File Sharing Application Using HASBE Scheme

Poonam Joshi,Yash Shah,Harsh Sanghani,Sharvari Vartak

***Abstract*— At present cloud computing is going to be very famous technology in IT enterprises. For a company, the data stored is huge and it is very precious. All functions are performed through networks. Thus, it becomes very important to have the secured use of data. In cloud computing, the ultimate important concerns of security are data security and confidentiality, and also flexible and scalable, fine grained access control must be keep in the cloud systems. Attribute based encryption (ABE), allows for rare access control on encrypted data. In its key policy extract, the primitive enables senders to encrypt messages under a set of attributes and private keys are associated with access structures that specify which cipher texts the key holder will be allowed to decrypt .we propose the Hierarchical Attribute Set Based Encryption (HASBE) to develop a new security feature for various organizational platforms. It is implemented using cipher text policy by encrypting and decrypting the data in the cloud so that the cloud system becomes more scalable and flexible by enforcing data owners to share their data with data consumers controlled by the domain authority.**

***Index Terms*— Access control, cloud computing, data security**

I. INTRODUCTION

A. Aims and Objectives

File Sharing is a new paradigm that builds a virtualization, parallel and distributed computing, utility computing and service oriented architecture. Now days File Sharing is emerged service, the File Sharing providing lot of benefits include the cost and capital expenditures, increased operational efficiencies, scalability and flexibility so on. Differ from the File Sharing provide the service oriented services such as Infrastructure as a service (IaaS), Platform as a service (PaaS) and Software as a Service (SaaS). Based on this services IT industry will get fine state on the hardware/software maintenances should be very easy to state. They save the cost on the Infrastructure and human resources.

Although the great benefits brought by File Sharing paradigm are exciting for IT companies, academic researchers, and potential server users, security problems in File Sharing become serious obstacles which, without being appropriately addressed, will prevent File Sharing extensive applications and usage in the future. One of the prominent security concerns is data security and privacy in File Sharing due to its Internet- based data storage and management.The benefits of File Sharing will get lot of works from those work we considered a major problem is the security for the server data from users access limits and authorization service. The major constriction of our work will provide securable and with specific access control along with authentication and maintain the data security. To provide the data security there several works available, those works will be majorly on attribute based encryption and access control solutions. Here we propose the **Tree Based Attribute Set Based Encryption (TB-ASBE)**. The TB-ASBE will prove high scalable, flexible and fine grade in access control.

Manuscript received January 19, 2015.

Poonam Joshi,Professor at department of I.T.,Atharva College Of Engineering, Mumbai, India.

Yash Shah, department of I.T.,Atharva College Of Engineering, Mumbai, India.

Harsh Sanghani, department of I.T.,Atharva College Of Engineering, Mumbai, India.

Sharvari Vartak, department of I.T.,Atharva College Of Engineering, Mumbai, India.

B. Problem Statement

In past years data sharing was done via a floppy or a disk drive which lack security .To over come this problem ,sharing of data over the network has become an prominent way of file sharing. In this application we propose hierarchical based network for data sharing along with encryption/decryption techniques. The application consists of three hierarchical levels .

Level:1-Highest priority , Level:2-Moderate priority & Level:3-Lowest priority(*Levels indicate both priority and authority*)*

C. Scope

A college based application
Level:1-HOD , Level:2-Professor & Level:3-Student
Here HOD has the access, read, write, manipulation, deletion permissions of all the profiles of professors as well as students.(level 1,level2,level3)
Professor has the same permissions restricted to their own profile along with their student's profile. (level2, level3)
Student have the same permissions restricted to their own profile.(level 3)
The Files shared are stored in a Database located in the admin PC which can be directly controlled by the administrator. .
The proposed scheme not only achieves scalability due to its hierarchical structure, but also inherits flexibility and fine-grained access control.

II. LITERATURE SURVEY

Attribute based encryption (ABE):- Sahai and Waters first introduced the attribute based encryption (ABE) for enforced access control through public key cryptography. The main goal for these models is to provide security and access control. The main aspects are to provide flexibility, scalability and fine grained access control. In classical model, and this can be achieved only when user and server are in a trusted domain. But what if their domains are not trusted or not same? So, the new access control scheme that is 'Attribute Based Encryption (ABE)' scheme was introduced which consist of key policy attribute based encryption (KP-ABE). As compared with classical model, KP-ABE provided fine grained access control. However it fails with

respect to flexibility and scalability when authorities at multiple levels are considered. In ABE scheme both the user secret key and the cipher text are associated with a set of attributes. The cipher text can be decrypted by a user only if overlap occurs in a threshold number of attributes between the cipher text and user secret key. ABE is implemented for one-to many encryption in which cipher-texts are not necessarily encrypted to one particular user, it may be for more than one number of users. Attribute-Based Encryption (ABE) in which policies are specified and enforced in the encryption algorithm itself. The existing ABE schemes are of two types. They are Key-Policy ABE (KP-ABE) scheme and Cipher text-Policy ABE (CPABE) scheme. That can be discussed further

