iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 4 **Issue:** III **Month of publication:** March 2016

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

Volume 4 Issue III, March 2016
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

An Attribute Based Secure Data Self-Destructing and Time Server

Bharath Kumar.B[1], Sakthivel.K[2], G.Senthil Kumar[3]
[1,2] B.E Student, Dept. of CSE, Panimalar Engineering College, Poonamalle, Tamilnadu, India.
[3]Associate Professor, Dept. of CSE, Panimalar Engineering College, Poonamalle, Tamilnadu, India.

Abstract: ***Recent years all are using the cloud server. The reason of cloud server easy to use and having the security. Once we upload the file store to the cloud server then that files access the world wide and any time. Here access the cloud server from the many users so have changes to unauthorized user access the other users file. So we are providing the file key for storing file in cloud server. When user want the file from the cloud server that time must give the file keyset. In existing system user like to share the file into friends circle that time upload the file into cloud server. Once that friends are download the files from the cloud server. Then that files store in permanently at cloud server. This main disadvantage of this unauthorized user access the file and chances to miss use the files. So this is big challenge to store files with secure in cloud server. So we are learning in this paper how to overcome this problem and file store in secure. In proposed when user want to share the file into friends circle via cloud server that time give the key for file download. And here additionally user allocate the particular time interval for the access the files from the cloud server. When friends want to access the file. That time asking to file user. File user send the file key and also time interval. That time only friends are access the file. If before and after the time interval that file can't access from the friends circle. This is mainly used for the secure the file in cloud server.***

I. INTRODUCTION

Cloud computing is considered as the next step in the evolution of on-demand information technology which combines a set of existing and new techniques from research areas such as service-oriented architectures (SOA) and virtualization. With the rapid development of versatile cloud computing technology and services, it is routine for users to leverage cloud storage services to share data with others in a friend circle, e.g., Dropbox, Google Drive and AliCloud [1]. The shared data in cloud servers, however, usually con- tains users' sensitive information (e.g., personal profile, financial data, health records, etc.) and needs to be well pro- tected [2]. As the ownership of the data is separated from the administration of them [3], the cloud servers may migrate users' data to other cloud servers in outsourcing or share them in cloud searching [4]. Therefore, it becomes a big challenge to protect the privacy of those shared data in cloud, especially in cross-cloud and big data environment [5]. In order to meet this challenge, it is necessary to design a comprehensive solution to support user-defined authori- zation period and to provide fine-grained access control during this period. The shared data should be self- destroyed after the user-defined expiration time.

II. LITERATURE SURVEY

©IJRASET : All Rights are Reserved

Volume 4 Issue III, March 2016
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

PAPER NAME	AUTHOR NAME	ALGORITHM USED	DISADVANTAGE
Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data	V. Goyal, O. Pandey, A. Sahai,	Randomized algorithm	Disadvantage of encrypting data is that it severely limits the ability of users to selectively share their encrypted data at a Øne-grained level. Suppose a particular user wants to grant decryption access to a party to all of its Internet tra±c logs for all entries on a particular range of dates that had a source IP address from a particular subnet.
"Revisiting the Security Model for Timed-Release Encryption with Pre-Open Capability	J. H. Cheon, N. Hopper, Y. Kim, and I. Osipkov,	Polynomial time algorithms	Many legal systems require that classi¯ed governmental information is disclosed after a certain period of time. This can be achieved by using a TRE-PC scheme, through which the classi¯ed information can be encrypted by the public key of a special agent which is responsible for disclosing classi¯ed information. Note that no original classi¯ed information is required to be stored, and in the case that the information needs to be prematurely released, a pre-open key can be sent to the special agent which is able to decrypt the encrypted classi¯ed information.

