Scalable Access Control in Cloud Computing using Hierarchical Attribute Set Based Encryption (HASBE)

A. Vishnukumar, G. Muruga Boopathi, S. Sabareessh

***Abstract-** 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 organisational platforms. We propose attribute based solution so that performance of cloud can be improved. 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:** Cloud Computing, Access Control, Data Security, Key Generation*

I. INTRODUCTION

On the need of sharing confidential corporate data on cloud servers, it is imperative to adopt an efficient encryption scheme with a fine-grained access control to encrypt outsourced data. Hierarchical Attribute

Based Encryption, as one of the most promising encryption systems in this field, allows the encryption of data by specifying an access control policy over attributes, so that only users with a set of attributes satisfying this policy can decrypt the corresponding data. The hierarchical Attribute Set-Based Encryption (HASBE) scheme is for accessing control in cloud computing and extended the cipher text policy attribute set based encryption. Hierarchical Attribute Based Encryption security for data's based on public key and master key with the help of Domain Authority Check.

II. RELATED WORK

A. Cipher-Text Policy

The trusted authority calls the algorithm to create system public parameters and master key. Public parameters will be made public to other parties and Master Key will be kept secret. The attributes asso- ciated with the ciphertext satisfy the tree access structure, can the user decrypt the ciphertext.

B. Kp-Abe Policy:

We utilize KP-ABE to escort data encryption keys of data Files. Such construction helps us to immediately enjoy fine-grandness 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 to satisfy policies

$a \equiv g^k$ (mod p); gcd(k, p-1) = 1; else $a \equiv 1$?

Message M (digraph, trigraph blocks)

Public key (g, p, $y \equiv g^x$ (mod p))

$M \equiv (xa + kb) \bmod (p-1)$

where $\quad x$ *= private key*

k *= random secret value*

Digital Signature (a,b) sent with M

$y^a a^b \equiv g^M \pmod p$

The Math :

$g^M \equiv g^{(xa+kb)} \bmod p$

$(g^x)^a (g^k)^b \equiv y^a a^b \pmod p$

If M was modified, congruence would be violated

III. IMPLEMENTATION

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, there are several drawbacks about this trivial solution. First of all, such a solution requires an efficient key management mechanism to distribute decryption keys to authorized users, which has been proven to be very difficult. Next, this approach lacks scalability and flexibility; as the number of authorized users becomes large, the solution will not be efficient anymore. 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. Last but not least, data owners need to be online all the time so as to encrypt or re-encrypt data and distribute keys to authorize users.

IV. CLOUD ARCHITECTURE DESIGN

Cloud computing has computational and sociological implications. In computational terms cloud computing is described as a subset of grid computing concerned with the use of special shared computing resources. For this reason it is described as a hybrid model exploiting computer networks resources, chiefly Internet, enhancing the features of the client/server scheme.

Manuscript received February, 2013.

A.Vishnukumar, Department of IT, VelTech High Tech Dr.Rangarajan Dr.Sakunthala Engineering College, Chennai, India.

Dr. G.Muruga Boopathi, Department of IT, VelTech Multi Tech Dr.Rangarajan Dr.Sakunthala Engineering College, Chennai, India.

S.Sabareessh, Department of IT, VelTech High Tech Dr.Rangarajan Dr.Sakunthala Engineering College, Chennai, India.

From a sociological standpoint on the other hand, by delocalizing hardware and software resources cloud computing changes the way the user works as he/she has to interact with the "clouds" on-line, instead of in the traditional stand-alone mode.

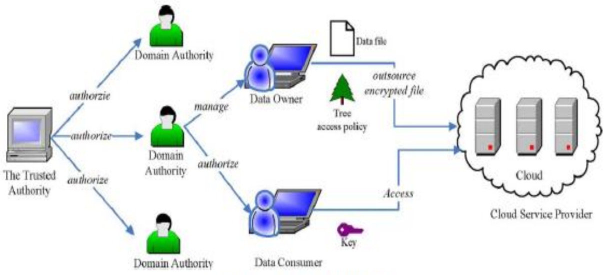

Fig. 1. System model.

V. DOMAIN AUTHORITY CHECK AND ATTRIBUTE BASED ENCRYPTION

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. To access the shared data files, data consumers download encrypted data files of their interest from the cloud and then decrypt them. 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.

