International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 3 Issue 4, April - 2014

A Scalable and Efficient Access Control in Cloud with Multi-Authority Attribute Based Encryption

Deepthi R [1]
PG student, Dept of CSE,
CIT ,Gubbi ,
Karnataka, India

Prof. Shantala C. P [2]
HOD, Dept of CSE,
CIT ,Gubbi,
Karnataka, India

***Abstract*-Cloud computing is come out a new computing model in the recent years.The challenges faced by this model are security issues and accessing of data by the unauthorized authority.Several encryption schemes are proposed but they are suffer from implementing compound access control policies.In this document,we propose multi-authority attribute-set-based encryption by extending attribute encryption of ciphertext-policy .This scheme also address compound value assignments and support compound attributes.**

key Terms- Fine grained access control, cloud computing, data security,compound attribute.

I. INTRODUCTION

Cloud computing is come out a new computing model in the recent years. The challenges faced by this model are security issues and accessing of data by the unauthorized authority.The service models are Infrastructure as a Service (IaaS) - IaaS support hardware and network components, Platform as a Service (PaaS)- PaaS support different operating systems and Software as a Service (SaaS)-it provides services to customers over the internet.Various commercial cloud computing systems are existing, e.g., Amazon's EC2 [1] of IaaS systems, Google App Engine [2] of PaaS systems and Google's Apps of SaaS systems.Deployment models have been proposed, including Public cloud-it impose no restrictions on any customers for using of services,Private cloud-it supports exclusively for a particular organization, Hybrid cloud- it is the combination of private and public cloud services.

Security trouble in cloud computing become serious problem. One of the important issue consider for the model of cloud is confidentiality and data security,since the model is based on Internet storage. In our application, users store the data into the cloud for storage but totally we cannot trust the cloud due the property of data leakage. The main asset for any group is data so if it is disclosed to any unauthorized person then it turn to a serious consequences. Therefore, cloud users must be aware about their data to be secure and not to disclosed with the outsiders. We cannot considered the data confidentiality be the main core of this model,together also take into consideration of fine-grained access control.In order to accomplish the issue of right to access, a different kinds of approaches are proposed. A recent proposed scheme is attributed-based encryption,it categories into 2 types:one is key-policy attribute-based encryption for the property of fine-grained access control. But, this scheme is unable to overcome the problem of management of attributes and lacks scalability in multiple-levels of attribute authorities.So to overcome the problem of key-policy attribute-based encryption,another type is proposed i.e ciphertext-policy attribute-based encryption, it suited best for the property of access control because it is very appropriate in describing access control policies.

In this work, we considered a multi-authority attribute-set-based encryption scheme for the model of cloud computing,it accomplishes the property of scalablity and access control and also it ellaborate the scheme of ciphertext-policy attribute- set-based encryption [5] with a hierarchical structure of system users.

The significant aid of our contribution are as follows. 1) It achieves fine-grainedness, scalability and data privacy for data access control in cloud computing; 2) It shows the extension of attribute set based encryption; 3) It supports compound attributes and multiple value assignments efficiently .

The document is planned as follows. Section II discusses related work. Section III presents system model. Section IV presents construction. We conclude this paper in Section V.

II. RELATED WORK

Encryption based on attribute(EBA), in this scheme, encryption is not dedicated for a single user compare to conventional public key cryptography. Rather, both ciphertexts and user's keys are linked with attribute set or a policy, if there is a match between decryption key and the ciphertext only then the decryption of the ciphertext is taken place.EBA schemes consists of two forms, namely,Attribute encryption of Key-Policy schemes and Attribute encryption of Ciphertext-Policy schemes. In KP-ABE[3], policies are associated with keys and ciphertext is with attributes. Only those keys associated with a policy that is satisfied by the attributes,are possible to decrypt the ciphertext.

In CP-ABE[4], policies are coupled with ciphertext and keys are with attributes.Decryption takes place only if user attributes are made to pass through the ciphertext's access structure . Attribute encryption of Ciphertext-Policy approaches are still far from reaching the needs of modern enterprise environments.First, it is tedious to capture "compound attributes", i.e., attributes build from other

attributes, and specifying policies using those attributes. Second, attribute encryption of Ciphertext-Policy support numerical attributes are limited to assigning only one value to any given numerical attribute within a key.However we can solve the problem by specifying ciphertext policy-attribute set based encryption,it can support compound attributes by flexibly combining different singleton attributes to form a meaningful policy and also multiple numerical assignments for a specified attribute.

