File Access using Domain Authority based Procedure

D.Saravanan
Faculty of Operations & IT
ICFAI Business School (IBS), Hyderabad,
The ICFAI Foundation for Higher Education (IFHE)
(Deemed to be university u/s 3 of the UGC Act 1956)
Hyderabad-India.

Abstract

Cloud computing has become one of the most emerging field in the technology park. Schemes such as attribute-based encryption technique are used for the access control of the third-party data. In this approach, hierarchical attribute-set based encryption (procedure is implemented by extending the cipher-text policy attribute-based encryption. The proposed system achieves fine access-control due to its hierarchical structure. It controls the access of complex structured data in a flexible and secured manner. The cipher-text policy enhances the flexible performance for the third-party data

Keywords *- Access control, cloud computing, Distributed Environment, Cryptography, Encryption, Decryption*

I. INTRODUCTION

Cloud computing is based on the distributed computing, network security and service-oriented architecture. Due to its various benefits, cloud computing has become the most beneficial pattern in the IT industry. Cloud computing reduces costs and capital expenditures, increases operational efficiencies, scalability, flexibility and immediate market growth. Commercial cloud computing has been built such as Google App Engine ,Amazon's S3, IBM's Blue cloud , Sales' Customer Relation Management .

One of the vital security concerns are privacy preserving and data security in cloud computing. Users send the data to the cloud service provider for storage while the cloud service provider is itself an innovative premises which cannot be trusted totally. So the confidential data are not to be disclosed to the business organization otherwise enterprise users will face serious outcomes. Henceforth the data security is at the priorest requirement.Fine-grained access control and flexible access is desired in the service-oriented architecture. For instance, the health-care system requires restricted access of medical records which should be displayed only to the eligible doctors, similarly, a customer relation management on a cloud should be allowed access of information to the high-level executives of the respective company only. Such sensitive records are either required by the legislation or by company regulations.

In this paper, first the hierarchical attribute set based encryption method is shown in extension with the ASBE algorithm with a hierarchical architecture to show flexible and scalable access of data [6] .Next this scheme enhances user grant , file creation, user revocation , file access and file deletion based on Hierarchical attributed set based encryption. Thirdly it analyzes its performance by enhancing CP-ABE technique. Lastly, hierarchical attributed set based encryption technique is implemented to experiment performance evaluation.

II. PROBLEM DEFINITION

A. Existing System

The traditional method to protect sensitive data from third parties is to store encrypted data on servers, while the decryption keys are disclosed to authorize users only. Such solution requires an efficient key management mechanism to distribute decryption keys to authorized users, which has been pr oven to be very difficult. Next, this scheme lacks scalability and flexibility; as the number of authorized users becomes large, the solution will not be efficient any more. In case, legitimate user needs to be revoked, related data has to be re-encrypted and new keys must be distributed to the existing legitimate users again. Data owners need to remain online every time so as to provide keys to authorize users as well as to encrypt or re-encrypt data.

B. Disadvantage

- Ciphertexts are encrypted to multiple user.
- No administrator is there to maintain security.
- Complex to store data since ABE scheme is not flexible.
- User revocation is difficult in CP-ABE scheme.

III. PROPOSED SYSTEM

The cloud computing system consists of five types of parties: a cloud service provider, data owners, data consumers, domain authority or a number of domain

authorities, and a trusted authority organized in an hierarchical manner. The cloud service provider manages a cloud to provide data storage service. The data files are encrypted by the data owners. Data owners store the encrypted files in the cloud for sharing it with the data consumers. Data consumers access the shared data files by downloading the encrypted data files from the cloud and decrypt them. Each data owner/consumer is controlled by a domain authority. A domain authority is managed by its head domain authority or the trusted authority. The trusted authority is the root authority, responsible for managing top-level domain authorities. Each domain authority is responsible for managing the domain authorities at the next level or the data owners/consumers in its domain[6].

A. Advantages

- Cipher texts are encrypted to one particular user as well as to multiple users.
- Domain authority performs the administrator process for security.
- Flexible and secure to store data since Hierarchical attribute set based encryption scheme is used.
- Efficient user revocation is followed.

