RESEARCH ARTICLE OPEN ACCESS

Empowered Service Delegation With Attribute Encryption For Distributed Cloud Computing

[1] S.Vidhya, [2] R.Raja Ramya, [3] N.kanagavalli
Assistant Professor/IT, Saveetha Engineering College, Chennai, vidhyas_1983@yahoo.com
Assistant Professor/IT, Saveetha Engineering College, Chennai,ramyanitha@gmail.com
Assistant Professor/IT, Saveetha Engineering College, Chennai, kvalli.818@gmail.com

Abstract
Cloud computing has emerged as one of the most influential paradigms in the IT industry. In this, new computing technology requires users to entrust their valuable data to cloud providers, there have been increasing security and privacy concerns on outsourced data. Several schemes employing attribute-based encryption (ABE) have been proposed for access control of outsourced data in cloud computing. The most of them suffer from inflexibility in implementing complex access control policies. In this paper, allowing cloud service providers (CSPs), which are not in the same trusted domains as enterprise users, to take care of confidential data, may raise potential security and privacy issues. To keep the sensitive user data confidential against untrusted CSPs, Natural way is to apply cryptographic approaches, by disclosing Decryption keys only to authorized users. But also provide high performance, full delegation, and scalability, so as to best serve the needs of accessing data anytime and anywhere, delegating within enterprises, and achieving a dynamic set of users.HASBE employs multiple value assignments for access expiration time to deal with user revocation more efficiently than existing schemes. It can be provide fine-grained access control and full delegation. Based on the HASBE model, Finally, we propose a scalable revocation scheme by delegating to the CSP most of the computing tasks in revocation, to achieve a dynamic set of users efficiently.
Keyword: To achieve scalability, flexibility, fine grained access control using service delegation simultaneously.

I. INTRODUCTION

Cloud computing is built on virtualization, parallel and distributed computing, utility computing and service-oriented architecture. We introduce new functionalities such as a flexible and dynamic description of resources; an advanced delegation mechanism and support for audit ability, accountability and access confinement. In this, computing on one hand, enterprise users no longer need to invest in hardware/software systems or hire IT professionals to maintain these IT systems, thus they save cost on IT infrastructure and human resources. On the other hand, computing utilities provided by cloud computing are being offered at a relatively, low price in a pay-as-you-use style.

In cloud computing, users have to give up their data to the cloud service provider for storage and business operations, while the cloud service provider is usually a commercial enterprise which cannot be totally trusted. Data confidentiality is not the only security requirement. Flexible and fine-grained access control is also strongly desired in the service-oriented cloud computing model.

Motivation: Our main design goal is to help the enterprise users to efficiently share confidential data on cloud servers. Specifically, we want to make our scheme more applicable in cloud computing by simultaneously achieving fine-grained access control, high performance, flexibility, and scalability.

Contribution of the paper: It is multifold. First, we show how HASBE extends the ASBE algorithm with a hierarchical structure to improve scalability and flexibility while at the same time inherits the feature of fine-grained access control of ASBE. Second, in the case of a large-scale industry, a delegation mechanism in the generation of keys inside an enterprise is needed. Although some CP-ABE schemes support delegation
Between users, this enables a user to generate attribute secret keys containing a subset of his own attribute
Secret keys for other users, we hope to achieve a full delegation. Third, we formally prove the security of the proposed scheme based on the security of the CP-ABE scheme and analyze its performance in terms of computational overhead.

II. RELATED WORK

In this section, we review the notion of attribute-based encryption (ABE), and provide a brief overview of the ASBE scheme. After that, we examine existing access control schemes based on ABE.

Attribute-Based Encryption

In the ABE scheme, cipher texts are not encrypted to one particular user as in traditional public-key cryptography. Both cipher texts and users' decryption keys are associated with a set of attributes or a policy over attributes. A user is able to decrypt a cipher text only if there is a match between his decryption key and the cipher text. ABE schemes are classified into key-policy attribute- based encryption (KP-ABE) and cipher text policy attribute based encryption (CP-ABE), depending how attributes and policy are associated with cipher texts and users' decryption keys

Access Control Solutions for Cloud Computing

The traditional method to protect sensitive data outsourced to third parties is to store encrypted data on servers, while the decryption keys are disclosed to authorize users only. However, such a solution requires an efficient key management mechanism to distribute decryption keys to authorized users, which has been proven to be very difficult. In case a previously legitimate user needs to be revoked, related data has to be re-encrypted and new keys must be distributed to existing legitimate users again.

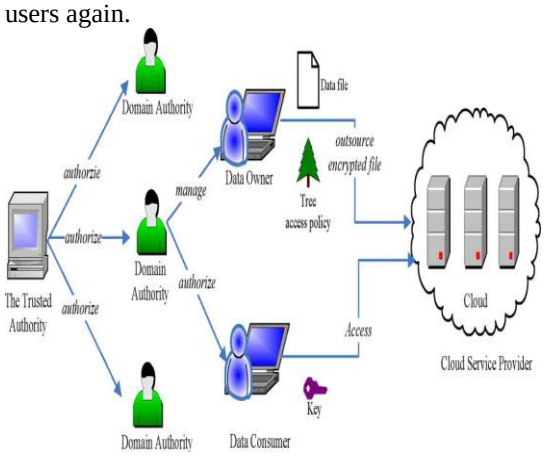

Fig.1. System model.

