International Journal for Research in Engineering Application & Management (IJREAM)
ISSN : 2454-9150 Vol-03, Issue-09, Dec 2017

Taxonomy Attribute Set Based Authentication And Flexible Access Control For Cloud Storage

[1]Mr. Ravindra B. Pandit, [2]Prof. Ritesh Thakur
[1]PG Student, [2]Professor, [1,2]Dept. of Computer Engineering, Institute Of Knowledge College Of Engineering, Pimple Jagtap, Pune, Maharashtra, India
[1]*ravindrapandit.19@gmail.com*

Abstract: Cloud computing is known as "Utility". Cloud Computing enabling users to remotely store their data in a server and provide services on-demand. Since this new computing technology requires user to entrust their valuable data to cloud providers, there have been increasing security and privacy concerns on outsourced data. We can increase security on access of the data in the cloud. However there are security concerns on outsourced data as the cloud servers are treated as untrusted. To overcome this problem many Attribute Based Encryption (ABE) techniques came into existence for secure access control. These techniques suffer from problems in implementing flexible access control mechanisms. A hierarchical attribute based solution which provides fine grained access control besides making it scalable. In this paper we implement this security scheme and build a prototype application that demonstrates the proof of concept. The empirical results revealed encouraging results.

Keywords: Access control, cloud computing, data security.

I. INTRODUCTION

Cloud computing has emerged as one of the most influential paradigms in the IT industry inrecent years. Since this new computing technology requires users to entrust their valuable datato cloud providers, there have been increasing security and privacy concerns on outsourced data. Several schemes employing attribute-based encryption (ABE) have been proposed for access control of outsourced data in cloud computing; however, most of them suffer from inflexibility in implementing complex access control policies. In order to realize scalable, flexible, and fine-grained access control of outsourced data in cloud computing, in this paper, we propose hierarchical attribute-set-based encryption (HASBE) by extending cipher text policy attribute set- based encryption (ASBE) with a hierarchical structure of users. The proposed scheme not only achieves scalability due to its hierarchical structure, but also inherits flexibility and fine grained access control in supporting compound attributes of ASBE. Data confidentiality is not the only security requirement. Flexible and fine-grained access control is also strongly desired in the service-oriented cloud computing model. A health-care information system on a cloud is required to restrict access of protected medical records to eligible doctors and a customer relation management system running on a cloud may allow access of customer information to high-level executives of the company only. In these cases, access control of sensitive data is either required by legislation (e.g., HIPAA) or company regulations. Access control is a classic security topic which dates back to the 1960s or early 1970s [9], and various access control models have been proposed since then. Among them, Bell-La Padula (BLP) [10] and BiBa [11] are two famous security models. To achieve flexible and fine-grained access control, a numbers of schemes [12]–[15] have been proposed more recently. Unfortunately, these schemes are only applicable to systems in which data owners and the service providers are within the same trusted domain. Since data owners and service providers are usually not in the same trusted domain in cloud computing, a new access control scheme employing attributed-based encryption [16] is proposed by Yu et al. [17], which adopts the so-called key-policy attribute-based encryption (KP-ABE) to enforce fine-grained access control. However, this scheme falls short of flexibility in attribute management and lacks scalability in dealing with multiple-levels of attribute authorities. 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. In addition, HASBE employs multiple value assignments for access expiration time to deal with user revocation more efficiently than existing schemes. We formally prove the security of HASBE based on security of the cipher text-policy attribute-based encryption (CP-ABE) scheme by Bethencourt et al. and analyze its performance and computational complexity. We implement our scheme and show that it is both efficient and flexible in dealing with access control for outsourced data in cloud computing with comprehensive experiments.

 DOI : 10.18231/2454-9150.2017.0060

II. RELATED WORK

Cloud computing is the use of computing resources (hardware and software) that are delivered as a service over a network (typically the Internet). The name comes from the common use of a cloud shaped symbol as an abstraction for the complex infrastructure it contains in system diagrams. Cloud computing entrusts remote services with a user's data, software and computation. Cloud computing consists of hardware and software resources made available on the Internet as managed third-party services. These services typically provide access to advanced software applications and high-end networks of server computers. The goal of cloud computing is to apply traditional supercomputing, or high-performance computing power, normally used by military and research facilities, to perform tens of trillions of computations per second, in consumer-oriented applications such as financial portfolios, to deliver personalized information, to provide data storage or to power large, immersive computer games power large, immersive computer games. Cloud computing is recognized as an alternative to traditional information technology due to its intrinsic resource-sharing and low-maintenance characteristics. In cloud computing, the cloud service providers (CSPs), such as Amazon, are able to deliver various services to cloud users with the help of powerful datacenters. By migrating the local data management systems into cloud servers, users can enjoy high-quality services and save significant investments on their local infrastructures. However, the complexities of user participation and revocation in these schemes are linearly increasing with the number of data owners and the number of revoked users, respectively. By setting a group with a single attribute, Lu et al. Proposed a secure provenance scheme based on the cipher text-policy attribute-based encryption technique, which allows any member in a group to share data with others. However, the issue of user revocation is not addressed in their scheme. Yu et al. presented a scalable and fine-grained data access control scheme in cloud computing based on the key policy attribute-based encryption (KP-ABE) technique. Unfortunately, the single- owner manner hinders the adoption of their

