryptographic solutions for cloud storage: challenges and research opportunities," *IEEE Transactions on Services Computing*, DOI: 10.1109/ TSC.2019.2937764.

[9] A. Sahai and B. Waters, "Fuzzy identity based encryption,"*Advances in Cryptology-Eurocrypt 2005, Lecture Notes in Computer Science, vol. 3494, Springer, 2005*, pp. 457-473.

[10] V. Goyal, O. Pandey, A. Sahai, and Brent Waters, "Attribute-based encryption for fine-

grained access control of encrypted data,"*Proc. 13th ACM Conference on Computer and Communications Security*, 2006, pp. 89–98.

[11] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption,"*IEEE Symposium on Security and Privacy*, vol. 2008, pp. 321-334, Jun. 2007.

[12] J. Lai, R. H. Deng, and Y. Li, "Expressive CP-ABE with partially hidden access structures," *Proc. 7th ACM Symposium on Information, Computer and Communications Security*, pp. 18-19, 2012.