Multiple Authorities Access under Public Cloud Storage: Review

Guide
Prof Roshani Talmale
HOD, CSE
TGPCET, Nagpur

Co-guide
Prof Vishal Tiwari
Dept. of CSE
TGPCET, Nagpur

Submitted By
Bhagyashree D. Masatkar
M. Tech. III Sem
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 only one authority to maintain attribute set which can bring a single-point bottleneck on 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 user 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

Cloud storage is one of the important service of cloud computing, which provides services for data owner 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, which are generally controlled by a fully trusted administrator. In public cloud storage systems, the cloud is usually maintained and managed by a semi-trusted third party. Data is no longer in data owner's trusted domains and the data owner cannot trust on the cloud server to conduct secure data access control. Therefore, the secure access control problem has become a critical challenging issue in public cloud storage, in which traditional security technologies cannot be directly applied.

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 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 usethreshold multi-authority CP-ABE 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.

II. LITERATURE REVIEW

Wei Li, et al. [1] suggested, a access control systems for public cloud storage, brings a single-point bottleneck on both security and performance against the single authority for any specific attribute. First design multiple-authority access control architecture to deal with the problem. By introducing the combining of (*t, n*) threshold secret sharing and multi-authority CP-ABE scheme, then

proposes and realizes a robust multi-authority access control system in public cloud storage, in which multiple authorities jointly manage a uniform attribute set. Further by efficiently combining the traditional multi-authority scheme with this scheme, design a hybrid one, which can satisfy the scenario of attributes coming from different authorities as well as achieving security and system-level robustness.

B.Waters [2] suggested Ciphertext-policy attribute encryption under concrete and non-interactive Cryptographic assumption in the standard Model. Our solution allow to specify access control in terms of any access formula for the attribute in the system. In our most efficient system cipher text size, encryption and decryption time scale linearly with the complexity of the access formula.

K.Yang and X.Jia[3] , suggested new access control for multi-authority system in cloud storage and provide secure

and efficient multi-authority access control scheme first defined an efficient multi-authority CP-ABE that does not require a gobal authority and can support any LSSS access structure.

T. Jung, X. Li, Z. Wan, and M. Wan [4] , suggested an anonymous attribute based privilege control scheme AnonyControl to provide the user privacy in a cloud storage server. By using multiple authorities in cloud computing system , proposed scheme provide fine-grained privilege control and anonymity while conducting privilege control which is based on user identity information.

S. Patil, P. Vhatkar, and J. Gajwani,[5] In this paper, we propose an effective and flexible distributed storage verification scheme with explicit dynamic data support to ensure the correctness and avail- ability of users' data in the cloud. This construction drastically reduces the communication and storage overhead as compared to the traditional replication-based file distribution techniques. By utilizing the homomorphic token with distributed verification of coded data, our scheme achieves the storage correctness insurance as well as data error localization: whenever data corruption has been detected during the storage correctness verification, our scheme can almost guarantee the simultaneous localization of data errors, i.e., the identification of the misbehaving server(s).

Cloud server is nothing but the large data server where data have to manage and control. So there required to provide the authority to multiple user access and control the system.for providing the security to data we can used the ECC Algorithum.

CONCLUSION

Proposed a revocable decentralized data access control system can support efficient attribute revocation for multi-authority cloud storage systems. It eliminates decryption overhead of users according to attributes. This secure attribute based encryption technique for robust data security that is being shared in the cloud. This revocable multi-authority data access scheme with verifiable outsourced decryption and it is secure and verifiable. This scheme will be a promising technique, which can be applied in any remote storage systems and online social networks etc.

REFERENCES

[1] Wei Li, Kaiping Xue, Yingjie Xue, 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. Conf Comput. 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. Parallel Distrib. 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., vol. 24, no. 1, pp. 131–143, Jan. 2013.

[9] 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.

[10] 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.

[11] 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.