©IJRASET : All Rights are Reserved

A Secure Cipher text Self-Destruction Scheme with Attribute-Based Encryption	J. Xiong, Z. Yao, J. Ma, X. Liu	symmetric encryption algorithms	there are security problems in the schemes of. Besides, these decentralized solutions adopt the symmetric encryption algorithms, which will bring complex key management and distribution problems. To solve these problems, an improved system called SafeVanish is proposed [
SoK: Secure Data Deletion	J. Reardon, D. Basin,	cryptographic scheme	There is a wealth of adversarial bounds corresponding to a spectrum of non-equivalent computational hardness problems, so others may benefit from dividing this spectrum further. However, for all the approaches discussed in this paper, it suffices to distinguish between adversaries who can break cryptographic standards such as AES and those who cannot.
SeDas: SELF - DESTRUCTION DATA SYSTEM FOR DISTRIBUTED OBJECT BASED ACTIVE STORAGE FRAMEWORK	L. Zeng, S. Chen, Q. Wei, and D. Feng	Shamir Secret Sharing Algorithm	There are multiple storage services for a user to store data. Meanwhile, to avoid the problem produced by the centralized “trusted” third party, the responsibility of SeDas is to protect the user key and provide the function of self-destructing data

III. CONCLUSIONS

With the rapid development of versatile cloud services, a lot of new challenges have emerged. One of the most important problems is how to securely delete the outsourced data stored in the cloud severs. In this paper, we proposed a novel KP-TSABE scheme

