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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 12, December 2015

A Survey on Privacy Preservation and Sharing Data Securely in Data Storage

Pooja Yedave, Reshma Shinde, Ashwini Mahajan, Shubhangi Bhor , Rupesh Mahajan

B.E. Students, Dept. of I.T, Dr .D. Y. Patil college of Engineering, Pimpri, Pune, India

Professor, Dr .D. Y. Patil college of Engineering, Pimpri, Pune, India

ABSTRACT : A secure multi-owner data sharing technique is proposed which is used for dynamic groups in the server. The fundamental service provided by the server is Data Storage that is increasingly more customers are starting to utilize server to online datastore and share. But because of the frequent change of the membership sharing data become a very difficult task. Therefore we propose secure data sharing for dynamic groups by combining group signature and dynamic encryption techniques. We also use DBE algorithm to improve performance of the system in terms of security. This guarantee any member can anonymously share the server resources. The major aims of this system a secure multi-owner data sharing theme. User revocation are merely achieved whereas not modification of the key. Keys of the remaining users the computation overhead of cryptography area unit constant with the quantity of revoked users. It provides on-demand, high scalability computing resources with greater availability and reliability. security is considered as one of the biggest obstacles for server computing. In this paper, we focus on the main security and privacy issues, to store and share data on untrusted server storage. We have investigated several existing approaches focused on security concerns in server.

KEYWORDS: Multi owner, cluster manager, revocation, Security, group signature, dynamic broadcast encryption,privacy-preserving, KP-ABE, auditing, access control .

I. INTRODUCTION

Nowadays, secure data storage is becoming a good solution for organizations that suffer from resource limitation.The service provider (SP) offers to the users the opportunity to get unlimited storage capacities, which is billed based on theactual amount of consumed resources [1]. Itoffers high scalability, redundancy and recoverycapabilities. It gives an opportunity toimprove security and privacy where data storage data aremaintained within a server, which can be reliable andfaster to restore data more the traditional data center[2]. The problem of user revocation is not addressed in their fine-grained knowledge access management theme in server computing supported the key policy attribute-based encoding (KP-ABE) technique .Sadly, the single owner manner stop the adoption of their theme into the case, any user is granted to store and share knowledge.

Our contributions to resolve the challenges mentionedabove, we have a tendency to propose Anglesey, a secure multi-owner knowledge sharing theme for dynamic teams within the server. The main contributions of this paper include:

1. We have a tendency to propose a secure owner knowledge sharing scheme. It implies that any user within the cluster will securely share knowledge with others by the untrusted server.
2. Our projected theme is in a position to support dynamic groups with efficiency. Specifically, new users can directly rewrite knowledge files uploaded before their participation while not contacting with knowledge house owners. Revocation may be simply achieved through a novel revocation list while not change the key keys of the remaining users.
3. We offer secure and privacy-preserving access control to users that guarantees any member during a group to anonymously utilize the server resources.

A basic solution provided by existing system is to ensure data security is encrypting the data files, before uploading into the server. But unfortunately designing a secure and efficient data sharing scheme for dynamic groups in the server is not simple task because of the some difficult issues are following:

A. Identity Privacy: The major problem for the wideadoption of server computing is Identity Privacy. Serverusers may be doubtful to join server based computingsystems without the assurance of identity privacybecause if Users privacy

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 12, December 2015

does not maintained properlythen the actual identities of the user can be disclosedeasily to the various kinds of intruders and service providers (SP).

B. No Multiple-owner Manner: Multiple-owner manner ismore secure than single owner manner becausemultiple owner manners allow every member in thegroup should be able to change their own data i.e. everymember able to not only read the data but also modifyhis part of data in the whole data file, whereas singleowner manner allow only group manager to store andmodify data in the server and members can only readthe data.

C. Effect of Effective Groups: The joining of new staff andrevocation of current employee makes the groupeffective in nature. The frequent alterations ofmembership make efficient and secure data sharing in Server.
Section II will give a brief review of all the concernedreference papers. It will give a brief discussion of the othercontributors and their solutions. Section III. will describe theproposed system and implementation details. Section IV. will give the Analysis on the entire paper.Finally, section V. Concludes this paperby summarizing the key points and other relatedwork.

II.LITERATURE SURVEY

Literature survey is the most important step in softwaredevelopment process. Below points is the literature survey ofsome existing technique.

