www.ijecs.in

International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 4 Issue 4 April 2015, Page No. 11609-11611

Achieving Multi Layered security, Flexibility, Scalability, Access Control in Cloud Computing Using Hierarchical Attribute Set Based Encryption (HASBE)

Priyanka Madhirjau
Assistant Professor: Dept. of CSE,
Jagruti Institute of Engineering and Technology
Chintapalliguda(V),Ibrahimpatnam(M), Ranga Reddy(Dist.),
Telangana, India
madhirajupriyanka@gmail.com

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. Cloud Computing, an emerging computing paradigm, requires additional security which is provided using HASBE and this can emerge as a new security feature for various organizational platforms. We propose attribute based solution so that performance of cloud can be improved. It is implemented using cipher text policy (CP-ABE) by encrypting and decrypting the data in the cloud and makes the data password protected so that the cloud system achieves scalability, flexibility and multi layered security by implementing data owners to share their data with data consumers controlled by the domain authority.***

Keywords - cloud computing, multi layered security, Flexibility, Scalability, Access Control

I.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. 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)..Sahai and Wa-ters proposed an attribute-based encryption (ABE) scheme in 2005.The ABE 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. proposed an keypolicy attribute-based encryption (KP-ABE) scheme. The KP-ABE scheme can achieve finegrained 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. 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 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 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. Cipher text-policy ASBE (CP-ABE) 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 ASBE schemes that use multiple parties to distribute attributes for users.

1.1 The Criteria of an Hierarchical Attribute based Encryption Scheme:

1.1.1 Multi Layered Security: 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. After downloading the file should be decrypted and also the data consumer should know the password to open the file.

1.1.2 Scalability: When the authorized users increase, the system can work efficiently. So the number of authorized users cannot affect the performance of the system.

1.1.3 Flexibility: Flexibility of the cloud allows companies to adjust to any problems that may occur during day-to-day operations. It also allows using extra resources at peak times, to satisfy consumer demands.

II. RELATED WORK

2.1 Cipher text-policy attribute-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.

2.2. Kp-Abe Policy:

We utilize KP-ABE to escort data encryption keys Files. Such construction helps us to immediately enjoy fine grained of access control. CP-ABE scheme, decryption keys only support user attributes that are organized logically as a single set, so users can only use all possible combinations of attributes in a single set issued in their keys

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 are 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

III. PROPOSED SYSTEM

The paper contributes in multiple criterion.

Firstly, 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 Security of ABE.

Secondly, we demonstrate how to implement a complete 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.

Fourthly, we demonstrate the type of file the data owner is uploading in to cloud and whether it is password protected or not that proves the security concept.

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

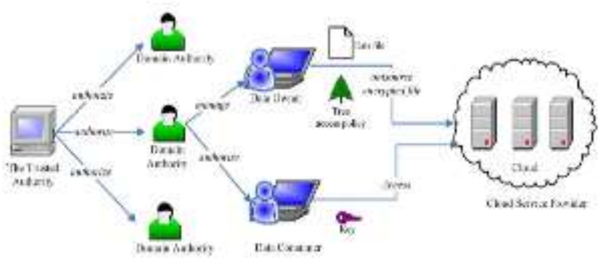

Figure 1.System Model

3.1 Domain Authority check

The cloud service provider manages a cloud to provide data storage service. Data owners will encrypt their data and store them in cloud. The data consumers download the required files from the cloud and decryt them with the help of key. The data owner/consumer is managed 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 parent Domain authority is taken care by a trusted authority which acts as a root of trust. The subordinate domain authorities or users work under the parent domain authority. Domain authority may some times try to get a private key of data of the subordianate domain authorities or users outside the domain.and the outside users also try to access the data within or outside the scope of their access previliges, so malicious users may collide with other. The trusted domain authority is responsible for generating and distributing thr system parametes and root master kay as well as authorizing the top level domain authorities.A Domain authority is responsible for generating and distributing master keys and for transferring keys to subordianate domain authorities of next level.

IV. IMPLEMENTATION

The aim of this paper is to add another layer of security by making the file password protected. If the data consumer want to download a file from the cloud he should know the master key for decryption and also he should know the password. The password will be a one time password which will be sent to his registered email and that will be valid only for that session.

V. CONCLUSION

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. HASBE based on the security of CP-ABE and implemented the scheme, and conducted comprehensive performance analysis and evaluation. Finally, the proposed scheme, is evaluated by making the uploaded files password protected by the data owners after decryption so that high the files in cloud will be highly secured , which showed its advantages and efficiency over existing schemes.

VI.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 attibutebased 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]*Google App Engine [Online]. Available: http://code.google.com/appengine/

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

VII. ACKNOWLEDGEMENT

The Authors sincerely thank the chairman of Jagruti Institute of Engineering and Technology , Dr. V.Surender Rao, Director for their encouragement to prepare this review. They further extends sincere thanks to Principal and Head of the Department of Information Technology of Jagruti Institute of Engineering and Technology for their constant support at every stage to complete this review.

VII. AUTHORS PROFILE

Priyanka Madhiraju received her B.Tech from Sindura college of engineering and technology in 2007 and M.Tech from Jagruti institute of Engineering and Technology in 2013. She is currently working as an Assistant Professor in CSE Department for Jagruti Institute of Engineering and Technology.