ISSN: 2350-0328

International Journal of Advanced Research in Science, Engineering and Technology

Vol. 2, Issue 12 , December 2015

Review Paper on Secure efficient data access control mechanism P2P storage cloud

Varsha S. Bandagar, Hema V. Kumbhar

P.G. Student, Department of Computer Engineering,P.V.P.I.T. College, Bavdhan, Pune, Maharashtra, India

Associate Professor, Department of Computer Engineering,P.V.P.I.T. College, Bavdhan, Pune, Maharashtra, India

ABSTRACT: A cloud computing in peer to peer storage by combining technique storage cloud can be formed to offer highly available storage services, lowering the economic cost by exploiting the storage space of participating users. However, since cloud severs and users are usually outside the trusted domain of data owners, peer to peer storage cloud brings forth new challenges for data security and access control when data owners store sensitive data for sharing in the trusted domain. Moreover, there are no mechanisms for access control in P2P storage cloud. To address this issue, we design a cipher text-policy attribute-based encryption (ABE) scheme. Based on them, we further propose a secure, efficient and fine-grained data Access Control mechanism for peer to peer storage Cloud named ACPC.As well as attribute based encryption scheme with efficient user revocation the performance evaluation computing overhead reducing when the compare the before user revocation data owner and server.

KEYWORDS: Cloud computing, peer to peer computing, access control, attribute-based encryption.

I. INTRODUCTION

CLOUD computing and Peer-to-Peer (P2P) computing is two of the Internet trends of the last decade, both of which is a form of large-scale distributed systems and have gained popularity in both research and industrial communities. Cloud computing [1,2] is a promising computing paradigm in which resources in the computing infrastructure are provided as services over the Internet by cloud service providers.Cloud computing relies on large data-centre's consisting of thousands of servers and all application processing and resources are centralized. When users store sensitive data in the cloud, maintaining confidentiality and privacy of the data become encryption scheme. A challenging [3] cloud servers are operated by commercial providers who are usually outside of the trusted domain of users; they are not entitled to access the confidential data. Overcome this Data access control has been well studied and the various technique, have been developed to specify different access rights for the individual user traditional access control model assume that the server are fully trusted by data owner and the let the server enforce all access control policies. However this assumption no longer holds in cloud computing to achieve access control of data stored untrusted cloud server. A feasible solution[4,5] would be storing data using dual attribute based encryption scheme. And the disclosing decryption key only authorized user. Will be motivate[6] this traditional access control models often assume that the entity enforcing access control policies is also the owner of data and resource. This assumption no longer holds when data is outsourced to third party storage provider such as the cloud existing access control solution mainly focus on preserving confidential of stored data from unauthorized access and storage provider.

However in this setting access control policies become privacy sensitive information that should be protected from the cloud. A recently proposed access control model, called attribute-based access control, defines access control policiesbased on the attributes of the user, environment, or the data. ABE [8,9] is a public-key cryptography primitive thatwas proposed to achieve the attribute-based access controlon untrusted storage. Compared to previous works, ABE can achieve the complexity of encryption and key management are independent from the numberof system users, and is just related to the number ofsystem attributes. User revocation[10]is an important issue in access control systems. However, it is hard to execute userrevocation efficiently in ABE schemes since each attribute isusually shared by multiple users. To revoke attributes from user, the data owner has to re-encrypt all the files associatedwith revoked attributes and update the secret keys forall the remaining users who share these attributes. Thoseoperations would introduce heavy computation overheadson the data owner and may also require the data owner tobe always online

ISSN: 2350-0328
International Journal of Advanced Research in Science, Engineering and Technology
Vol. 2, Issue 12 , December 2015