A. Cryptographic Data Storage
In [2], files stored on the untrusted server involved two parts: file metadata and file data. The file metadata implies the access control information involving a list of encrypted key blocks, each of which is encrypted under the public key of authorized users.
The size of the file metadata is proportional to the number of authorized users. The user revocation in the system is an intractable issue especially for large-scale sharing, since the file metadata needs to be updated.

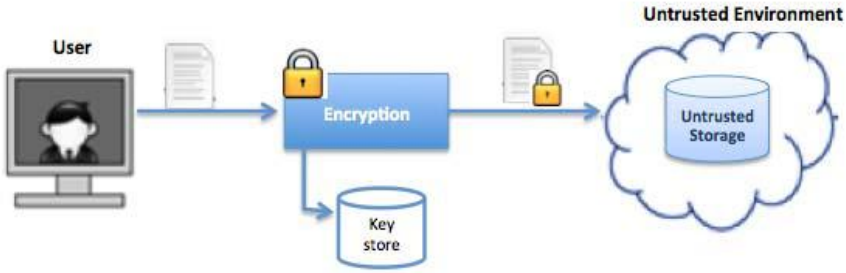

Fig 1: Architecture of secure data storage

*B.Improved Proxy Re-Encryption Schemes withApplications to Secure Distributed Storage***.**
M. Kallahalla et al. [2] proposed cryptographic storagesystem which is known as Plutus. Plutus enables secure filedistribution on untrusted server by using client based keydistribution. Plutus allow client to handle all the keymanagement and participationoperations. As compare toclient, Server incurs very little cryptographic overheadbecause Plutus does not place much belive on server, iteliminate almost all requirement of server trust.
Ateniese et al. [4] leveraged proxy reencryptions to secure distributed storage. specifically, the data owner encrypts blocks of content with unique and symmetric content keys, which are further encrypted under a master public key..

C. Achieving Secure, Scalable, and Fine-Grained Data Access Control
Yu et al. [5] offered a scalable and fine-grained data accesscontrol scheme by defining access polices based on dataattributes and KP-ABE technique. The combination ofattribute-based encryption (ABE), proxy re-encryption andlazy re encryption permit the data owner to assign thecomputation tasks to untrusted server without revealing thenecessary contents of data.

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 12, December 2015

III.PROPOSED SYSTEM

In our proposed system there is an efficient and secure approach for storing data over server for dynamic groups. Also, it support efficient user revocation and submission of dynamic groups.Compared toexisting work our proposed system provide some unique
features such as
a) Any group member able to store and share datafiles with others within a group.
b) This system support dynamic group efficiently. Itimplies that new user joining and user revocationare easily achieved without involving remainingusers.
c) This system provides rigorous security using AESencryption technique.

The system model consists of three different entities:
- The server
- A group manager (i.e., Admin)
- A large number of group members.

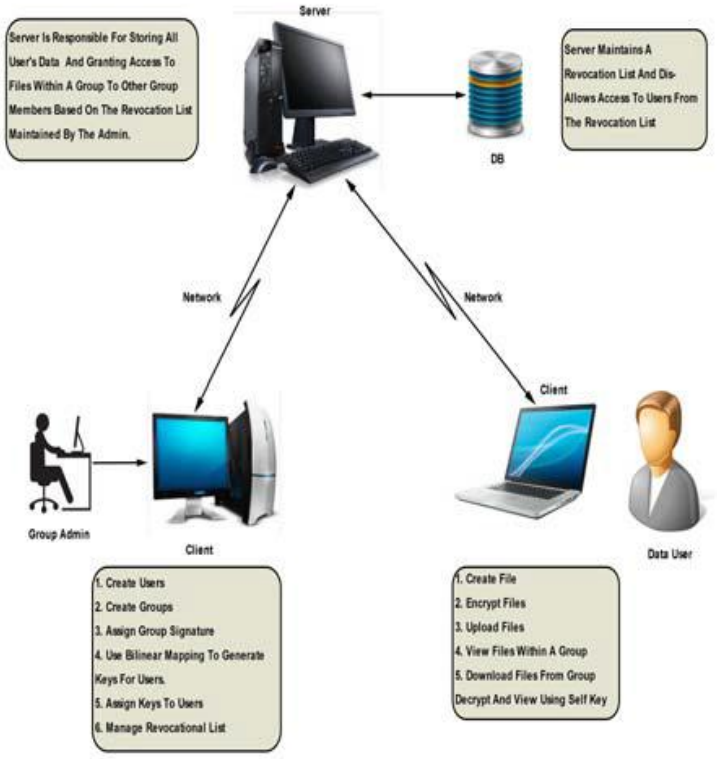

Fig 2 : Architecture of data Sharing Scheme.