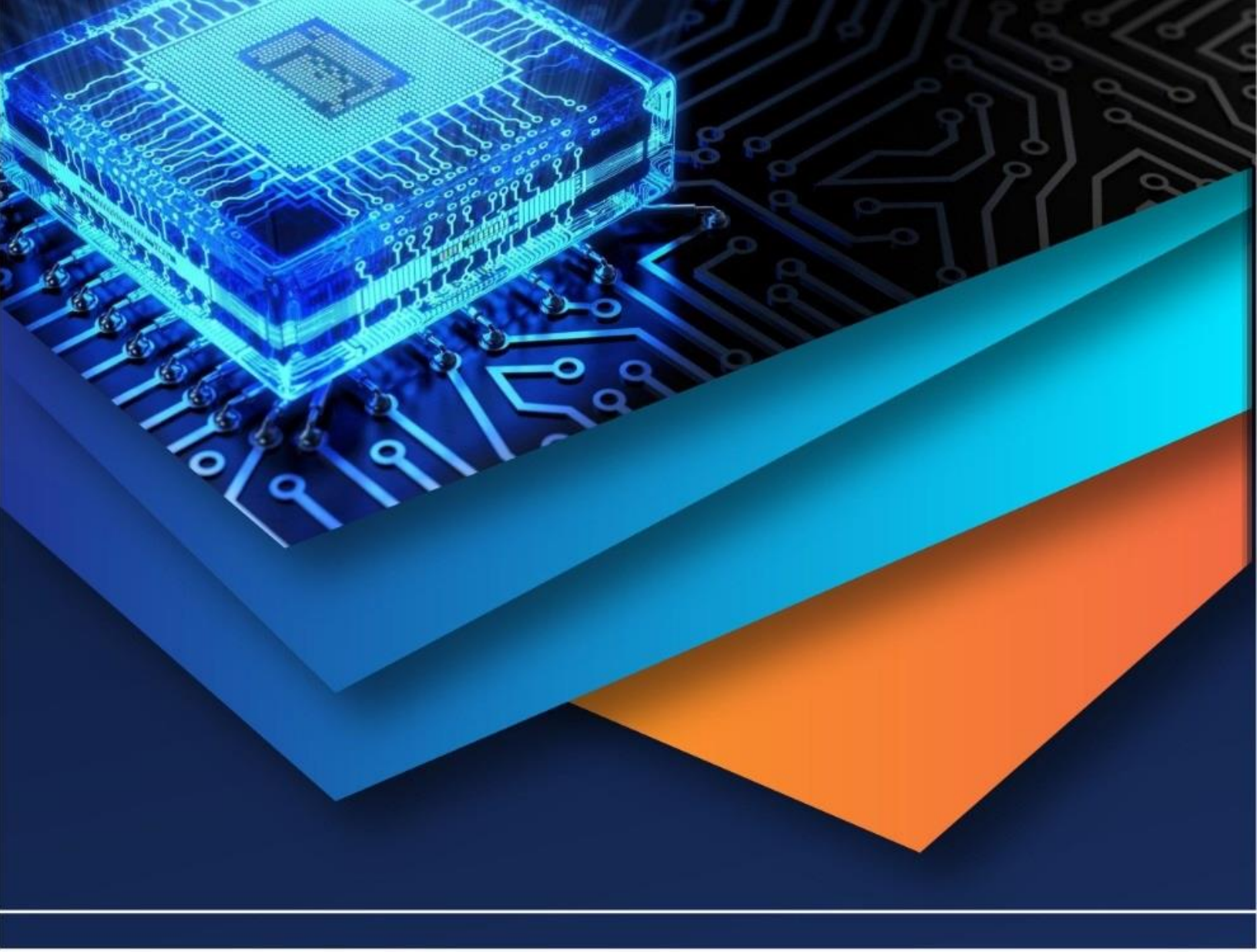
©IJRASET : All Rights are Reserved

which is able to achieve the time- specified ciphertext in order to solve these problems by implementing flexible fine-grained access control during the authorization period and time-controllable self-destruc- tion after expiration to the shared and outsourced data in cloud computing. We also gave a system model and a secu- rity model for the KP-TSABE scheme. Furthermore, we proved that KP-TSABE is secure under the standard model with the decision l-Expanded BDHI assumption. The com- prehensive analysis indicates that the proposed KP-TSABE scheme is superior to other existing schemes.

REFERENCES

[1] B. Wang, B. Li, and H. Li, "Oruta: Privacy-preserving public auditing for shared data in the cloud," IEEE Trans. Cloud Comput., vol. 2, no. 1, pp. 43–56, Jan.–Mar. 2014.
[2] J. Xiong, Z. Yao, J. Ma, X. Liu, Q. Li, and J. Ma, "Priam: Privacy preserving identity and access management scheme in cloud," KSII Trans. Internet Inf. Syst., vol. 8, no. 1, pp. 282–304, 2014.
[3] J. Xiong, F. Li, J. Ma, X. Liu, Z. Yao, and P. S. Chen, "A full life- cycle privacy protection scheme for sensitive data in cloud computing," Peer-to-Peer Netw. Appl., Jun. 2014, DOI:10.1007/ s12083-014-0295-x.
[4] P. Jamshidi, A. Ahmad, and C. Pahl, "Cloud migration research: A systematic review," IEEE Trans. Cloud Comput., vol. 1, no. 2, pp. 142–157, Jul.–Dec. 2013.
[5] R. Lu, H. Zhu, X. Liu, J. K. Liu, and J. Shao, "Toward efficient and privacy-preserving computing in big data era," IEEE Netw., vol. 28, no. 4, pp. 46–50, Jul./Aug. 2014.
[6] X. Liu, J. Ma, J. Xiong, and G. Liu, "Ciphertext-policy hierarchical attribute-based encryption for fine-grained access control of encryption data," Int. J. Netw. Security, vol. 16, no. 4, pp. 351–357, 2014.
[7] A. Sahai and B. Waters, "Fuzzy identity-based encryption," in Proc. Adv. Cryptol., 2005, pp. 457–473.
[8] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in Proc. 13th ACM Conf. Comput. Commun. Security, 2006, pp. 89–98.
[9] A. F. Chan and I. F. Blake, "Scalable, server-passive, user-anony- mous timed release cryptography," in Proc. Int. Conf. Distrib. Com- put. Syst., 2005, pp. 504–513.
[10] K. G. Paterson and E. A. Quaglia, "Time-specific encryption," in Proc. 7th Int. Conf. Security Cryptography Netw., 2010, pp. 1–16.
[11] Q. Li, J. Ma, R. Li, J. Xiong, and X. Liu, "Large universe decentral- ized key-policy attribute-based encryption," Security Commun. Netw., Mar. 2014, DOI: 10.1002/sec.997.
[12] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attri- bute-based encryption," in Proc. 28th IEEE Symp. Security Privacy, 2007, pp. 321–334.
[13] L. Cheung and C. C. Newport, "Provably secure ciphertext policy abe," in Proc. 14th ACM Conf. Comput. Commun Security, 2007, pp. 456–465.
[14] B. Waters, "Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization," in Proc. Public Key Cryptography, 2011, pp. 53–70.
[15] A. Shamir, "How to share a secret," Commun. ACM, vol. 22, no. 11, pp. 612–613, 1979.

©IJRASET : All Rights are Reserved



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)