III. SYSTEM MODEL AND ASSUMPTION

A. System Model

The cloud computing system under consideration consists of five types of parties: a cloud service provider, data owners, data consumers, a number of domain authorities, and a trusted authority. The cloud service provider manages a cloud to provide data storage service. Data owners encrypt their data files and store them in the cloud for sharing with data consumers. In our system, neither data owners nor data consumers will be always online. They come online only when necessary, while the cloud service provider, the trusted authority, and domain authorities are always online.

B. Security Model

We assume that the cloud server provider is untrusted in the sense that it may collude with malicious users (short for data owners/data consumers) to harvest file contents stored in the cloud for its own benefit. In the hierarchical structure of the system users given in each party is associated with a public key and a private key, with the latter being kept secretly by the party.

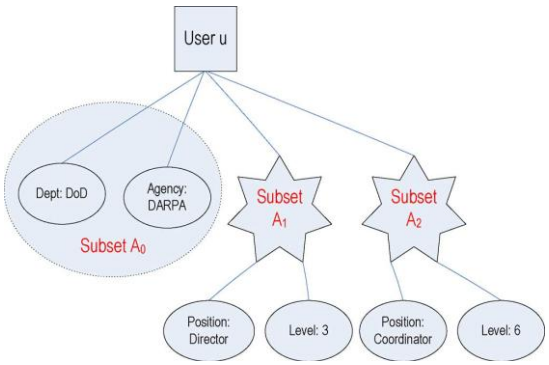

Fig .2. Example key structure

The trusted authority acts as the root of trust and authorizes the top-level domain authorities. A domain authority is trusted by its subordinate domain authorities or users that it administrates, but may try to get the private keys of users outside its domain. Users may try to access data files either within or outside the scope of their access privileges.

IV. HASBE SCHEME

The proposed HASBE scheme seamlessly extends the ASBE scheme to handle the hierarchical structure of system users. The main operations of HASBE: System Setup, Top-Level Domain Authority Grant, New Domain Authority/User Grant, New File Creation, User Revocation, File Access, and File Deletion.

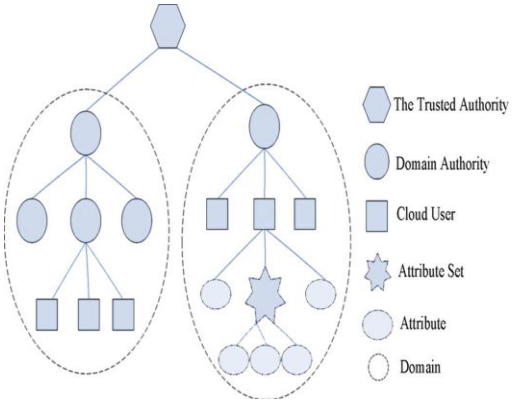

Fig.3. Hierarchical Structure of User

New File Creation:

To protect data stored on the cloud, a data owner first encrypts data files and then stores the encrypted data files on the cloud. A data file is processed by the data owner as follows:

• Pick a unique ID for this data file.

• Randomly choose a symmetric data encryption key, where is the key space, and encrypt the data file using.

• Define a tree access structure for the file and encrypt with using algorithm of HASBE which returns ciphetext. Finally, the encrypted data file is stored.

User Revocation:

Whenever there is a user to be revoked, the system must make sure the revoked user cannot access the associated data files any more. One way to solve this problem is to re-encrypt all the associated data files used to be accessed by the revoked user, but must also ensure that other users who still have access privileges
to these data files can access them correctly. HASBE inherits the advantage of ASBE in efficient user revocation.

V. SECURITY PROOF AND DISCUSSION

A.Security Proof

HASBE is extended from ASBE *with* a hierarchical structure using a delegation algorithm similar to the one described in the CP-ABE scheme. It prove the security of our scheme directly based on the security of CP-ABE. Thus, HASBE is expected to have the same security property as CP-ABE, which has been proven to be secure under the generic bilinear group model

Definition 1: A cipher text-policy ABE scheme is secure if all polynomial time adversaries have at most a negligible advantage.

Theorem 1: Suppose there is no polytime adversary who can break the security of CP-ABE with no negligible advantage; then there is no polytime adversary who can break our system with non negligible advantage.

Proof: Suppose we have an adversary with non negligible advantage against our proposed scheme. Using, we show how to build an adversary that breaks the CP-ABE scheme with no negligible advantage. The adversary can play a similar game with the CP-ABE scheme. The CP-ABE security model is also composed of four steps: Setup, Phase 1, Challenge, Phase 2 and Guess.