V. SHARED RESOURCES AND TRUSTED AUTHORITY

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, so malicious users may collude with each other to get sensitive files beyond their privileges. The trusted 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 delegating keys to subordinate domain authorities at the next level or users in its domain. Each user in the system is assigned a key structure which specifies the attributes associated with the user's decryption key.

VI. 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.

ACKNOWLEDGEMENT

The Authors sincerely thank the chairman of VelTech Group of Institution Col. Prof. Dr. Vel Sri. R. Rangarajan, Chairperson and Managing Trustee, Director for their encouragement to prepare this review. They further extends sincere thanks to Principal and Head of the Department of Information Technology of Vel Tech Multi Tech Dr.Rangarajan Dr.Sakunthala Engineering College for their constant support at every stage to complete this review

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, pp. 599–616, 2009.
2. Amazon Elastic Compute Cloud (Amazon EC2) [Online]. Available: http://aws.amazon.com/ec2/
3. Amazon Web Services (AWS) [Online]. Available: https://s3.amazonaws.com/
4. R. Martin, "IBM brings cloud computing to earth with massive new data centers," Information Week Aug. 2008 [Online]. Available: http://www.informationweek.com/news/hardware/data_centers/209901523
5. Google App Engine [Online]. Available: http://code.google.com/appengine/
6. B. Barbara, "Salesforce.com: Raising the level of networking," Inf. Today, vol. 27, pp. 45–45, 2010.
7. 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.
8. J. Li, N. Li, and W. H. Winsborough, "Automated trust negotiation using cryptographic credentials," in Proc. ACM Conf. Computer and Communications Security (CCS), Alexandria, VA, 2005.
9. A. Ross, "Technical perspective: A chilly sense of security," Commun. ACM, vol. 52, pp. 90–90, 2009.
10. D. E. Bell and L. J. LaPadula, Secure Computer Systems: Unified Exposition and Multics Interpretation The MITRE Corporation, Tech. Rep., 1976.
11. K. J. Biba, Integrity Considerations for Secure Computer Systems The MITRE Corporation, Tech. Rep., 1977.
12. H. Harney, A. Colgrove, and P. D. McDaniel, "Principles of policy in secure groups," in Proc. NDSS, San Diego, CA, 2001.
13. P. D. McDaniel and A. Prakash, "Methods and limitations of security policy reconciliation," in Proc. IEEE Symp. Security and Privacy, Berkeley, CA, 2002.
14. 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.
15. J. Li, N. Li, and W. H. Winsborough, "Automated trust negotiation using cryptographic credentials," in Proc. ACM Conf. Computer and Communications Security (CCS), Alexandria, VA, 2005.
16. 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 (ACM CCS), Alexandria,
17. Zhiguo Wan, Jun'e Liu, and Robert H. Deng, "HASBE: A Hierearchical Attribute-Based Solution for Flexible and Scalable Access Control in Cloud Computing",

AUTHORS PROFILE

Mr. A. VishnuKumar, received her B.E., Degree from IFET college Engineering, which is affiliated to Anna University in 2007. he received his M.E., Degree from Govt. College of Engineering - Anna University in 2009. At present working as Assistant Professor in Vel Tech High Tech Dr. Rangarajan Dr. Sakunthala Engineering College, Chennai, Avadi from 2009 to tilldate. He registered his Ph.D. in Anna University, Tirunelveli, and his research work is progressively going on in the area of Cloud Computing.

Dr. G. Murugaboopathi received the Undergraduate Degree in Computer Science and Engineering from Madurai Kamaraj University, in 2000, the Post Graduate degree in Digital Communication and Network from Madurai Kamaraj University, in 2002 and Ph.D in Computer Science and Engineering at Bharath University, Chennai. He has more than 20 publications in National, International Conference and International Journal proceedings. He has more than 10 years of teaching experience. His areas of interest include Wireless Sensor Networks, Mobile Communication, Mobile Computing, Mobile Adhoc Networks, Computer Networks, Network Security, High Speed Networks, Network and Data Security, Cryptography and Network security, DBMS and etc., He is currently working as an Head R & D and Associate Professor in the Department of Information Technology at Vel Tech Multi Tech Dr.Rangarajan Dr.Sakunthala Engineering College Chennai India.

Mr. S.Sabareessh Studying a Bachelor of Engineering, in the department of IT at Veltech high tech Dr.Rangarajan Dr.Sakunthala Engineering college, Avadi, Chennai.