International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Impact Factor (2012): 3.358

# Literature Review on: Secure Sharing of Data for Dynamic Groups in Cloud

**Shazadi Fatima Rizvi[1], A. N. Jaiswal[2]**

[1] Department of CSE, G H Raisoni Institute of Engineering and Technology for Women RTMNU, Nagpur, MH, India

[2]Professor, Department of CSE, G H Raisoni Institute of Engineering and Technology for Women RTMNU, Nagpur, MH, India

**Abstract:** ***Cloud computing is an emerging computing paradigm aiming to share storage, computation and service transparently among a massive users and to gathered great momentum from not only industry but also academia. Clod computing had overlaps many existing concepts such as distributed system. Data security is the challenging issue in cloud computing paradigm where the user store sensitive information on cloud servers. Also, data confidentiality against cloud server is required, when users outsource data for storage in the cloud. Existing solutions generally use cryptographic methods like encryption and decryption. The biggest concerns with cloud data storage is that of data integrity verification at untrusted server. To preserve data privacy, a basic solution is to encrypt data files, and then upload the encrypted data into the cloud. By adding the reliability as well as improving the scalability by increasing the number of group managers dynamically we can secure multi-users data sharing for dynamic groups in the cloud.***

**Keywords**: Cloud Computing, dynamic groups, data sharing, reliability, integrity, Scalability, KP-ABE. Privacy preserving, auditing

## 1. Introduction

As cloud computing is emerging there is a lot of resource-sharing services provided by the cloud service providers (CSPs) such as Amazon's EC2. Google App Engine and Microsoft Azure provide users with scalable resource in the pay-as-you-use fashion at relatively low price. With the help of powerfull data-centers cloud service providers provide various services to cloud users. Data Storage is one the service provided by cloud service providers. Cloud computing is also being used in academia and industry. Cloud computing includes various type of services such as infrastructure as service (IaaS) where customer make use of a service provider's for storage and for infrastructure, Platform as a service (PaaS), where a customer leverages the provider's resources to run custom applications, and finally software as as a service (SaaS), where customer use software that run the provider's infrastructure [2].

Cloud computing also bring many new challenges for data security and access control when users outsource sensitive data for sharing on cloud servers,.. In cloud computing to achieve secure, scalable and fine grain data access control a technique [3] named attribute-based encryption (ABE), proxy re-encryption, and lazy re-encryption are combined uniquely. Also, the secure provenance scheme [7] in cloud computing provide sensitive documents which is highly confidential and stored in cloud, along with anonymous authentication on user access and provenanace tracking on dispute documents. This scheme is used for data forensic in cloud computing. To make cloud computing efficient group signature technique[12] is used in MONA scheme. To transmit encrypted data to a set of user broadcast encryption[16] technique is used so that only privileged user can decrypt the key.

This paper is organized as follows: Various techniques and literature survey are discussed in section I, proposed scheme is discussed in section II, comparative analysis of different techniques or scheme is conducted in section III and section IV gives conclusion.

## 2. Review of Literature

### A. A View of Cloud Computing

In this paper [1] author had defined cloud computing as application which provide service over an internet and the datacenters hardware and software which provide those services. In this paper cloud is datacenters made of hardware and software. When cloud is available in pay-as-you go bases then it is made available to public and it is called public cloud, whereas we refer private cloud as internal datacenters of some organization or a business, this is not available to general public. Cloud computing is the sum of SaaS i.e software as a service and utility computing. Cloud computing can offer services below the cost medium-size datacenters. In cloud computing people can be users or providers like utility computing. In this paper they given there more focus in application software which needs to scale up and down more rapidly to match needs of cloud computing. Also, infrastructure software needs to be aware that it will no longer run on bare metal but can be run on VMs. And lastly hardware machine should be designed in such a way that its purchasing cost is low.

### B. Cryptographic Cloud Storage

In this paper [2] author had considered a problem of building a secure cloud storage service on top of public cloud infrastructure where the service provider does not trust the customer. In order to achieve our goal they had describe several architecture that combine non-cryptographic primitives. Two encryption scheme has been described in this paper i.e searchable encryption scheme and attribute based encryption scheme. Searchable encryption scheme is a method to encrypt a search index so that its data is hidden from the adversary and is known only to the party who has token. Search index is generated with the help of collection of files. In attribute-based encryption scheme each user is having a decryption key along with the set of attributes.

Decryption is performed only if the attributes associated with the decryption key will match the encrypted message.

### C. Achieving Secure, Scalable, and Fine-Grained Data Access Control in Cloud Computing

In the paper [3] author had used key-policy attribute based encryption technique. This technique is combined with proxy re-encryption and lazy encryption technique. With the help of KP-ABE technique we can access fine-grained data access control and can do the efficient operation such as file creation/deletion and can also grant new user. When proxy re-encryption technique is combined with KP-ABE we can resolve the issue of user revocation. With the help of this data owner can delegate their computational task to cloud servers. Cloud server keep a partial copy of each user having a secret key. When there is a need of user revocation the data owner re-defines a certain set of attributes along with proxy re-encryption keys and sends them to cloud servers. When these proxy re –encryption keys is received to cloud server it update user secret key components and again re-encrypt the data files without knowing the plaintext of data files. This improvement releases the data owner from the huge computational overhead on user revocation. To degrade the computational overhead from cloud server on user revocation, we use technique of lazy re-encryption. Using lazy re-encryption, cloud server will aggregate multiple successive secret key and then update file re-encryption operations into one, and thus statistically save the computational overhead. Thus, confidentiality of user access privilege and user secret key accountability can be achieved.