III. PROPOSED SYSTEM

To achieve the reliable and scalable The objective of this work is to expand HASBE scheme is to realize scalable, supple, and fine grained access control in cloud computing. The HASBE method flawlessly integrates a hierarchical structure of scheme customers by concerning an allocation algorithm to ASBE. HASBE not only maintains compound attributes due to flexible attribute set combinations, but also attains efficient user revocation because of multiple value assignments of attributes. We properly proved the security of HASBE based on the security of CP ABE. To end with, we realized the suggested proposal, and accomplished complete performance analysis and evaluation, which demonstrated its effectiveness and benefits over obtainable schemes. The scope of the project is to build up a new computing technology necessitates users to hand over their precious data to cloud providers, thereby raising safety and confidentiality concerns on outsourced data. Several methods utilizing attribute based encryption (ABE) have been proposed for access control of outsourced data in cloud computing; though, most of them suffer from hardness in implementing complex access control policies. Even though the great profits brought by cloud. In this method we are further presenting how we are managing the risks like failure of group manager by increasing the number of backup group manager, hanging of group manager in case number of requests more by sharing the workload in multiple group managers. This method claims required efficiency, scalability and most importantly reliability.

To provide the best solutions for the problems imposed by existing methods, recently the new method was presented called [1]. This approach presents the design of secure data sharing scheme, , for dynamic groups in an untrusted cloud. In, a user is able to share data with others in the group without revealing identity privacy to the cloud. Additionally, it supports efficient user revocation and new user joining. More specially, efficient user revocation can be achieved through a public revocation list without updating the private keys of the remaining users, and new users can directly decrypt files stored in the cloud before their participation. Moreover, the storage overhead and the encryption computation cost are constant. Therefore practically in all cases outperforms the existing methods.

IV. RESULT AND ANALYSIS

Fig 2.Certificate Authority

In this user can generate ID and check valid user or not and send details to AA.

 DOI : 10.18231/2454-9150.2017.0060

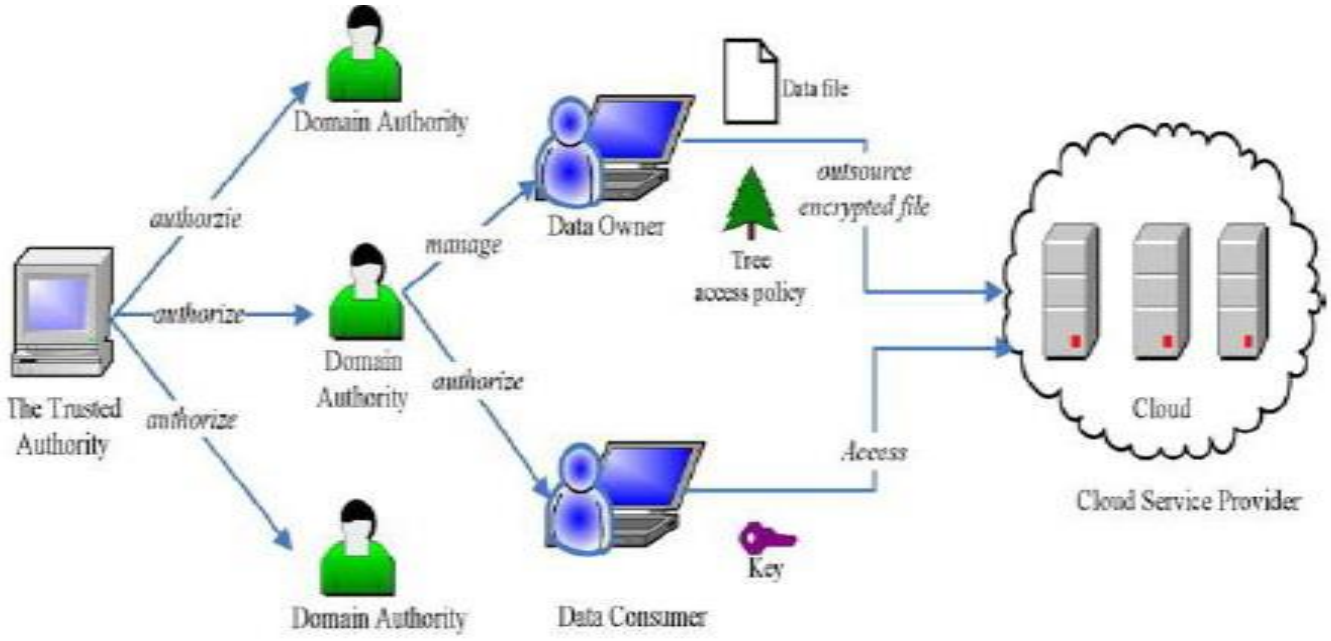

Fig. 1 System Diagram

In this figure client can set his attribute Revocation.