A. .iphertext-policyattribute-based encryption(CP-ABE):

CP-ABE (cipher text-policy attribute-based encryption) is used to encrypt the data which can be kept confidential even if the storage server is untrusted. An arbitrary number of attributes expressed as strings a primary key is associated. On the other hand, when a party encrypts a message in this system, they specify an associated access structure over attributes. If the user's attributes pass through the cipher text's access structure then only user can be able to decrypt a cipher text. Access structures in this system are described by a monotonic "access tree", can be described at mathematical level. Where nodes of the access structure are composed of threshold gates and the leaves describe attributes .We note that AND gates can be constructed as n-of-n threshold gates and OR gates as 1-of-n threshold gates. Furthermore, we can manage
more complex access controls such as numeric ranges by converting them to small access trees.

B. Key-policy attribute-based encryption:

Setup: This algorithm takes as input a security parameter κ and returns the public key PK and a system master secret key MK. For encryption message senders uses the PK. User secret keys generated by using MK and is known only to the authority.

Encryption: This algorithm takes as input a message M, the public key PK, and a set of attributes .It outputs the cipher text E.

Key Generation: This algorithm takes access structure T and the master secret key MK as input. To enable the user to decrypt a message encrypted under a set of attributes if and only if matches, the algorithm outputs SK secret key T.

Decryption: User's secret key SK for access structure T and the cipher text E is taken as input, which was encrypted under the attribute set .If and only if the attribute set satisfies the user's access structure T, this algorithm outputs M

C. Identity Based Encryption (IBE):

In an identity-based encryption scheme, an arbitrary key is used as the key for data encryption and for decryption, a key is mapped by a key authority.

D. Hierarchical Identity Based Encryption (HIBE):

HIBEis the hierarchical form of a single IBE. The concept of HIBE scheme help to explain security. In a regular IBE (1-HIBE) scheme; there is only one private key generator (PKG) that distributes private keys to each users, having public keys are their primitive ID (PID) arbitrary strings. A two-level HIBE (2-HIBE) scheme consists of a rootPKG, domain PKGs and users, all of which are associated with PID's. A user's public key consists of their PID and their domain's PID (in combine, called an address). In a 2-HIBE, users retrieve their private key from their domain PKG. Private key PK of any user in their domain can be computed by Domain PKGs, provided they have previously requested their domain secret key-SK from the root PKG. Similarly, is for number of sub-domains. There also includes a trusted third party or root certificate authority that allows a hierarchy of certificate authorities: Root certificate authority issues certificates for other authorities or users in their respective domains.

The original system does not allow for such structure. However, a hierarchy of PKGs is reduces the workload on root server and allows key assignment at several levels. In this paper, we are going to implement scheme for access control in cloud computing using HIERARCHICAL ATTRIBUTE SET BASED ENCRYPTION (HASBE).HASBE extends the cipher text-policy attribute-set-based encryption (CP-ASBE, or ASBE for short) scheme proposed by Bobba et al. with system users having hierarchical structure, to achieve flexible, scalable, and access control.

III. PROPOSED SYSTEM

The paper contributes in multiform. Initially ,we show how ASBE algorithm is been enhanced by HASBE with a hierarchical structure with the better features like flexibility ,scalability and the common feature of fine grained access control of ASBE.

Secondly, we demonstrate how to implement a full-fledged access control scheme for cloud computing based on HASBE.

The scheme provides support for file creation, file deletion, hierarchical user grant, and user revocation in cloud computing.

Thirdly, we prove the security of the proposed scheme based on the security of the CP-ABE scheme by Bethen court et al. and analyse its performance in terms of computational overhead. Lastly, we implement HASBE and conduct experiments for performance evaluation, and experiments demonstrate that HASBE has satisfactory performance.

