RESEARCH ARTICLE OPEN ACCESS

A Study on Recent Trends on Cloud Computing and Attribute-Based Datastorage Concepts

Dr. P. Julia Grace[1], Kousalya[2]
[1]*Assistant Professor & Research Supervisor Department of Computer Science JBAS College for Women, Chennai.*
[2]*M.Phil., Computer Science Scholar Mother Teresa Women's University Kodaikanal.*
Corresponding Author: Dr. P. Julia Grace

ABSTRACT
Due to the enormous development in cloud computing, outsourcing data to cloud server attracts lots of attentions. To guarantee better security, attribute based encryption (ABE) was proposed and used in cloud storage system already. In this paper, we have studied the recent trends in cloud computing and implemented the concepts - ciphertext-policy attribute based encryption (CP-ABE) scheme with efficient user revocation for cloud storage system.
Keywords: cloud computing, attribute based data storage, recent trends

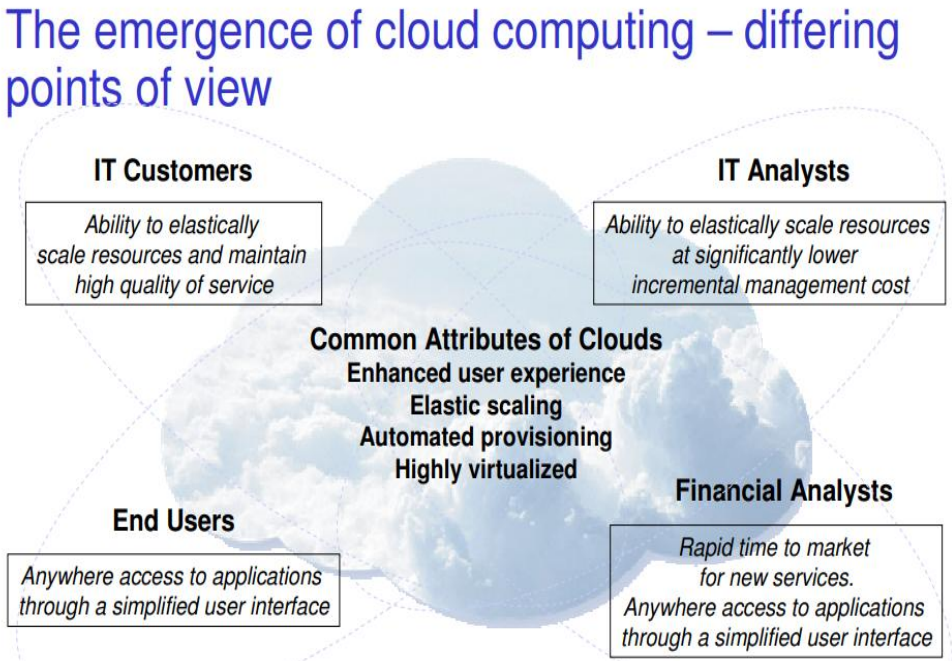
Date of Submission: 04-07-2017 Date of acceptance: 15-07-2017

I. CLOUD COMPUTING - INTRODUCTION

Cloud computing, a new type of internet based computing is regarded as a prospective computing paradigm in which resource issupplied as service over the Internet. It has met the increasing needs of computing resources and storage resources for someenterprises due to its advantages of economy, scalability, and accessibility. It is both a combination of software and hardware based computing services deliveredas a network service. The working models are deployment model and service model.

1.1 Recent trends

The cloud has already become global. Cloud services are of four types – machines in the cloud, storage in the cloud, databases in the cloud and applications in the cloud. In addition to these, the cloud provides offer other services such as message queues and data mining. All of these things are lumped into the generic term "Cloud computing". The different view points on the emergence of cloud are as follows.



Cloud platforms enable new complex business models in 2017 than in previous years. Recent news revealed, Amazon web services (AWS) attained 43% year over year growth. In another study, it is proved that cloud computing is growing at 4.5 times the rate of IT spendings since 2009 and is expected to grow 6 times more in 2020. Hence, Cloud has a good future ahead.

II. CLOUD STORAGE

Cloud storage is a model of data storage in which the digital data is stored in logical pools. It is a service where data is remotely maintained, managed, and backed up. The service allows the users to store files online, so that they can access them from any location via the Internet.

2.1 Advantages of Cloud Storage

2.1.1. Usability: All cloud storage services reviewed in this topic have desktop folders for Mac's and PC's. This allows users to drag and drop files between the cloud storage and their local storage.

2.1.2. Bandwidth: You can avoid emailing files to individuals and instead send a web link to recipients through your email.