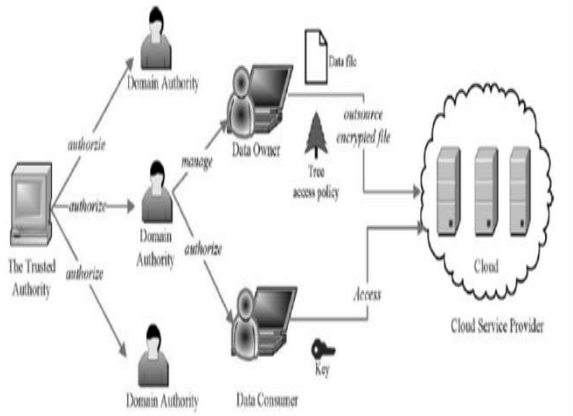
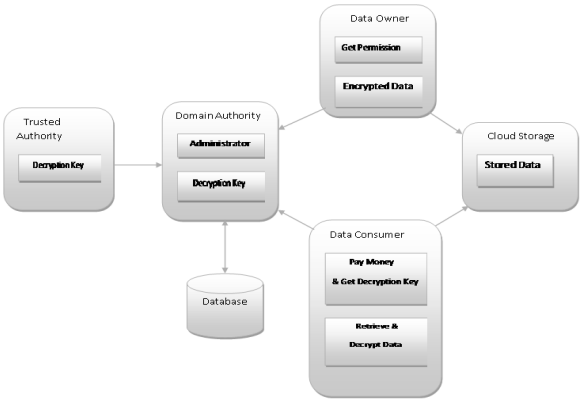


Fig.1. Hierarchical attribute set based encryption System Model

The data owner gets the public key from the domain authority provided by the trusted authority. The data owner encrypts the data file with the help of the key provided. The domain authority is the chief administrator who manages the data owner as well as the data consumer. The domain authority distributes the keys to the data owner and the consumer. The trusted authority is the main authority that generates the public and private keys. The data owner store the encrypted file in the cloud storage for sharing it with the authorize consumers. The data consumer gets the encrypted file from the cloud and then decrypts it with the help of private key provided by the trusted authority.



IV. EXPERIMENTAL SETUP

First, the hierarchical ASBE extends the ASBE algorithm improves flexibility and security thereby inherits the feature of fine access control. Second, a full-fledged access control scheme based on hierarchical attribute set based encryption scheme is used. The scheme supports authority grant, user grant, creation/deletion of file, and user revocation in cloud computing. The system model consists of a trusted authority, multiple domain authorities, and several users corresponding to data owners and consumers. The trusted authority generates root master keys, provides system parameters as well as authorizes the top-level domain authorities. A domain authority distributes keys to the sub-domain authorities. Each user is assigned a key structure which specifies the attributes associated with the decryption key.

Algorithm: Hierarchical attribute set based encryption scheme is used.

Step1: System Setup: Declare d as dept parameter.
It outputs public key PK declared public and master key MK which is kept secret.
Step2: KeyGen (MK, u, A)
It inputs master secret key MK, user u andkey structure A and outputs master secret key SKu for user u.
Step3: Encrypt (PK, M, T)
It inputs public key PK, message M and access tree T and outputs cipher text CT.
Step4: Decrypt(CT, SKu)
It takes input a ciphertext CT and
a secret key SKu for user and it outputs a message m . If
the key structure associated with the secret key
satisfies the access tree T, associated with the ciphertext CT,then m is the original correct message M otherwise m null.

V. EXPERIMENTAL RESULT

This page show that the data owner send request to the domain authority and receives request by the trusted authority.

Fig. 3. Domain authority receives request from data consumer and send it to the trusted authority

This page shows that the trusted authority sends public key to the domain authority.

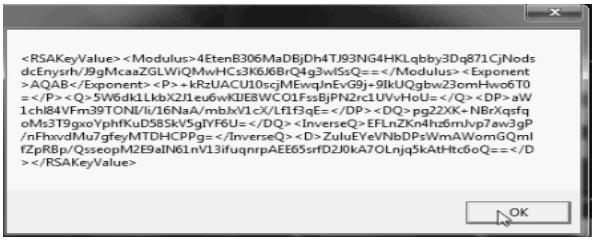


Fig. 4. Trusted authority sends the private key to the domain authority.

This page shows that the domain sends the private key to the data consumer.

Fig. 5. Domain authority sends the private key to the data consumer

This page shows that the cloud storage sends the encrypted file to the data consumer.

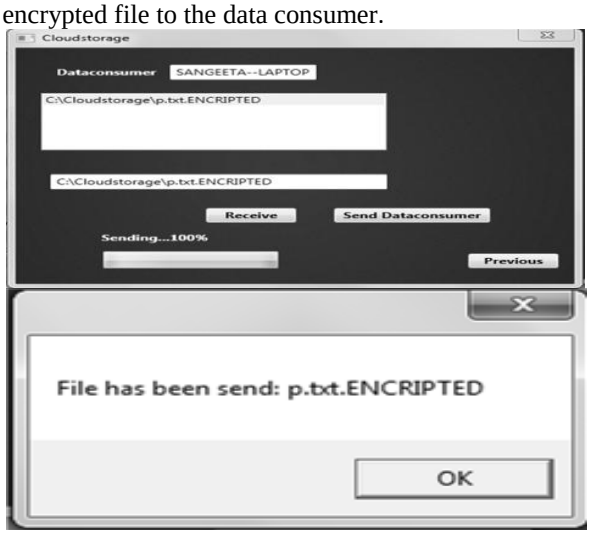


Fig. 6. Cloud storage sends the encryptedfile to the data consumer

This page shows that the data consumer receives the encrypted file and then decrypts it with the help of private key.

