ISSN: 2348-2079

FEB-2015

International Journal of Intellectual Advancements and Research in Engineering Computations

SECURING MULTI OWNER DATA SHARING THROUGH SECRET KEY GENERATION FOR DYNAMIC GROUPS IN THE CLOUD

[1]R.Gowthami, [1]S.Hemambika, [1]N.Jayaprakash, [1]B.Santhosh Kumar

ABSTRACT

Cloud computing provides an cost-effective and competent solution for sharing group resource among cloud consumers. Inappropriately, data sharing in a multi-owner manner while preserving data and identity privacy from an untrusted cloud is still a perplexing issue, due to the recurrent change of the participation. In this paper, we propose a secure multi owner data sharing scheme, named Mona, for dynamic groups in the cloud. With help of generating a unique secrete keys, it provides more security. Our ultimate aim is to provide more confidential access among the dynamic users. Meanwhile, the storage overhead and encryption computation cost are independent with the number of repealed users.

Index terms: Privacy preservation, Secret key generation, Revocation, Confidential access.

INTRODUCTION

Cloud Computing is new class of network based computing that takes place over the internet. It is an alternate to ancient data technology due to its core resource sharing and low-maintenance individualities. Cloud is operated by cloud a service provider which provides abundant storage services. However, the cloud is not fully trusted by users since the CSPs are very likely to be outside of the cloud users' trusted domain. It is based on utility and consumption of computing resources. It involves deploying groups of remote servers and software networks that allow centralized data storage and online access to computer resources or services in the cloud.

With the help of local data management users can access high quality services. The most basic service provided by cloud providers is data storage [2]. To preserve data privacy, encryption is one the mechanism that can be incorporated .Identity privacy is one of the most significant impediments for the wide distribution of cloud computing. It provides variety of services with the help of powerful data centers .Any members in the group should be able to access all data and avail the services provided by the cloud. There exist variations between single and multi owner scheme. In multi owner scheme group manager takes place a major role in providing services to the consumers. Dynamic users are involved in cloud, at the same time maintaining secure communication becomes a challenging issue.

Revocation mechanism involved to minimize the complexity of key management [3]. Group manager has to register their existence and will handle list of authorized users. The consumers need to register and can avail the needed services in a secured manner. Once the users have been registered, the secret key generation will takes place. With the help of secret key, the requested file can be downloaded for their purpose. The secret key will be generated only for the requested files and it can be modified. Multi owner scheme named Mona provide secure and private access dynamically. Group manager is a centralized authority capable of providing any services to users [4]. Once the users are registered under group manager, the unique id

Author for Correspondence:

[1]Final year B.E. CSE, Department of CSE, SNS College Of Technology, Coimbatore, India, gowthami.feb24@gmail.com

will be provided for all users. In some cases users might be unwilling to hitch in cloud computing systems because their real identities could be disclosed to attackers.

EXISTING SYSTEM

To preserve data privacy, a basic methodology is to do file encryption, and after that upload the encrypted data into the cloud. Tactlessly, designing an optimistic solution for sharing data among dynamic users is not an easy assignment. Data owners store the encrypted data files in untrusted storage and will provide corresponding decryption keys only to the users who have been authenticated. So the unauthorized users as well as cannot learn the content of the data files because they don't have any authorized mechanism to access the encrypted files . The complexities increase in proportion with increase in the no of dynamic users. Only the group manager can store and modify data in the cloud. The changes of membership the secure data sharing is extremely difficult [7]. The dispute of user revocation is not addressed.

PROPOSED SYSTEM

We propose a secure multi-owner data sharing scheme. It entails that any user in the group can securely share data with others .It support dynamic groups efficiently [2]. Precisely, new granted or authorized users can directly decrypt the files before their participation. User revocation can be easily accomplished through a novel revocation list without updating the secret keys of the remaining users [5]. The computation overhead of encryption is constant and independent with the number of revoked users. Multi owner scheme provides privacy-preserving access control to users, which guarantees that any member can properly utilize the cloud resource.

MODULE DESCRIPTION

a. REGISTRATION

Group manager takes major role in generating system parameters, user registration, user revocation and revealing the real identity of data owner. The group manager has to register first and has the control over other users [3].The users of cloud resources has to register under the group manager and unique identity .The unique identity will be updated for each users. Group manager is coordinating all works.

b. CREATION OF DYNAMIC GROUPS

The registered users who are collectively known as group members can decrypt the files through authorization process. The number of users under certain group depends on the group manager. The users are instructed under the guidance of group manager. The group manager will be created by the administrator, and group manager have all access control mechanisms.

c. KEY DISTRIBUTION

After the creation of dynamic group, secret key will be generated to access the file. The secret key will be unique for each file and with the help of that secret key the respective files can be downloaded.

d. USER REVOCATION

The user can leave the group which is controlled by group manager without any issue. once the user leaves the group, their unique identity will be removed and preventing from accessing the resources [6].

CONCLUSION

In this paper, we design a multi owner data sharing for dynamic groups in the cloud. In Mona, secret key will be generated for secured data access. User revocation can be done without any changes or updation in the private key of the remaining users. Group members who are all the set of authorized users can decrypt the files with the help of secret key. Extensive analysis shows that our proposed scheme satisfies the desired security and guarantees efficiency.

Copyrights © International Journal of Intellectual Advancements and Research in Engineering Computations, www.ijiarec.com

REFERENCES

[1]. C.Wang, Q.Wang, K. Ren, and W. Lou, "Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing, "*Proc. IEEE 29th Int'l Conf. Computer Comm. (INFOCOM),* pp.525-533, 2010.

[2]. B. Wang, B. Li, and H. Li, "Knox: Privacy-Preserving Auditing for Shared Data with Large Groups in the Cloud," Proc. 10th Int'l Conf. Applied Cryptography and Network Security, pp. 507-525, 2012.

[3]. M. Armbrust, A. Fox, R. Griffith, A.D. Joseph, R.H. Katz, A. Konwinski, G. Lee, D.A. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, "A View of Cloud Computing," Comm. ACM, vol. 53, no. 4, pp. 50-58, Apr. 2010.

[4]. D. Naor, M. Naor, and J.B. Lotspiech, "Revocation and Tracing Schemes for Stateless Receivers," Proc. Ann. Int'l Cryptology Conf, Advances in Cryptology (CRYPTO), pp. 41-62, 2001.

[5]. R.Kalaiselvi,"Secure data sharing for dynamic and large groups in the cloud", Proc, *IEEE 29th Int'l Conf. Computer Comm. (INFOCOM),* pp.505-538, 2010.

[6]. M V Rajesh1, Soma Sekhar and Siva Rama Krishna, "Enhanced Secure Data Access Model for Public Clouds "Issue-1, Volume-1, 039-045.

[7]. Ayad F. Barsoum and M. Anwar Hasan "Enabling Data Dynamic and Indirect Mutual Trust for Cloud Computing Storage Systems" Issue-1, Volume-1, 035-049.

Copyrights © International Journal of Intellectual Advancements and Research in Engineering Computations, www.ijiarec.com