### D. Secure Provenance: The Essential of Bread and Butter of Data Forensics in Cloud Computing

In the paper [7] author had construct a new secure provenance scheme based on bilinear pairings technique to provide trusted evidence for data forensics in cloud computing. The scheme provide confidential information on sensitive documents which is stored in cloud. If a provenance is given then the given data objects can report who created it and who modified its contents. Provenance is mostly used in data forensics to provide digital evidence for post investigation. Also, when a dispute occur in a document stored in a cloud provenance is required. Secure provenance scheme can guarantee the confidentiality of the information, anonymous authentication, authorization access and provenance tracking. Secure provenance scheme can be used for data forensics in cloud computing. As documents are normally stored in cloud, the main issue is privacy. If any dispute occur the service provider will provide all provenance information related to all version of the documents to system manager. Then with the help of provenance tracking algorithm the system manager will plot a visible provenance chain to track the specific user identity. Also, group signature and ciphertext policy attribute based technique is used to built a secure provenance scheme. The system used in this scheme is set with a single attribute, here each user obtain two keys after registration i.e group signature key and an attribute key. User revocation is not supported in this scheme.

### E. Short Group Signature

In the paper [12] author had construct short group signature scheme this means that the computation time taken to complete the task is very less. Group signature is a method for allowing a member of a group to anonymously sign a message on behalf of the group. Group manager has the ability to reveal the original signer in the event of disputes. These group signature are a generalization of credential/membership authentication schemes, in which one person prove that he belong to certain group. Security of a group signature is based on strong deffie-hellman assumption. In bilinear groups there is a new assumption called decision linear assumption. Random oracle model is used to provide security. Short group signature scheme length is below 200 bytes and it provide approximately same security to that of RSA signature length. Strong deffie-hellman was constructed without random oracle. In this they had also make use of zero- knowledge proof of knowledge protocol to provide solution to strong deffie-hellman problem. With the help of Fiat-shamir heuristic algorithm signature scheme will be secure under random oracle model.There are three properties that a group signature scheme must satisfy

1. Correctness
2. Full-anonymity
3. Full-traceability

Correctness ensure that the signature generated must be verified and trace correctly. Full-anonymity ensure that the signature do not reveal their signer's identity. And full-traceability ensure that all signatures, even those created by the collusion of multiple users and the group manager, trace to a member of the forging coalition. Using these properties they had proves the security of group signature. Revocation mechanism has been used for a group signature. In this revocation list is given to all user in the group. Revocation list contain private keys of all revoked user. It is used to update the group public keys which is used to verify signatures.

### F. Broadcast Encryption

In this paper [16] author had introduce new theoretical measures for broadcast transmission. They had designed qualitative and quantitative assessment of encryption scheme. In this paper they had present several scheme which allow center to broadcast secret key to any subset of privileged user which does not come in the universe of size n so that coalitions of K users which is not in the privilege set cannot learn the secret key.

## 3. Proposed Scheme

In our proposed system there is an efficient and secure approach for storing data over cloud for dynamic groups. Also, it support efficient user revocation and submission of dynamic groups in cloud computing. Group signature scheme has been used in our proposed system. By using it any member in our group is allowed to sign the message without revealing its identity. While assigning new users and revoking old users the key structure and file structure should not be changed for other users. Efficient user revocation can be achieved through a public revocation list without updating the private keys of the remaining users, and new users can directly decrypt files stored in the cloud before their participation. And by using broadcast encryption technique group manager can dynamically include new member while preserving previously computed information.

Moreover, the storage overhead and the encryption computation cost are constant.

## 4. Comparative Analysis

There are various techniques/scheme for securing data over cloud for dynamic groups in cloud. 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 cloud computing.

Two encryption scheme has been given in paper[2]. Properties of both the encryption scheme is used for securing data over cloud for dynamic groups.

KP-ABE scheme[3] is being used for securing data over cloud for dynamic groups. 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 cloud 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.

Group signature scheme[12] provide anonymity for signers. Also, group manager have a capability to find dispute when it occur. Also, revocation mechanism is been used to update the private key of the revoked users. But in this paper signature generation and verification require a few exponentiations with short exponents.

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.

## 5. Conclusion

Thus in the proposed system user is able to share data with others in the group without revealing identity privacy to the cloud. Also, the proposed system will reduce the development cost and storage and execution overhead. It also supports efficient user revocation and new user joining.

## References

[1] Xuefeng Liu, Yuqing Zhang, Boyang Wang, and Jingbo Yan. “Mona:Secure Multi-Owner Data Sharing for Dynamic Groups in the cloud” IEEE transaction on parallel and distributed systems, vol. 24, no.6, june 2013.
[2] 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.
[3] S. Kamara and K. Lauter, “ Cryptographic Cloud Storage,” Proc. Int’l Conf. Financial Cryptography and Data Security (FC), pp. 136- 149, Jan. 2010.
[4] S. Yu, C. Wang, K. Ren, and W. Lou, “Achieving Secure, Scalable, and Fine-Grained Data Access Control in Cloud Computing,” Proc. IEEE INFOCOM, pp. 534-542, 2010.
[5] R. Lu, X. Lin, X. Liang, and X. Shen, “Secure Provenance: The Essential of Bread and Butter of Data Forensics in Cloud Computing,” Proc. ACM Symp. Information, Computer and Comm. Security, pp. 282-292, 2010.
[6] D. Boneh, X. Boyen, and H. Shacham, “Short Group Signature,”Proc. Int’l Cryptology Conf. Advances in Cryptology (CRYPTO), pp. 41-55, 2004.
[7] A. Fiat and M. Naor, “Broadcast Encryption,” Proc. Int’l CryptologyConf. Advances in Cryptology (CRYPTO), pp. 480-491, 1993.