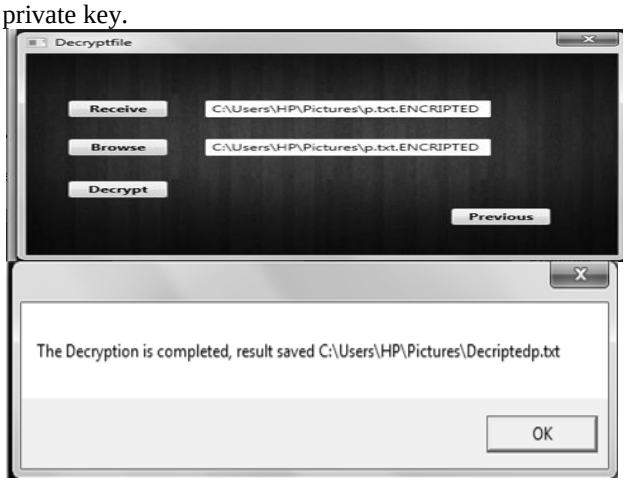


Fig. 7. Dataconsumer decrypt the encrypted file

VI. CONCLUSION AND FUTURE WORK

The goal is achieved by exploiting and individually combining techniques of attribute-based Encryption proxy re-encryption, and lazy re-encryption. Our proposed scheme also has most important properties of user access privilege confidentiality and user secret key accountability. Extensive analysis shows that our proposed schemes is highly efficient and provably secure under existing security models.ur analysis shows that proposed schemes is highly efficient and proved to be secure under existing security models. These proposed schemes only support the text files. As a future work we can implement the image files.

REFERENCES

[1] R. Buyya, C. ShinYeo, J. Broberg, and I. Brandic, "Cloud computing and emerging it platforms: Vision, hype, and reality for delivering computing as the 5th utility," Future Generation Comput. Syst., vol. 25, pp.599–616, 2009.

[2] S. Yu, C. Wang, K. Ren, and W. Lou, "Achiving secure, scalable, and fine-grained data access control in cloud computing," in Proc. IEEE INFOCOM 2010, 2010, pp. 534–542.

[3] D.Saravanan, Dr.S.Srinivasan, " A proposed New Algorithm for Hierarchical Clustering suitable for Video Data mining.", International journal of Data Mining and Knowledge Engineering", Volume 3, Number 9, July2011.Pages 569-572

[4] D.Saravanan, "Clustering the irregularity events in intelligence surrounding systems" Int. Journal of pure and applied mathematics, Vol. 119, No.12(2018), Pages 15025-15035, May-2018 (Special Issues) , ISSN:1311-8080.

[5] R. Bobba, H. Khurana, and M. Prabhakaran, "Attribute-sets: A practically motivated enhancement to attribute-based encryption," in Proc. ESORICS, Saint Malo, France, 2009.

[6] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attributebased encryption," in Proc. IEEE Symp. Security and Privacy, Oakland, CA, 2007.

[7] A. Sahai and B. Waters, "Fuzzy identity based encryption," in Proc. Acvances in Cryptology—Eurocrypt, 2005, vol. 3494, LNCS, pp. 457–473.

[6] G.Wang, Q. Liu, and J.Wu, "Hierachical attibute-based encryption for fine-grained access control in cloud storage services," in Proc. ACM Conf. Computer and Communications Security (ACM CCS), Chicago, IL, 2010.

[7] D.Saravanan, "Video data image retrieval using – BRICH", World journal of Engineering, Vol.14, Issuu 4, Pages 318-323, Aug 2017.

[8] D.Saravanan, Dr.S.Srinivasan, "Video Image Retrieval Using Data Mining Techniques "Journal of Computer pplications, Volume V, Issue No.1. Jan-Mar 2012. Pages39-42. ISSN: 0974-1925

[9] V. Goyal, O. Pandey, A. Sahai, and B.Waters, "Attibute-based encryption for fine-grained access control of encrypted data," in Proc. ACM Conf. Computer and Communications Security (ACM CCS), Alexandria, VA, 2006.

[10] H. Harney, A. Colgrove, and P. D. McDaniel, "Principles of policy in secure groups," in Proc. NDSS, San Diego, CA, 2001.

[11] P. D. McDaniel and A. Prakash, "Methods and limitations of security policy reconciliation," in Proc. IEEE Symp. Security and Privacy, Berkeley, CA, 2002.

[10] T. Yu and M. Winslett, "A unified scheme for resource protection in automated trust negotiation," in Proc. IEEE Symp. Security and Privacy, Berkel ey, CA, 2003.