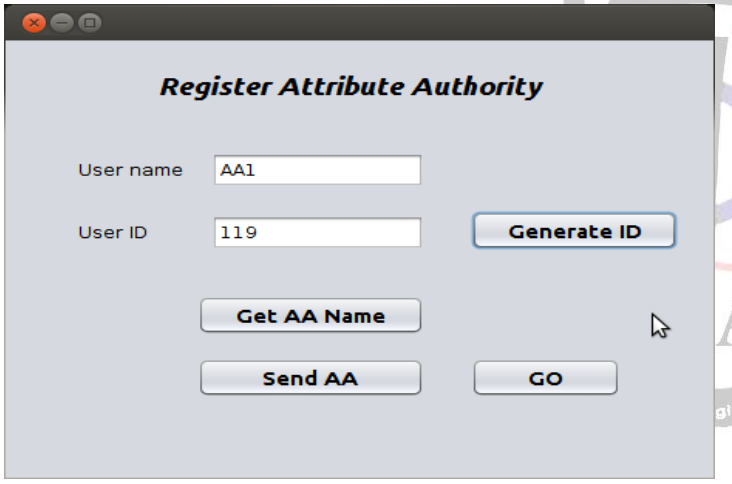

Fig 3.Register Attribute Authority

In this Register his ID and get AA Name and send to AA.

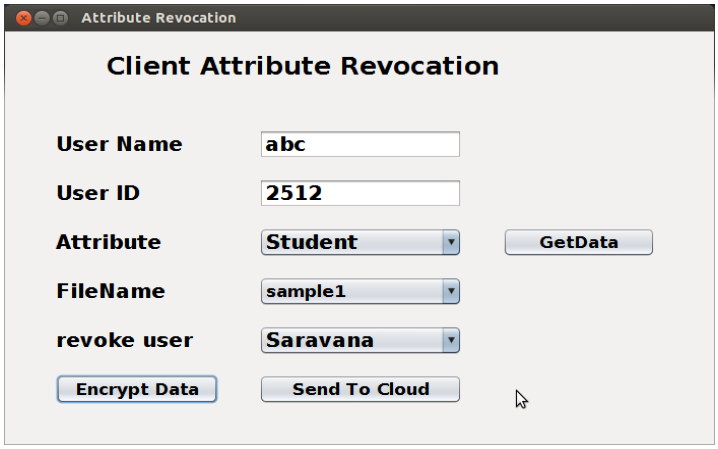

Fig 4.Client Attribute Revocation

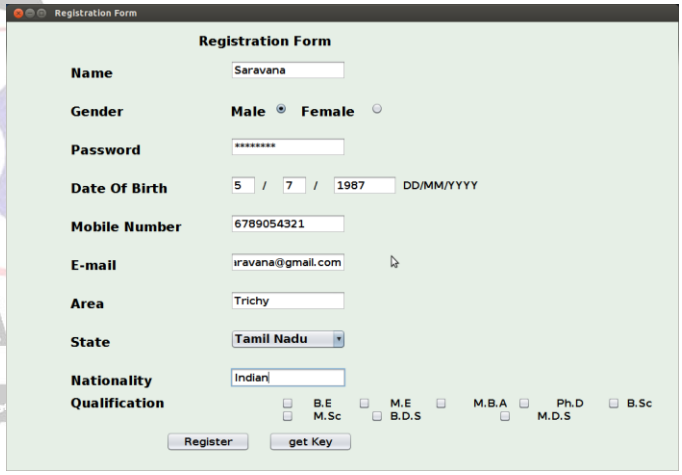

Fig 5.Client Registration

Here Client will Register all Field Name, Gender, DOB, Mobile, Email, State And Also Qualification.