2.1.3. Accessibility: Stored files can be accessed from anywhere via Internet connection.

2.1.4. Disaster Recovery: It is highly recommended that businesses have an emergency backup plan ready in the case of an emergency. Cloud storage can be used as a back-up plan by businesses by providing a second copy of important files. These files are stored at a remote location and can be accessed through an internet connection.

2.1.5. Cost Savings: Businesses and organizations can often reduce annual operating costs by using cloud storage; cloud storage costs about 3 cents per gigabyte to store data internally. Users can see additional cost savings because it does not require internal power to store information remotely.

III. IMPLEMENTATION

With the increasing ofsensitive data outsourced tocloud, cloud storage services are facing many challenges includingdata security and data access control. To solve those problems, attribute-based encryption (ABE) schemes have been applied to cloud storage services. Sahai and Waters first proposed ABE scheme named fuzzy identity-based encryption which is derived from identity-based encryption (IBE). As a new proposed cryptographic primitive, ABE scheme not only has the advantage of IBE scheme, but also provides the characteristic of "one-to-many" encryption. Presently, ABE mainly includes two categories called ciphertext-policy ABE (CP-ABE) and key-policy ABE (KP-ABE). In CP-ABE, ciphertextsareassociated with access policiesand user's private keysareassociated with attribute sets. A user can decrypt the ciphertext if his attributes satisfy the access policy embedded in the ciphertext. It is contrary in KP-ABE. CP-ABE is more suitable forthe outsourcing data architecture than KP-ABE because the access policy is defined by the data owners.In this paper, we have implemented through software, this efficient CP-ABE with user revocation ability.

Security issues are mainobstacles for wide application of cloud computing. Recently, Yu et al. presented a multi keyword top-k retrieval searchable encryption scheme so as tosolve data privacy issues.To ensuresecurity for data outsourcing, Yang et al. proposeda secure over-lay cloud storage system with ability for file assured deletion and policy-based access control. In this article, we focus on designing a CP-ABE scheme with efficient user revocation for cloud storage system.We aim to modelcollusion attack performed by revoked users cooperating with existingusers.

3.1ATTRIBUTE BASED ENCRYPTION

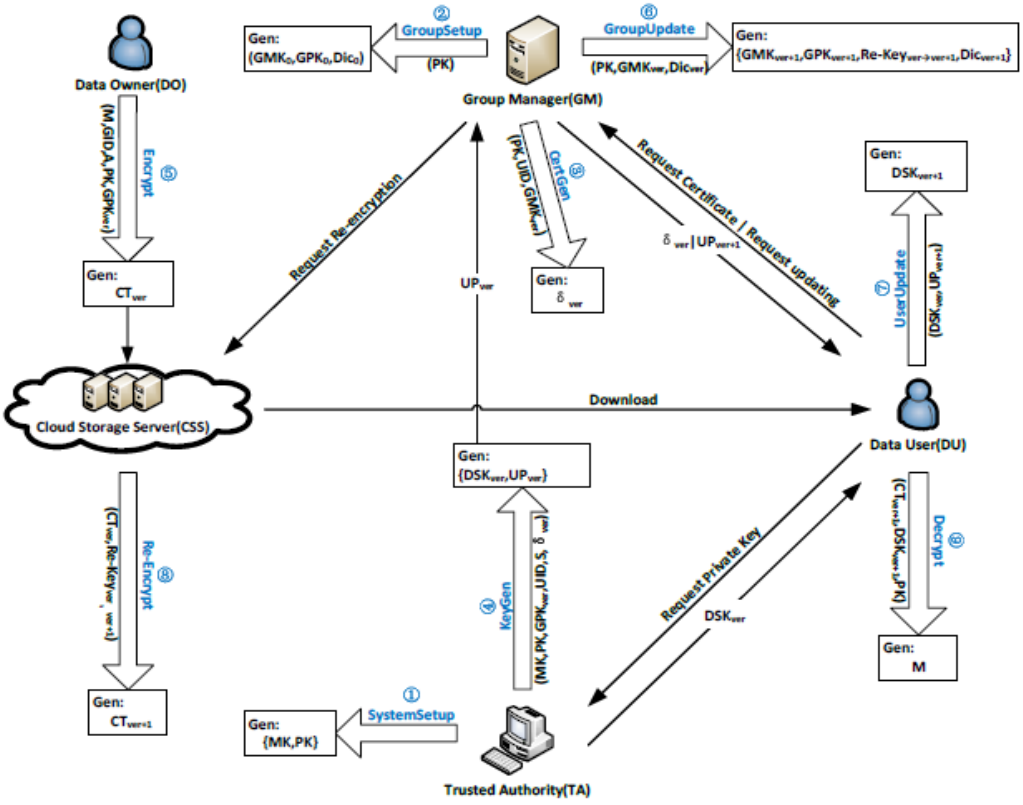
The notion of ABE was first introduced by Sahai and Watersas a new method for fuzzy identity-based encryption. The primary drawback of the scheme is that its threshold semantics lacks expressibility. Several efforts followed in the literature to try to solve the expressibility problem. In the ABE scheme, ciphertexts are not encrypted to one particular user as in traditional public key cryptography. Rather, both ciphertexts and users' decryption keys are associated with a set of attributes or a policy over attributes. A user is able to decrypt a ciphertext only if there is a match between his decryption key and the ciphertext. ABE schemes are classified into key-policy attribute- based encryption (KPABE) and ciphertext-policy attribute- based encryption (CPABE), depending how attributes and policy are associated with ciphertexts and users' decryption keys. Basic CP-ABE schemes are far from enough to support access control in modern enterprise environments, which require considerable flexibility and efficiency in specifying policies and managing user attributes. In a 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. To solve this problem, Bobbaetal.introducedciphertext-policy attributeset-based encryption (CP-ASBE or ASBE for short). ASBE is an extended form of CP-ABE which organizes user attributes into a recursive set structure. The following is an example of a key structure of depth 2, which is the depth of the recursive set structure.