Hierarchical attribute-based encryption (HABE) is proposed by Wang et al. to achieve fine-grained access control in cloud storage services by combining hierarchical identity-based encryption (HIBE) and CP-ABE. This HABE scheme also supports fine-grained access control and fully delegating computation to the cloud providers. HABE uses disjunctive normal form policy and assumes all attributes in one conjunctive clause are administrated by the same domain master. Thus same attribute may be administrated by multiple domain masters according to particular specific policies. Furthermore, if we compare with ASBE, this scheme cannot support multiple value
assignments. And also does not support compound attributes

efficiently

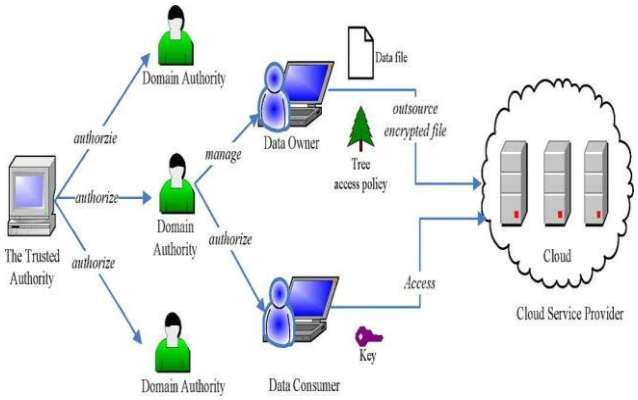

Fig. 1. System model

A. Domain authority check and attribute based encryption:

The cloud service provider manages a cloud to provide data storage service.. For sharing with data consumers, data owners encrypt their data files and store them in cloud.Data consumers download encrypted data files of their interest from the cloud and then decrypt them to access the shared data files. Each data owner/consumer is administrated by a domain authority. Parent domain authority manages domain authority. For managing the domain authorities at the next level or the data owners/consumers in its domain, responsible to each domain authority.

B. Shared resources and trusted authority:

The top level domain authorities are authorised by the trusted authority which acts as a root of trust. Subordinate domain authorities or users are administered and trusted by the domain authority. But the Domain Authority may sometimes try to get the private key of subordinate domain authorities or users outside its domain. Similarly users may try to access data files either within or outside the scope of their access privileges, so mallicious users may collude with each other to get sensitive files beyond their privileges. The trusted domain authority is responsible for generating and distributing system parameters and root master keys as well as authorizing the top-level domain authorities. A domain authority is responsible for transferring keys to subordinate domain authorities at the next level or users in its domain. A key is assigned to each user in the system which specifies the associated attributes for the decryption of users.

IV. CONCLUSION

In this paper, we introduced the HASBE scheme for the purpose of experiencing scalable, flexible, and fine-grained access control in cloud computing. The HASBE scheme incorporates a hierarchical structure of system users by applying a delegation algorithm to ASBE. HASBE supports compound attributes due to flexible attribute set combinations, and also achieves efficient user revocation because of multiple value assignments of attributes. Finally, the proposed scheme, is implemented and conducted comprehensive performance analysis and evaluation, which showed its advantages and efficiency over existing schemes**.**

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

[2]B. Barbara, “Salesforce.com: Raising the level of networking,” Inf. Today, vol. 27, pp. 45–45, 2010.

[3]T. Yu and M. Winslett, “A unified scheme for resource protection in automated trust negotiation,” in *Proc. IEEE* Symp. Security and Privacy, Berkeley, CA, 2003.

[4]J. Li, N. Li, and W. H. Winsborough, “Automated trust negotiation using cryptographic credentials,” in Proc. ACMConf. Computer and Communications Security (CCS), Alexandria, VA, 2005

[5]A. Ross, “Technical perspective: A chilly sense of security,” Commun. ACM, vol. 52, pp. 90–90, 2009.

[6]D. E. Bell and L. J. LaPadula, Secure Computer Systems: Unified Exposition and Multics Interpretation The MITRE Corporation, Tech. Rep., 1976.

[7]K. J. Biba, Integrity Considerations for Secure Computer Systems The MITRE Corporation, Tech. Rep., 1977.

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

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

[10] A. Sahai and B. Waters, “Fuzzy identity based encryption,” in Proc.Acvancesin Cryptology—Eurocrypt, 2005, vol. 3494, LNCS, pp. 457–473.

[11] G.Wang, Q. Liu, and J.Wu, “Hierachical attibute-based encryption for fine-grained access control in cloud storage services,” in Proc. ACMConf. Computer and Communications Security(ACM CCS), Chicago,

[12]T. Yu and M. Winslett, “A unified scheme for resource protection in automated trust negotiation,” in *Proc.* IEEE Symp. Security and Privacy, Berkeley, CA, 2003.Conf.Computer and Communications Security (ACMCCS), Alexandria,

[13] Zhiguo Wan, Jun’e Liu, and Robert H. Deng, “HASBE: A Hierearchical Attribute-Based Solution for Flexible and Scalable Access Control in Cloud Computing