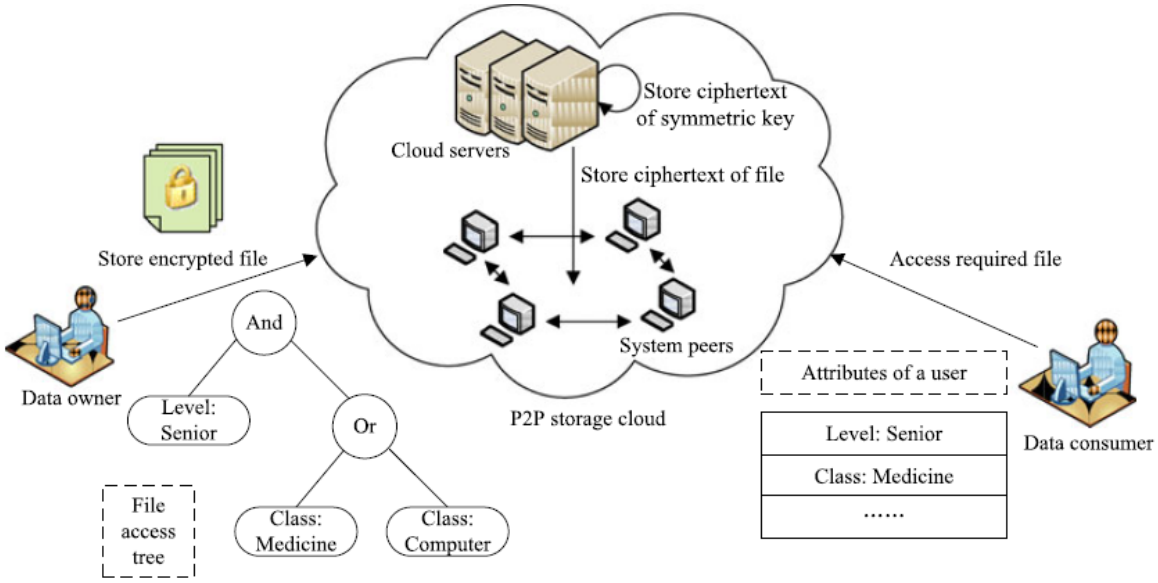

Fig. shows an example process data access control mechanism ACPC

The communication channels between cloud servers and users are assumed secured under existing security protocols. In P2P cloud, a peer's comprehensive reputation value is computed by its reputation rating from other peers and its computing power, contributing storagespace and online time. We assume that there exists well-designed P2P reputation system in P2P cloud which can help us to select peers with high reputation values. For these selected peers, we assume that most of them are trustful, while a few of them may be semi-trustful or malicious. Trustful and semi-trustful peers will perform our proposed mechanism in general, while malicious peers will not. Semi-trusted peers and malicious peers may collude with revoked users to access files. Note that, for designed P2P reputation system, only trusted peers with legitimate behaviours can keep high reputation rating.

II. LITERATURE SURVEY

[1] Hung He, Ruixuan Li, Xinhua Dong, and Zhao Zhang "Secure, Efficient and Fine-Grained Data Access Control Mechanism for P2P Storage Cloud" IEEE transactions oncloud computing, vol. 2, no. 4, october-december 2014:
In this paper we first briefly present the technique preliminaries closely related to ACPC, and then present the system model and some security assumptions of ACPC. At a high level, our work is similar to the recent work. attribute based encryption (KP-ABE), however we require substantially new techniques. In key-policy attribute based encryption, cipher texts are associated with sets of descriptive attributes, and user keys are associated with policies (the reverse of our situation).

[2] P. Mell and T. Grange, "The NIST definition of cloud computing, NIST Special800-145, Sep. 2011:
In this survey paper we stress that in key-policy ABE, the encrypted exerts no control over who has access to the data she encrypts, except by her choice of descriptive attributes for the data. Rather, she must trust that the key-issuer issues the appropriate keys to grant or deny access to the appropriate users. In other words, in the intelligence" is assumed to be with the key issuer, and not the encrypted. In our setting, the encryption must be able to intelligently decide who should or should not have access to the data that she encrypts 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 un trusted; moreover, our methods are secure against collusion attacks.