3.1.1 KP-ABE

As more sensitive data is shared and stored by third-party sites on the Internet, there will be a need to encrypt data stored at these sites. One drawback of encrypting data is that it can be selectively shared only at a coarse-grained level (i.e., giving another party your private key). We develop a new cryptosystem for fine-grained sharing of encrypted data that we call Key-Policy Attribute-Based Encryption (KP-ABE). In our cryptosystem, cipher texts are labeled with sets of attributes and private keys are associated with access structures that control which cipher texts a user is able to decrypt. We demonstrate the applicability of our construction to sharing of audit-log information and broadcast encryption.

3.1.2 CP-ABE

In several distributed systems a user should only be able to access data if a user posses a certain set of credentials or attributes. Currently, the only method for enforcing such policies is to employ a trusted server to store the data and mediate access control. However, if any server storing the data is compromised, then the confidentiality of the data will be compromised. In this paper we present a system for realizing complex access control on encrypted data that we call Cipher text-Policy Attribute-Based Encryption. By using our techniques encrypted data can be kept confidential even if the storage server is not trusted; moreover, our methods are secure against collusion attacks. Previous Attribute- Based Encryption systems used attributes to describe the encrypted data and built policies into uses keys; while in our system attributes are used to describe ausers credentials, and a party encrypting data deter-mines a policy for who can decrypt. Thus, our methods are conceptually closer to traditional access control methods such as Role-Based Access Control (RBAC). In addition, we provide an implementation of our sys- tem and give performance measurements



CP-ABE with efficient user revocation

IV. CONCLUSION

The future can be notoriously hard to predict, but cloud computing is certain to continue having a significant effect on business operations. In this paper, we have dealt with the recent trends in cloud computing and implemented the security model for CP-ABE with user revocation.

REFERENCE

[1] A. Sahai and B. Waters,"Fuzzy Identity-Based Encryption,"EUROCRYPT'05, LNCS, vol. 3494, pp. 457-473,2005.

[2] J.Bethencourt,A.Sahai and B.Waters,"Ciphertext-PolicyAttribute-BasedEncryption,"Proc. IEEE Symposium

on Security and Privacy, pp.321-334, May 2007, doi: 10.1109/SP.2007.11.

[3] V. Goyal, O. Pandey, A. Sahai, andB. Waters, "Attribute-Based En-cryption for Fine-Grained Access Control of Encrypted Data,"Proc.13th ACM Conference on Computer and Communications Security(CCS '06), pp. 89-98, 2006, doi:10.1145/1180405.1180418.

[4] D. Boneh and M.K. Franklin,"Identity-Based Encryption from the Weil Pairing," SIAM Journal of Computing, vol. 32, no. 3,pp. 586-615,2003.

[5] A. Boldyreva, V. Goyal, and V. Kumar,"Identity-Based En-cryption with Efficient Revocation,"Proc.15th ACM conference on Computer and communications security(CCS ' 08),pp. 417-426,2008.

International Journal of Engineering Research and Applications (IJERA) is **UGC approved** Journal with Sl. No. 4525, Journal no. 47088. Indexed in Cross Ref, Index Copernicus (ICV 80.82), NASA, Ads, Researcher Id Thomson Reuters, DOAJ.

Dr. P. Julia Grace. "A Study on Recent Trends on Cloud Computing and Attribute-Based Datastorage Concepts." International Journal of Engineering Research and Applications (IJERA) 7.7 (2017): 01-04.