ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 4, Issue 12, December 2016

A Survey on Secure Anti Collusion Mechanism with Distributed Storage in Cloud Computing

Sanyogita Kamble[1], Prof. Arti Mohanpurkar[2]

M. E Student, Dept. of Computer Engineering, Dr. D. Y. Patil School of Engineering and Technology, Lohegaon, Pune, Maharashtra, India[1]

Professor, Dept. of Computer Engineering, Dr. D. Y. Patil School of Engineering and Technology, Lohegaon, Pune, Maharashtra, India[2]

ABSTRACT: Benefited from cloud computing, users can do a good and economical approach for information sharing among cluster members within the cloud with the characters of low maintenance and tiny management value. Meanwhile, it should offer security guarantees for the sharing information files since they're outsourced. sadly, attributable to the frequent amendment of the membership, sharing information whereas providing privacy-preserving continues to be a difficult issue, particularly for AN untrusted cloud because of the collusion attack.[5] what is more, for existing schemes, the protection of key distribution is predicated on the secure line, however, to possess such channel may be a robust assumption and is troublesome for observe. During this paper propose a secure information sharing theme for dynamic members. Firstly, propose a secure method for key distribution with none secure communication channels, and therefore the users will firmly get their non-public keys from cluster manager.[6] Second, this theme can do fine-grained access management, any user within the cluster will use the supply within the cloud and revoked users cannot access the cloud once more when they're revoked. Thirdly, system will defend the theme from collusion attack, which implies that revoked users cannot get the initial record even though they conspire with the untrusted cloud. [1] During this approach, by leverage polynomial perform, it can do a secure user revocation theme.

KEYWORDS: Access control, privacy-preserving, key distribution, cloud computing, Encryption, Decryption.

I. INTRODUCTION

The growth of cloud computing persuades efforts for what's more, associations to outsource their data to outsider cloud service provider (CSPs),which will enhance the capacity impediment of asset oblige nearby gadgets. With the characteristics of data sharing provides better utilization of services and resources[1]. Provides security over user data by hiding their data information.Providing security to users data stored in cloud is become main constraint becoz users outsource their data[4]. User's data is protected as it will be stored in encrypted format but it is difficult for cloud to provide a secure storage structure for dynamic group of user in cloud as it is difficult to provide authentications.

Many schemes have been proposed to provide a secure data storage and retrieval schemes in system and provides authentication and secure group management system for cloud[5]. But any system of them can not provide security and efficient group user management.Kallahalla et al presented a cryptographic storage system that enables secure data sharing on untrustworthy servers based on the techniques that dividing files into file groups and encrypting each file group with a file-block key.Yu et al exploited and combined techniques of key policy attribute-based encryption, proxy re-encryption and lazy re-encryption to achieve fine-grained data access control without disclosing data contents[3]. For giving the respectability and accessibility of remote cloud store, a few arrangements, and their variations, have been proposed. In these arrangements, when a plan bolsters information alteration, call it element plan, generally static one (or restricted element plan, if a plan could just effectively bolster some predetermined operation, for example, affix). So propose a secure data sharing scheme and key distribution and group management.This system provide following mechanism for group sharing in cloud:Secure data sharing scheme provides effective key distribution

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 4, Issue 12, December 2016

without any secure channel user will get their secret keys from group manager [2].User in group can access all resources available in cloud but revoked user cannot access files or any resources in cloud. Private Key of that user does not need to update or recomputed.So provide a security analysis to prove the security of this scheme.

II. LITRATURE SURVEY

This system is of many user in group and access files among group, User of this group of system can may revoked or new user are added at any time so this cannot manage authentication of and many time new user cannot access files in cloud and user who revoked from group are accessing file. Once user is added in group it becomes permanent member of group so security concern occurs[1]. As owner of group stores file on cloud and cloud is semi trusted authority so files security on cloud cannot be ensure these files may be hacked or corrupted. Once owners file on cloud is lost then this file is lost permanently also there is no authentication of any key provider is provided to manage file uploads and file downloads [2]. It is also difficult to share files or resources among group members and also it is costly and require high maintenance[3.]Also an important issue is raise as how to control and prevent unauthorized access to data stored in the cloud[4]. System also does not have any efficient encryption technique to protect data of files on cloud[5]. If user who revoked and again want to join group then there is no such provision for joining group again.

III.DATA SECURITY

1. Data Confidentiality
Data confidentiality is that the property that knowledge contents aren't created offered or disclosed to extralegal users. Outsourced knowledge is hold on during a cloud and out of the owners' direct management. solely approved users will access the sensitive knowledge whereas others, as well as CSPs, shouldn't gain any info of the info. Meanwhile, knowledge house owners expect to completely utilize cloud knowledge services[2], e.g., knowledge search, knowledge computation, and knowledge sharing, while not the outpouring of the info contents to CSPs or different adversaries.