V. CONCLUSION

A revocable multi-authority CP-ABE scheme can support efficient attribute revocation. Then, we constructed an effective data access control scheme for multi-authority cloud storage systems. The revocable multi-authority CP-ABE is a promising technique, which can be applied in any remote storage systems and online social networks etc. In conclusion, cloud computing is very attractive environment for business world in term of providing required services in a very cost effective way. However, assuring and enhancing security and privacy practices will attract more enterprises to world of the cloud computing In Thus to achieve the reliable and scalable

 DOI : 10.18231/2454-9150.2017.0060

In this paper, we introduced the HASBE scheme for realizing scalable, flexible, and fine-grained access control in cloud computing. 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. We formally proved the security of HASBE based on the security of CP-ABE by Bethencourt et al.. Finally, we implemented the proposed scheme, and conducted comprehensive performance analysis and evaluation, which showed its efficiency and advantages over existing schemes.

REFERENCES

[1] Xuefeng Liu, Yuqing Zhang, Boyang Wang, and Jingbo Yan, "Mona: Secure Multi-OwnerData Sharing for Dynamic Groups in the Cloud", IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 24, NO. 6, JUNE 2013 [1].

[2] Zhiguo Wan, Jun'e Liu, and Robert H. Deng, Senior Member, IEEE ," HASBE: A HierarchicalAttribute-Based Solution for Flexible and Scalable Access Control in Cloud Computing"in IEEE transection on information forensic and security ., vol. 7, no. 2, April 2012 [3].

[3] SanchalRamteke, Purvamodi, ApurvaRaghojiwar, VijayaKarad, Prof.P.D.Kale.,"HASBE:Hierarchical Attribute based solution for flexible and scalable access control in cloud computing-in International Journal of Scientific and Research Publications, Volume 4, Issue 1, January 2014 [4].

[4] Rajanikanthaluvalu,lakshmiMuddana," A Survey on Access Control Models in Cloud Computing"-in Springer International Publishing, Advances in Intelligent Systems and Computing 337

[5] Md.Akram Ali, Ch.Pravallika, P.V.S. Srinivas," Multi-Attribute Based Access Control PolicyEnforcement for File Accesses in Cloud"-in International Journal of Engineering Science andInnovative Technology (IJESIT) Volume 2, Issue 5, September 2013

[6] John Bethencourt, Computer Sciences Department Carnegie Mellon University," Intro toBilinear Maps"

[7] A. Sahai and B. Waters, "Fuzzy identity-based encryption," inProc.EUROCRYPT, 2005, pp.457473

[8]] V. Goyal, O. Pandey, A. Sahai, and B.Waters, "Attibute-based encryption for fine-grainedaccess control of encrypted data," in Proc. ACM Conf. Computer and CommunicationsSecurity (ACM CCS), Alexandria, VA, 2006.38

[9] S. Jaiswal and A. Nandi, J. Bettencourt, A. Sahai, and B.Waters"Ciphertext-policy attributebased encryption "in Proceedings of IEEE Symposium on Security and Privacy, pp. 321V334,2007.

[10] Vinayak D. Shinde, "Fear of Data Privacy and Security in Cloud Computing Technology", International Journal for Research in Engineering Application & Management (IJREAM), Vol- 01, Issue -09, Dec-15.

[11] S. Gokuldev, S.Leelavathi Associate Professor, PG Scholar Department of Computer Science and Engineering SNS College of Engineering, Coimbatore, India," HASBE: A Hierarchical Attribute-Based Solution for Flexible and Scalable Access Control by Separate Encryption/Decryption in Cloud Computing"-in International Journal of Engineering Science and Innovative Technology (IJESIT) Volume 2, Issue 3, May 2013

[12] B. Carbunar, R. Sion, R. Potharaju, and M. Ehsan, "The shy mayor: Private badges in geosocial networks," in Proc. 10th Int. Conf. ACNS, pp. 436–454, 2012.

[13] Zhibin Zhou and Dijiang Huang Arizona State University On Efficient Ciphertext-Policy Attribute Based Encryption and Broadcast Encryption.

[14] Minu George1, Dr. C.Suresh Gnanadhas2, Saranya.K3," A Survey on Attribute Based Encryption Scheme in Cloud Computing"-in International Journal of Advanced Research in

Computer and Communication Engineering Vol. 2, Issue 11, November 2013

[15] Mauro José A. de Melo, Zair Abdelouahab," A STUDY OF ACCESS CONTROL IN CLOUD COMPUTING ENVIRONMENT" in International Journal of Computers Technolog Volume 3 No. 3, Nov-Dec, 2012

[16] B. Raja Sekhar,B. Sunil Kumar, L. Swathi Reddy, V. PoornaChandar," CP-ABE Based Encryption for Secured Cloud Storage Access"-in International Journal of Scientific Engineering Research, Volume 3, Issue 9, September-2012

[17] N.krishna. L.Bhavani," HASBE: A Hierarchical Attribute Set Based Encryption For Flexible, Scalable And Fine Grained Access Control In Cloud Computing-International Journal of Computer Organization Trends –Volume 3 Issue 9 – Oct 2013.

 DOI : 10.18231/2454-9150.2017.0060