III. SYSTEM MODEL

A model consists of a cloud, vendor, customers, a number of field authorities, and a trusted authority.Here trusted authority is considered to be the root and responsible for managing the field authority, field authority in turn manage the vendor and customer. The cloud maintains the data storage service. Encryption of data files is done by data vendor and upload the data file into the cloud ,encrypted data files of their interest are download by the customers from the cloud and then decrypt them. Parent trusted authority is managed the field authority. Customers, vendor, field authorities, and the trusted authority are structured in a hierarchical way are shown in Fig. 1.

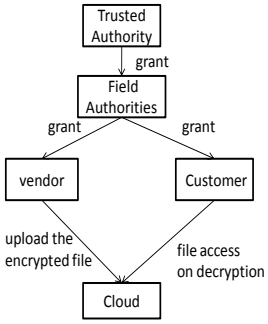

Fig1:system model

File Creation: Before loading data files to the cloud, a data file is encrypted by the vendor using a symmetric data encryption key.
File Access:When a user wants to access the data files on the cloud then it first sends the request to the cloud,the cloud sends the corresponding ciphertext to the user.The user decrypt data files using data encryption key.
File Deletion: Encrypted form of data files can be deleted by the vendor, only on the request of the respected vendor.In order to delete an encrypted data file, the vendor sends the file's unique ID to the cloud. On successful verification of the vendor and the request, the data file is deleted by the cloud.
User Revocation:In cloud computing,user revocation can be handled by using multiple value assignments.So we can update user's key by simply adding new value to the existing key.

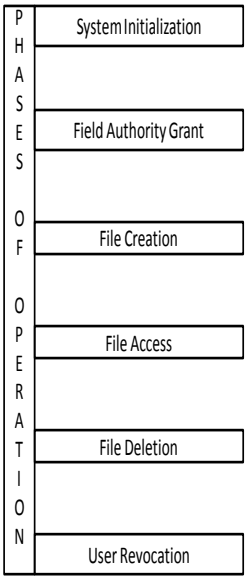

Fig 2:phases of operation

IV. CONSTRUCTION

Multi-authority attribute based encryption scheme handle the users in a hierarchical fashion.The significant operations of hierarchical attribute set based encryption[6]: System Initialization, Field Authority Grant, File Creation, File Access, File Deletion and User Revocation as shown in Fig 2.
System Initialization:Initialization of public key and master key to trusted authority.
Field Authority Grant:If field authority wants to unite with the system, the trusted authority will first verify whether it is a valid field authority. If so,then the trusted authority issues the master key to respected field authority.

V. CONCLUSION

In this work,we created a system for multi-authority attribute based encryption, that organizes user attributes into a recursive family of sets and allows users to impose constraints on how attributes may be combined. We showed how this scheme can naturally support user revocation, compound attributes, and multiple value assignments.Also accomplishing scalablity and provide the authorization for accessing of data in cloud service model.

REFERENCES

1. Available: http://aws.amazon.com/ec2/,
Amazon Elastic Compute Cloud (Amazon EC2) [Online].
2. Available:http://code.google.com/appengine/ ,Google App Engine [Online].
3. "Attibute-based encryption for fine-grained access control of encrypted data," V. Goyal, O. Pandey, A. Sahai, and B.Waters, in Proc. ACM Conf. Computer and Communications Security *(ACM CCS)*, Alexandria, VA, 2006.
4. "Ciphertext-policy attribute based encryption," , J. Bethencourt, A. Sahai, and B. Waters, 2007.
5. "Attribute-sets: A practically motivated enhancement to attribute-based encryption," in Proc. *ESORICS*, Saint Malo, France, 2009, R. Bobba, H. Khurana, and M. Prabhakaran.
6. "HASBE: A Hierarchical Attribute-Based Solution for Flexible and Scalable Access Control in Cloud Computing", Zhiguo Wan, Jun'e Liu, and Robert H. Deng.