International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169
Volume: 5 Issue: 5 1033 – 1034

Multiple Authorities Access under Public Cloud Storage

Bhagyashree D. Masatkar
M. Tech. III Sem
TGPCET, Nagpur

Prof Roshani Talmale
HOD, CSE
TGPCET, Nagpur

Prof Vishal Tiwari
CSE Department
TGPCET, Nagpur

Abstract **-** Public cloud storage is a cloud storage model that provide services to individuals and organizations to store, edit and manage data. Public cloud storage service is also known as storage service, utility storage and online storage. Cloud storage has many advantages, there is still remain various challenges among which privacy and security of users data have major issues in public cloud storage. Attribute Based Encryption(ABE) is a cryptographic technique which provides data owner direct control over their data in public cloud storage. In the traditional ABE scheme involve single authority to maintain attribute set which can bring a single-point bottleneck on both security and performance. Now we use threshold multi-authority Cipher text-Policy Attribute-Based Encryption (CP-ABE) access control scheme, name TMACS. TMACS is Threshold Multi-Authority Access Control System. In TMACS,multiple authority jointly manages the whole attribute set but no one has full control of any specific attribute. By combining threshold secret sharing (t,n) and multi-authority CP-ABE scheme, we developed efficient multi-authority access control system in public cloud storage.

Index Terms *-Access control, Attributes-Based Encryption, data storage, Multi-Authority*

*****

I. INTRODUCTION

1.1 Background

Cloud storage is an important service of cloud computing, which provides services for data owners to outsource data to store in cloud via Internet. As cloud storage has many advantages ,there is still remains various challenges among which ,privacy and security of users' data have major issues in public cloud storage. Traditionally, a data owner stores his/her data in trusted servers, controlled by a fully tru administrator[3].

Attribute-based Encryption (ABE) is regarded as one of the most suitable schemes to conduct data access control in public clouds for it can guarantee data owners direct control over their data and provide a fine-grained access control service. In most existing CP-ABE[1], [9] schemes there is only one authority responsible for attribute management and key distribution. This only-one-authority scenario can bring a single-point bottleneck on both security and performance.

Now we use threshold multi-authority CP-ABE [13],[14]access control scheme, named TMACS, to deal with the single-point bottleneck on both security and performance in most existing schemes. TMACS is Threshold Multi-Authority Access Control System. In TMACS, multiple authorities jointly manage the whole attribute set but no one has full control of any specific attribute.

1.2Our contribution

In this paper we areintroduces multi-authority data access control for cloud storage system with Attributes-Based Encryption. Threshold multi-authority CP-ABE access control scheme called as TMACS , which deals with the single-point bottleneck on both security and performance. In TMACS, multiple authority jointly manages the whole attribute set but no one has full control of any specific attribute. In CP-ABE schemes, there is always a secret key(SK) used to generate attribute private keys, we introduce(t, n) threshold secret sharing into our scheme to share the secret key among authorities.

II. Related work

Cryptographic techniques are well applied to access control for cloud storage system.[3]The data owners encrypt files by using the symmetric encryption approach with content keys and then use every user's public key to encrypt the content keys.Attribute-based Encryption (ABE) is a promising technique that is very suitable for access control of encrypted data.In CP-ABE schemes,[1] there is always a secret key(SK) used to generate attribute private keys, we introduce(t, n) threshold secret sharing into our scheme to share the secret key among authorities. In existing access control systems for public cloud storage, there brings a single-point bottleneck on both security and performance against the single authority for any specific attribute.[1]By introducing the combining of (t;n) threshold secret sharing and multi-authority CP-ABE scheme we propose multi- authority access control system in public cloud storage, in which multiple authorities jointly manage a uniform attribute set. By combining the traditional multi-authority scheme with ours, we construct a hybrid one, which can satisfy the scenario of attributes coming from different authorities which can solve single point bottleneck problem and provide security.

MODULE

1. **CertificateAuthority:** Certificate Authority is responsible for the construction of the system by setting up system parameters and attribute public key(PK) of each attribute in whole attribute set.
2. **Attribute authority**: Attribute authority focuses on the attribute management and key generation. AA jointly manages the whole attribute set , any one of the AA can not assign users secrete key alone for the master key is shared by AA.
3. **Data Owner:** Owner encrypts his/her file and define access about who can get access to his/her data. Owner encrypts his/her data with a symmetric encryption algorithm .Then the owner formulates access policy over an attribute set and encrypts the symmetric key under the policy according to attribute public key gained from CA .
4. **Data Consumer:** In this module, Users are having authentication and security to access the detail which is presented in the system. Before accessing the details user should have the account in that otherwise they should register first. CA can assign user identity uid and password to data consumer.[1]
5. **Public Cloud Server:**An entity which is managed by cloud server provider to provide data storage services . In cloud data storage , a user store his data in cloud server .In cloud data storage system , user store their data in clouds and no longer possess the data locally. Thus the correctness and availability of the data files being stored on the distributed cloud server must be guaranteed.