ISSN: 2350-0328

International Journal of Advanced Research in Science, Engineering and Technology

Vol. 2, Issue 12 , December 2015

[3] Rodrigues and P. Urschel, "Peer-to-peer systems," Common ACM, vol. 53, no. 10, pp.72-82, Oct. 2010:
In this paper Attribute-Based Encryption systems used attributes to describe the encrypted data and built policies into user's keys while in our system attributes are used to describe a user's credentials, and a party encrypting data determines a policy for who can decrypt. Thus, our methods are conceptually closer to traditional access control methods. We provide an implementation of our system to show that our system performs well in practice. We provide a description of both our API and the structure of our implementation. In addition, we provide several techniques for optimizing decryption performance and measure our performance features experimentally.

4] J. Li and Q. Huang, "Erasure resilient codes in peer-to-peer storage cloud" in Proc. IEEE Int. Conf. Acoustics, Speech Signalling Process.,2006, pp. 14-19:
This paper Cinematic-Quality in a P2P Storage Cloud: Design, Implementation and Measurement we explore the design space and practice of a new peer-to-peer (P2P) storage cloud, which is capable of replicating, refreshing and on demand streaming of cinematic-quality video streams, in a decentralized fashion using local storage spaces of end users. We identify key design challenges and trade off in such a P2P storage cloud, and how these are addressed by making informed design choices in a step-by-step fashion. Following our design choices, we have implemented a real world Video-on-Demand (VOD) system with over 100,000 lines of code, called Novak, which features new coding-aware peer storage replacement and server push to- peer strategies, in order to maintain media availability and to balance the system-wide supply-demand relationship in the P2P storage cloud. General understanding on the design trade off of P2P storage cloud and practical experiences with Nova skymay bring valuable guidelines to future designs of production-quality P2P storage cloud systems.

[5] H. Kivalina and A. Montresor, "P2P and cloud: A marriage of convenience for replicaManagement," in Proc. 6th IFIP TC 6 Int. Conf. Self-Organizing Syst., 2012, pp. 60-71:
This paper Decentralized Access Control with Anonymous Authentication of Data Stored in Cloud We propose a new decentralized access control scheme for secure data storage in clouds that supports anonymous authentication. In the proposed scheme, the cloud verifies the authenticity of the series without knowing the user's identity before storing data. Our scheme also has the added feature of access control in which only valid users are able to decrypt the stored information. The scheme prevents replay attacks and supports creation, modification, and reading data stored in the cloud. We also address user revocation. Moreover, our authentication and access control scheme is decentralized and robust, unlike other access control schemes designed for clouds which are centralized. The communication,computation,and storage overheads are comparable to centralized approaches.

III. EXISTING METHODOLOGY

In ACPC, we associate each file with an expressive access tree which is defined over attributes, and associate each user secret key with a set of these attributes. Since CP-ABE is inefficient when it is directly used to encrypt the data file, especially for the files of large size, the data owner encrypts the file using symmetric encryption algorithm first, and then encryptsthe symmetric key with PCCP-ABE. The cipher text of the symmetric key including the fileaccess tree is stored in cloud servers, while the cipher text of the file is stored in P2P cloud. Thedata consumer can decrypt the symmetric key using his secret key if the associated attributessatisfy the file access tree, and then he can decrypt the file using the symmetric key. User revocationis a challenging issue when we utilize this construction to enforce access control in P2Pwhere user revocation may occur frequently and in different granularities. For instance,users can unsubscribe any attributes at any time in the example. When revoking a user, thedata owner may require revoking all the attributes of the user, or just a subset of the attributes. Then he needs to re-encrypt all the files associated with revoked attributes and update secret keys for all the remaining users who also have these attributes. User revocation will introduce heavy computation overheads and cumbersome online requirements towards the data owner, if the data owner performs all these tasks.

A. PCCP-ABE

Consists of four algorithmsnamely setup, secret key generation, encryption and decryption. We describe them as follows. PCCP-ABE setup, generate system public key and a system master key, according to the attribute

ISSN: 2350-0328
International Journal of Advanced Research in Science, Engineering and Technology
Vol. 2, Issue 12 , December 2015

universe. Generates a user secret key associated with an attribute set, according to PCCP-ABE encryption algorithm encrypts the data plaintext under its access tree, according to PK. A user can decrypt the cipher text only when the attributes associated with the user's SK satisfy the access tree.