2. **Data Access Controllability**
Access controllability implies that information owner will perform the selective restriction of access to his data outsourced to cloud. Legal users are often licensed by the owner to access the info, whereas others cannot access it while not permissions. Further, it's fascinating to enforce fine-grained access management to the outsourced information, i.e., totally different users ought to be granted different access privileges with relevancy different information items[1]. The access authorization should be controlled solely by the owner in untrusted cloud environments.

3. **Data Integrity**
Data integrity demands maintaining and reassuring the accuracy and completeness of knowledge[6]. Information owner continuously expects that his data in a very cloud will be keep properly and trustworthily. It means the information mustn't be lawlessly tampered, improperly changed, deliberately deleted, or maliciously fictitious. If any undesirable operations corrupt or delete the information, the owner ought to be ready to observe the corruption or loss. Further, once some of the outsourced knowledge is corrupted or lost, it will still be retrieved by the information users.

IV.SCOPE

Scope of system is to provide services to cloud user by implementing an efficient anti collusion detection system for group of users who share files in cloud and also use resources in cloud .System manage all users in group and also user revocation. If any user removes from group then new user is added in group and all authority is provided to that user. Revoked user cannot access files or cannot share resources also.

V. CONCLUSION

In this paper, we design a secure anti-collusion data sharing scheme for groups in cloud.in our scheme group users can securely get key from data owner and can upload files. Also data owner can send files verification request to third party

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 4, Issue 12, December 2016

auditor and attribute authority challenge to cloud for verification. If file is hacked then file will regenerate from proxy. Our scheme is efficient to support dynamic groups smartly, when a new user joins in the group or a user is revoked from the group, the private keys of the other users do not need to be recomputed and updated. Also revoked user can reregister in group of cloud.

ACKNOWLEDGMENT

We might want to thank the analysts and also distributers for making their assets accessible. We additionally appreciative to commentator for their significant recommendations furthermore thank the school powers for giving the obliged base and backing.

REFERENCES

[1] Zhongma Zhu and Rui Jiang, "A Secure Anti-Collusion Data Sharing Scheme for Dynamic Groups in the Cloud" VOL. 27, NO. 1, JANUARY 2016
[2] E. Goh, H. Shacham, N. Modadugu, and D. Boneh, "Sirius: Securing remote untrusted storage," in Proc. Netw. Distrib. Syst. Security Symp., 2003, pp. 131–145.
[3] G. Ateniese, K. Fu, M. Green, and S. Hohenberger, "Improved proxy re-encryption schemes with applications to secure distributed storage," in Proc. Netw. Distrib. Syst. Security Symp, 2005, pp. 29–43.
[4] X. Liu, Y. Zhang, B. Wang, and J. Yang, "Mona: Secure multiowner data sharing for dynamic groups in the cloud," IEEE Trans. Parallel Distrib. Syst., vol. 24, no. 6, pp. 1182–1191, Jun. 2013.
[5] L. Zhou, V. Varadharajan, and M. Hitchens, "Achieving secure role-based access control on encrypted data in cloud storage," IEEE Trans. Inf. Forensics Security, vol. 8, no. 12, pp. 1947–1960, Dec. 2013.
[6] M. Nabeel, N. Shang, and E. Bertino, "Privacy preserving policy based content sharing in public clouds," IEEE Trans. Know. Data Eng., vol. 25, no. 11, pp. 2602–2614, Nov. 2013.
[7] M. Nabeel, N. Shang, and E. Bertino, "Privacy preserving policy based content sharing in public clouds," IEEE Trans. Know. Data Eng., vol. 25, no. 11, pp. 2602–2614, Nov. 2013.
[8] X. Zou, Y.-S. Dai, and E. Bertino, "A practical and flexible key management mechanism for trusted collaborative computing," in Proc. IEEE Conf. Comput. Commun., 2008, pp. 1211–1219.
[9] B. Dan and F. Matt, "Identity-based encryption from the weil pairing," in Proc. 21st Annu. Int. Cryptol. Conf. Adv. Cryptol., 2001, vol. 2139, pp. 213–229.
[10]Arti Arun Mohanpurkar, Madhuri Satish Joshi, "A Traitor Identification Technique for Numeric Relational Databases with Distortion Minimization and Collusion Avoidance" International Journal of Ambient Computing and Intelligence Volume 7 • Issue 2 • July-December 2016
[11] Arti Mohanpurkar, Madhuri Joshi, " The Effect of the Novel Anti-Collusion Fingerprinting Scheme on the Knowledge from Numeric Databases" International Journal of Scientific & Engineering Research, Volume 6, Issue 12, December-2015 ISSN 2229-5518
[12] Arti Mohanpurkar, Madhuri Joshi, " Fingerprinting Numeric Databases with Information Preservation and Collusion Avoidance" International Journal of Computer Applications (0975 – 8887) Volume 130 – No.5, November2015