HASBE: A Hierarchical Attribute Set Based Encryption for Flexible, Scalable and Fine Grained Access Control in Cloud Computing

N.krishna, L.Bhavani
Asst. Professor, Dept. of C.S.E,
Sri Sivani College of Engineering, Chilakapalem, A.P., India

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.*

Keywords - *Access control, cloud computing, data security*

1. INTRODUCTION

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 [1]. 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. Exclusive for small and medium-sized enterprises with limited budget, they can achieve cost savings and productivity enhancements In general data owners and service providers are not in the same trusted domain in cloud computing. Service providers should not be a trusted one anyhow they are all third party. Before uploading the data to cloud, data must be encrypted now confidentiality of stored data more protective. Different service-oriented cloud computing models have been designed, Platform as a Service (PaaS), including Infrastructure as a Service (IaaS), and Software as a Service (SaaS). At different levels, frequent commercial cloud computing systems had builted, e.g., Google App Engine and Yahoo Pig are representative PaaS systems, whereas Amazon's EC2 [2], Amazon's S3[3], and IBM's Blue Cloud[4] are IaaS systems[5], and Google's Apps[6] and Sales force's Customer Relation Management (CRM) System[7] be owned by SaaS systems .Sahai and Wa-ters proposed an attribute-based encryption (ABE) scheme in 2005.TheABE scheme used an user's identity as attributes, and a set of attributes were used to encrypt and decrypt data. The ABE scheme can result the problem that data owner needs to use every authorized user's public key to encrypt data. In 2006, Goyal et al [8]. Proposed a key-policy attribute-based encryption (KP-ABE) scheme [16]. The KP-ABE scheme can achieve fine-grained access control and more flexibility to control users than ABE scheme. But the disadvantage of KP-ABE is that the access policy is built into an user's private key, so data owner can't choose who can decrypt the data except choosing a set of attributes which can describe this data[12]-[15]. And it is unsuitable in certain application because a data owner has to trust the key issuer. Besides, the access structure in KP-ABE is a monotonic access structure, it can't express the negative attribute to exclude the parties with whom data owner didn't want to share data from memberships. However, this scheme drops short of flexibility [9]-[11] in attribute management and lacks scalability in dealing with multiple-levels of attribute authorities. Bethencourt et al. proposed a cipher text-policy attribute based (CP-ABE) scheme [14] in the same year, and the CP-ABE scheme built the access policy into the encrypted data; a set of attributes is in an user's key. The CP-ABE scheme addresses the problem of KP-ABE that data owner only trusts the key issuer. After that, several schemes were proposed based on the CP-ABE scheme we note that in contrast to KP-ABE, cipher text-policy ABE (CP-ABE) [18] turns out to be well suited for access control due to its expressiveness in describing access control policies. Wang et al. proposed a hierarchical attribute-based encryption scheme (HABE) in 2010 and 2011. This scheme uses the disjunctive normal

form policy and generates the keys hierarchically. And this scheme assumed that all attributes in one conjunctive clause are administered by the same domain authority. In addition to this, there are multi authorities ABE schemes that use multiple parties to distribute attributes for users.

1.1The Criteria of an Hierarchical Attribute based Encryption Scheme:

Data confidentiality: Before uploading data to the cloud, the data was encrypted by the data owner. Therefore, unauthorized parties including the cloud cannot know the information about the encrypted data. **Fine-grained access control**: In the same group, the system provides the different access right to individual user. The users are on the same group, but each user can be granted the different access right to access data. Even if users in the same group, users access rights are not the same. **Scalability**: When the authorized users increase, the system can work efficiently. So the number of authorized users cannot affect the performance of the system. **Flexibility**: Flexibility of the cloud allows companies to adjust to any problems that may occur during day-to-day operations. It also allows to use extra resources at peak times, to satisfy consumer demands.

2. LITERATURE SURVEY

Attribute based encryption (ABE):- Sahai and Waters first introduced the attribute based encryption (ABE) [13] 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)' [13] scheme was introduced which consist of key policy attribute based encryption (KP-ABE) [13]. 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) [13] scheme and Cipher text-Policy ABE (CPABE) [15] scheme. That can be discussed further

2.1Ciphertext-policy attribute-based encryption:

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.

2.2Key-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

2.3Identity 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.

2.4Hierarchical 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[9]. with system users having hierarchical structure, to achieve flexible, scalable, and fine grained access control.

3. 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 [15]. 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

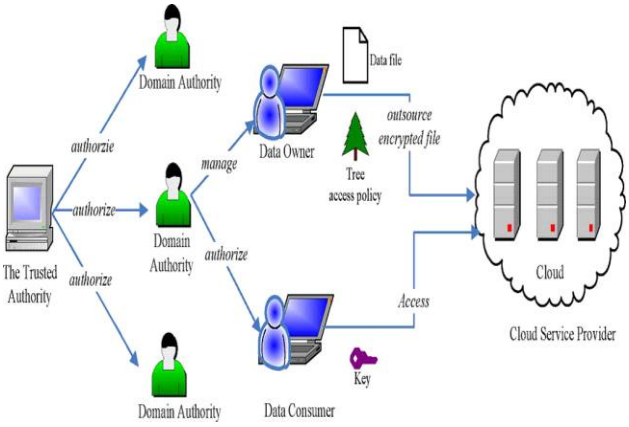

Fig. 1. System model

3.1Domain 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. A domain authority is managed by its parent domain authority. Each domain authority is responsible for managing the domain authorities at the next level or the data owners/consumers in its domain.

3.2Shared 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 malicious 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.

4. 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.

[13] J. Li, N. Li, and W. H. Winsborough, "Automated trust negotiation using cryptographic credentials," in Proc. ACM Conf. Computer andCommunications Security (CCS),Alexandria, VA, *2005.*

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

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