B. PC-PRE

PC-PRE consists of three algorithms, namely attribute update, cipher text component re encryption,secret key component update. We describe them as follows. PCPRE attribute update updates an attribute by redefining its master key component and itspublic key component, and then generates a PRE key to update the old master key componentand public key component. PC-PRE cipher text component-encryption algorithm re-encrypt cipher text component of an attribute using the third component of the corresponding PREkey. The re-encrypted ciphertext component coincides with the latest master key componentof the attribute. Thecorresponding user secret key can be used to decrypt the re-encrypted Ciphertext only when the secret key component of the attribute is also updated.

C. ACPC

In describe the system operations in ACPC, which include system setup, new file creation,new user grant, user revocation, file access, and reputable peer removal. User revocation isa challenging issue when we utilize this construction to enforce access control in P2P cloud,where user revocation may occur frequently and in different. In ACPC, we delegate secret keyupdate to reputable peer picked out by P2P reputation system. However, some of these peermay be not fully trusted and may collude with revoked users, updating secret key componentsfor them to access files. To prevent such collusion, we randomly select a pair of peers tocooperatively update the secret keycomponent of an attribute.

IV. CONCLUSION

This paper aims at providing secure, efficient and fine grained data access control in P2P storage cloud, which is not supported by current works. To achieve this goal, we design an efficient CP-ABE scheme and a corresponding PRE scheme, i.e., PCCP-ABE and PCPRE, and then propose ACPC based on those schemes. To efficiently address the issue of user revocation, in ACPC we integrate P2P reputation system and enable the data owner to delegate file re encryption to cloud servers and delegate user secret key update, the most computation intensive task, to the reputable system peers picked out by P2P reputation system. Moreover, ACPC is provably secure under the standard security model and can resist collusion attacks and protect user access privilege information effectively.

REFERENCES

[1] Hung He, Ruixuan Li, Xinhua Dong, and Zhao Zhang "Secure, Efficient and Fine-Grained Data Access Control Mechanism for P2P Storage Cloud" IEEE transactions oncloud computing, vol. 2, no. 4, october-december 2014.
[2] P. Mell and T. Grange, "The NIST definition of cloud computing, NIST Special800-145, Sep. 2011.
[3] Rodrigues and P. Urschel, "Peer-to-peer systems," Common ACM, vol. 53, no. 10, pp.72-82, Oct. 2010.
[4] J. Li and Q. Huang, "Erasure resilient codes in peer-to-peer storage cloud" in Proc. IEEEInt. Conf. Acoustics, Speech Signalling Process.,2006, pp. 14-19.
[5] H. Kivalina and A. Montresor, "P2P and cloud: A marriage ofconvenience for replicaManagement," in Proc. 6th IFIP TC 6 Int. Conf. Self-Organizing Syst., 2012, pp. 60-71.
[6] R.Rajah, L. Zhao, Xu, A. Liao. Quiroz, andM. Preacher, "Peerto-peer cloud:Service discovery and load-balancing,"in Cloud Compute.: Principles, Systems andApplications, Part 2,N.Antonopoulos,L.Gillam, Ed. London: Springer, pp. 195-217,May2010.
[7] L. Bremer and K. Graffiti, "Symbiotic coupling of P2P and cloudsystems: TheWikipediacase," in Proc. IEEE Int. Conf. Communed.,2013, pp. 3444-3449.
[8] Z. Yang, B. Zhao, Y. Xing, S. Ding, F. Xiao, and Y. Dai,"Amazing store: Available, lowonline storage service usingcloudlets," in Proc. 9th Int.Workshop Peer-to-Peer Syst.,2010, pp.105-234.
[9] Symport web site. (2014). Available: http://symform.com/
[10] T. Maher, E. Bier sack, and P. Misheard, "A measurement study of the Wala on-line storage service," in Proc. 12th IEEE Int. Conf. Peer-to-Peer compute., 2012, pp. 237-248.