IV.SIMULATION RESULTS

There are various techniques/scheme for securing data over server for dynamic groups in server. From paper[1] SaaS i.e software as a service and utility computing has been used since it offer service below the cost of medium size datacenter. But in this paper they had focus only on application software which needs to scale up and down more rapidly to match needs of server computing.
Two encryption scheme has been given in paper[2]. Properties of both the encryption scheme is used for securing data over server for dynamic groups. KP-ABE scheme[3] is being used for securing data over server for dynamic groups.

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 12, December 2015

But, in this paper KP-ABE is combined with proxy re-encryption and lazy re-encryption scheme. So, because of re-encrypting the data the time consumption will be more.

Secure provenance scheme[7] is being used for securing data over server for dynamic groups. Provenance scheme is used for data forensics to provide digital evidence for post investigation. But in this paper it does not support user revocation.

Broadcast encryption technique[16] is used to transit encrypted data to a set of users. Using this technique only a priviledge subset of user can decrypt the data. Also, it allows group manager to include new members and its information dynamically. But in this paper random resiliency scheme is used which works only for expected no. of users.

V.CONCLUSION AND FUTURE WORK

In this paper, focuses onthe security issues related to share and store data onuntrusted service provider. Basically, to increase user trust in using data storage, SP should provide a complete security guarantee to the data throughout the entire process from the owner to the data storage, and then to authorize users. Therefore, when the owner store data on data storage, the data have to stay private, and the owner should has the control on the data access and share.

In this paper, we survey several existing techniques and classify them based on three categorizes, which are: encryption and key management approaches, searching over encrypted data and access control schemes.

We conclude that to enhance the security, and enjoy the benefit,there is a need to provide asstrong- as-possible mechanisms, without heavycomputation overhead on the data owner. Moreover, thesolutions should take consideration of the performanceand pay attention to the speed of searching and decryptingsince the amount of data in the database is huge, whereas thetechnique will be inefficient if it takes too long time toretrieve data to users. Finally, we presented in this surveythe limitations and challenges that requiring futureresearches to handle them.

REFERENCES

1. Xuefeng Liu, Yuqing Zhang, Boyang Wang, and Jingbo Yan,"Mona: Secure Multi-Owner Data Sharing for Dynamic Groups inthe Cloud", IEEE TRANSACTIONS ON PARALLEL ANDDISTRIBUTED SYSTEMS, VOL.24, NO. 6, JUNE 2013
2. M. Kallahalla, E. Riedel, R. Swami Nathan, Q. Wang, and K.Fu,"Plutus: Scalable Secure File Sharing on Untrusted Storage," Proc.USENIX Conf. File and Storage Technologies, pp. 29-42, 2003.
3. E. Goh, H. Shacham, N. Modadugu, and D. Boneh, "Sirius:Securing Remote Untrusted Storage," Proc. Network and DistributedSystems Security Symp. (NDSS), pp. 131-145, 2003
4. G. Ateniese, K. Fu, M. Green, and S. Hohenberger, "Improved ProxyRe-Encryption Schemes with Applications to Secure DistributedStorage," Proc. Network and Distributed Systems Security Symp.(NDSS), pp. 29-43, 2005
5. S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving Secure, Scalable,and Fine-Grained Data Access Control " Proc.IEEE INFOCOM, pp. 534-542, 2010.
6. R. Lu, X. Lin, X. Liang, and X. Shen, "Secure Provenance: TheEssential of Bread and Butter of Data Forensics .Computing," Proc. ACM Symp. Information, Computer and Comm.Security, pp. 282-292, 2010
7. Yong CHENG, Jun MA and Zhi-ying "Efficient revocation incipertext-policy attribute-based encryption based cryptographic cloudstorage" Zhejiang University and Springer-Verlag Berlin 2013.
8. B. Wang, B. Li, and H. Li, "Knox: Privacy-Preserving Auditing forShared Data with Large Groups in the Cloud," Proc. 10th Int'l Conf.Applied Cryptography and Network Security, pp. 507-525, 2012

BIOGRAPHY

Ashwini Mahajan ,Reshma Shinde, Pooja Yedave, Shubhangi Bhor are pursuing B.E. degree in Pune University.They are working on project named New approach for anonymous data sharing using access control. The results also confirmed the effectiveness and efficiency of our solution.