B. Discussion

1) Scalability: We extend ASBE with a hierarchical structure to effectively delegate the trusted authority's private attribute key generation operation to lower-level domain authorities. By doing so, the workload of the trusted root authority is shifted to lower-level domain authorities.

2) Flexibility:
HASBE organizes user attributes into a recursive set structure and allows users to impose dynamic constraints on how those attributes may be combined to satisfy a policy. So HASBE can support compound attributes and multiple numerical assignments for a given attribute conveniently

3) Fine-grained access control:
Based on HASBE, our scheme can easily achieve fine-grained access control. A data owner can define and enforce expressive and flexible access policy for data files as the scheme.

4) Efficient User Revocation: To deal with user revocation in Cloud computing, we add an attribute to each user's key and employ multiple value assignments for this attribute. So we can update user's key by simply adding a new expiration value to the existing key.

5) Expressiveness:
In HASBE, a user's key is associated with a set of attributes, so HASBE is conceptually closer to traditional access control methods such as Role Based Access Control (RBAC).Thus, it is more natural to apply HASBE, instead of KP-ABE, to enforce access control.

VI. PERFORMANCE ANALYSIS AND IMPLEMENTATION

A. Performance Analysis

System Setup

When the system is set up, the trusted authority selects a bilinear group and some random

numbers.When and is generated; there will be several exponentiation operations. So the computation complexity of System Setup.

Top-Level Domain Authority Grant

This operation is performed by the trusted authority. The master key of a domain authority is in the form of, where is the key structure associated with a new domain authority, is the set of . Let be the number of attributes in , and be the number of sets in . Then the computation of consists of two exponentiations for each attribute in , and one exponentiations for every set in . The computation complexity of Top-Level Domain Authority Grant operation is 0(2N+M).

New User/Domain Authority Grant

In this operation, a new user or new domain authority is associated with an attribute set, which is the set of that of the upper level domain authority. The main computation overhead of this operation is rerandomizing the key. The computation complexity is , where is the number of attributes in the set of the new user or domain authority, and is the number of sets in A.

B. Implementation

Hasbe-setup
Hasbe-keygen
Hasbe-keydel
Hasbe-keyup
Hasbe-enc
Hasbe-dec
Hasbe-rec

T**op-Level Domain Authority Grant**

It is performed with the command line tool **hasbe-keygen**. The cost is determined by the number of subsets and attributes in the key structure. When there is only one subset in the key structure, the cost grows linearly with the number of attributes as shows. While the number of attributes in the key structure is fixed to be 50, the cost also increases linearly with the number of subsets as with the command; a domain authority DA can perform *New User/Domain Authority Grant* for a new user or another domain authority in his domain. The cost depends on the number of subsets and attributes to be delegated.

VII. CONCLUSION

In this HASBE scheme for realizing scalable, flexible, and fine-grained access control in cloud computing. The HASBE scheme seamlessly incorporates a hierarchical structure of system users by applying a delegation algorithm to ASBE. HASBE not only supports compound attributes due to flexible attribute set combinations, but also achieves efficient user revocation because of multiple value assignments of attributes. We formally proved the security of HASBE based on the security of CP-ABE Finally, we implemented the proposed scheme, and conducted comprehensive performance analysis and evaluation, which showed its efficiency and advantages over existing schemes.

REFERENCES

[1] R. Buyya, C. ShinYeo, J. Broberg, and I. Brandic, "Cloud computing and emerging it platforms: Future Generation Comput.Syst" vol.25, pp. 599–616, 2009.
[2] B. Barbara, "Salesforce.com: Raising the level of networking," Inf. Today, vol. 27, pp. 45–45, 2010.
[3] J.Bell, Hosting Enterprise Datainthe Cloud Part9: InvestmentValue Zeta, Tech. Rep., 2010.
[4] A. Ross, "Technical perspective: A chilly sense of security," Commun. ACM, vol. 52, pp. 90–90, 2009.
[5] G. Wang, Q. Liu, and J. Wu, "Hierarchical attribute based encryption for fine-grained access control in cloud storage services," in Proc. ACM Conf. Computer and Communications Security (ACM CCS), Chicago, IL, 2010.
[6] S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving secure, scalable, and fine-grained data access control in cloud computing," in Proc. IEEE INFOCOM 2010, 2010, pp. 534–542.
[7] R. Bobba, H. Khorana, and M. Prabhakaran, "Attribute-sets: A practically motivated enhancement to attribute-based encryption," in Proc. ESORICS, Saint Malo, France, 2009.
[8] J. Bethencourt, A. Sahai, and B. Waters, "Cipher text-policy attribute- based encryption," in Proc. IEEE Symp. Security and Privacy, Oak- land, CA, 2007.
[9] K. Barlow and J. Lane, "Like technology from an advanced alien cul ture: Google apps for education at ASU," in Proc. ACM SIGUCCS User Services Conf., Orland, FL, 2007.
[10] S. Muller, S. Katzenbeisser, and C. Eckert. Distributed Attribute-Based Encryption. In Proceedings of ICISC 2008, pages 20-36.