III. CONCLUSION

In this paper, we proposed multi-authority access control scheme,in public cloud storage. In this scheme multiple authority jointly manages the whole attribute set and share the master key. This scheme avoids a single-point bottle neck on both security and performance

Acknowledgment

The authors would like to CSE Department and Principal of TGPCET TulsiramGaiyakwadPatil College of Engineering & Technology providing their support and facilities like labs, softwares etc. requiredto hold out this work.

.

REFERENCES

[1] Wei Li, KaipingXue, YingjieXue, and Jianan Hong. "TMACS: A Robust and Verifiable Threshold Multi-Authority Access Control System in Public Cloud Storage" VOL. 27, NO. 5, MAY 2016

[2] B. Waters, "Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization," in Proc.14th Int. Conf. Practice Theory Public Key Cryptography, 2011, pp. 53–70

[3] K. Yang and X. Jia, "Attributed-based access control for multi-authority systems in cloud storage," in Proc. IEEE 32nd Int. Conf.Distrib. Comput. Syst., 2012, pp. 536–545.

[4] T. Jung, X. Li, Z. Wan, and M. Wan, "Privacy preserving cloud data access with multi-authorities," in Proc. 32nd IEEE Int. ConfComput. Commun., 2013, pp. 2625–2633.

[5] S. Patil, P. Vhatkar, and J. Gajwani, "Towards secure and dependable storage services in cloud computing," Int. J. Innovative Res.Adv. Eng., vol. 1, no. 9, pp. 57–64, 2014.

[6] S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving secure, scalable, and fine-grained data access control in cloud computing," in Proc.29th IEEE Int. Conf. Comput. Commun., 2010, pp. 1–9.

[7] J. Li, X. Huang, J. Li, X. Chen, and Y. Xiang, "Securely outsourcing attribute-based encryption with checkability," IEEE Trans. ParallelDistrib. Syst., vol. 25, no. 8, pp. 2201–2210, Aug. 2014.

[8] M. Li, S. Yu, Y. Zheng, K. Ren, and W. Lou, "Scalable and secure sharing of personal health records in cloud computing using attribute- based encryption," IEEE Trans. Parallel Distrib. Syst., v[9] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attri- bute-based encryption," in Proc. IEEE Symp. Security Privacy, 2007, pp. 321–334ol. 24, no. 1, pp. 131–143, Jan. 2013.

[9] J. Hur, "Improving security and efficiency in attribute-based data sharing," IEEE Trans. Knowl. Data Eng., vol. 25, no. 10, pp. 2271– 2282, Oct. 2013.

[10] Z. Wan, J. Liu, and R. Deng, "Hasbe: A hierarchical attribute based solution for flexible and scalable access control in cloud computing," IEEE Trans. Inf. Forensics Security, vol. 7, no. 2, pp. 743–754, Apr. 2012.

[11] Y. Wu, Z. Wei, and H. Deng, "Attribute-based access to scalable media in cloud-assisted content sharing," IEEE Trans. Multimedia, vol. 15, no. 4, pp. 778–788, Jun. 2013

[12] M. Chase, "Multi-authority attribute based encryption," in Proc. 4th Theory Cryptography Conf., 2007, pp. 515–534.

[13] G.Rajesh Babu, Ananth Kumar ,"Security In Inter Cloud Data Transfer" International Journal of Innovative Research in Computer Science & Technology (IJIRCST) ISSN: 2347-5552, Volume-2, Issue-5, September-2014.

[14] A. Lewko and B. Waters, "Decentralizing attribute-based encryption," in Proc. 30th Annu. Int. Conf. Theory Appl. Crypto- graphic Techn., 2011, pp. 568–588

[15] H. Lin, Z. Cao, X. Liang, and J. Shao, "Secure threshold multi- authority attribute based encryption without a central authority," Inf. Sci., vol. 180, no. 13, pp. 2618–2632, 2010.

[16] T. Pedersen, "A threshold cryptosystem without a trusted party," in Proc. 10th Annu. Int. Conf. Theory Appl. Cryptographic Techn., 1991, pp. 522–526.

[17] G.Rajesh Babu, G.Ananth Kumar, Vishal Tiwari," Security Risks Associated with the Cloud Computing, International Journal of Research (IJR) ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 06, June 2015.

[18] A. Shamir, "How to share a secret," Commun. ACM, vol. 22, no. 11, pp. 612–613, 1979.