Impact Factor (SJIF): 5.301

International Journal of Advance Research in Engineering, Science & Technology

e-ISSN: 2393-9877, p-ISSN: 2394-2444

Volume 5, Issue 3, March-2018

PRIVACY PROTECTION FOR SHARED DATA WITH MULTI-USER IN CLOUD

S. Panimalar[1], Surneni Rajeev[2], G. Vamsi Krishna[3], Nimmagadda Yogesh[4]

Associate Professor, Department of CSE, Panimalar Institute of Technology, Chennai, Tamil Nadu, India[1]

panimalarjerome@gmail.com[1]

Student, Department of CSE, Panimalar Institute of Technology, Chennai, Tamil Nadu, India[2,3,4]

surnenirajeev241@gmail.com[2], victory.vamsi99@gmail.com[3], 1996yogeshnimmagadda@gmail.com[4]

Abstract: - Cloud computing is an emerging computing premise in which consists of a virtualized pool of highly scalable computing resources and provided as an internet-based computing where many organizations store, reacquire and modify data among cloud users. Auditor place main role of monitoring the data transmission and data manipulations between the data owner and server. Load Balancing is also implemented to process the User requested job by allocating to the sub servers which will process the task by evaluating the CPU performance level. We introduced a secure and efficient dynamic auditing protocol by using the File segmentation and distribution, Tag generation, and Random Challenge and verification algorithms.

Keywords: Cloud Computing, Data Security, AES, Attribute Based Encryption Techniques, Auditing.

I. INTRODUCTION

Cloud computing is a wide-ranging term that transmits hosted services over the internet and recognized as an alternative to traditional information technology due to its intrinsic resource-sharing and low-maintenance characteristics. One of the most fundamental services offered by cloud providers is data storage. Owners would worry that the data could be lost in the cloud. This is because loss of data might happen in any software or hardware and it cannot consider what high degree of reliable measures cloud service providers.

By utilizing cloud, students and other employees can get relevant information on a request basis. However, it poses some confidentiality risks. The cloud service provider or third party may not fully trusted by the users. A possible approach would be to encrypt entire data files before outsourcing in order to achieve more integrity. Unfortunately, scheming an effective and protected data sharing scheme for groups in the cloud is not an easy task due to the subsequent challenging issues.

However, it is due to the huge number of data tags, their examining protocols may tolerate a substantial storage overhead on the server. Zhu et al. proposed a cooperative verifiable data possession scheme that can support the batch auditing for several clouds and also extend it to support the energetic auditing [1]. This is for parameters for generating the data tags used by each owner are different and thus they cannot association the data tags from numerous owners to conduct the group auditing.

II. RELATED WORK

Cloud Computing is presently one of the hottest topics in information technology (IT). Since the outsourcing of all the essential data is available with a third party, there is always having a concern of cloud service providers trustworthiness. Due to data privacy, it is essential for users to encrypt their sensitive data before storing them into the cloud [2]. The study of secure data sharing in the Cloud is fairly new and has become increasingly important with the advancements and growing popularity of the Cloud as well as the growing need to share data between people. We categorize the existing review articles in two aspects: data sharing and Cloud security [3].

To ensure security in distributed storage. Specifically, the data owner encrypts blocks of content with unique and symmetric. Yu et al. presented a scalable and fine-grained data access control scheme in cloud computing based on the key policy attribute-based encryption (KP-ABE) technique [4].

Lu et al proposed a secure derivation scheme, which is assembled upon assembly signs and cipher text-policy attribute-based encryption techniques. Each user obtains two keys after the registration: a group signature key and an attribute key. Thus, any user is able to encrypt a data file using attribute-based encryption and others in the group can decrypt the encrypted data using their attribute keys. However, user revocation is not supported in their scheme

III. EXISTING MECHANISM

Numerous security systems for data sharing on untrusted servers have been suggested. Here, the data owners manage the encrypted data files in untrusted storage and give out the corresponding decryption keys only to specific users. Accordingly, illegal users as well as storage servers cannot learn the content of the data files because they have no idea of the decryption keys. On the other hand, unconditional identity privacy may acquire the mishandling of privacy.

3.1. Drawbacks of Existing Method

1) The variations of membership make secure data sharing enormously challenging the issue of consumer revocation is not addressed.
2) Only the group manager can store and modify data in the cloud.
3) Identity transparency is not preserved for distribution of a file in cloud group.

IV. PROPOSED WORK

This paper recommends an advanced approach for protected multi-owner data sharing scheme for dynamic groups in the cloud computing [5]. It can be attained by a technique called Attribute Based Encryption (ABE) in which each data files can be encrypted along with attributes related to the data file.

4.1. Group Signature

In a group signature key allows any member of the group to sign messages while keeping the identity secret from verifiers. Alternative side the nominated group manager can expose the identity of the sign's originator when a argument occurs, which is denoted as traceability.

4.2. Dynamic Broadcast Encryption

It permits a presenter to transmit encrypted data to a set of users so that only a honored subset of users can decrypt the data. The initial proper description and creation of dynamic broadcast encryption are presented based on the bilinear pairing technique, which will be used as the source for file sharing in dynamic groups.

V. SYSTEM MODEL AND SCHEME DESCRIPTION

5.1. System Model

System model comprises of three entities i.e., the cloud, a group manager and a number of group members. The users are not entirely trusted on cloud. But the cloud server will not erase or alter user data which is stored on cloud due to numerous security techniques. Group members are a set of authorized users that will store their secretive data into the cloud server and share them with others in the group.

5.2. Scheme Description

5.2.1. Bilinear Map

Let $G1$ and $G2$be an additive cyclic group and a multiplicative cyclic group of the same prime order q, respectively. Let e:$1*G1 \rightarrow G2$ denote a bilinear map constructed with the following properties:

1. Bilinear: For all a, b $\epsilon Zq*$ and P, Q ϵ $G1$, e(aP, bQ)=e$(P,Q)ab$.
2. Non-degenerate: There exists a point P such that e(P,P)≠1.
3. Computable: There is an efficient algorithm to compute e(P,Q) for any P,Q$\epsilon G1$.

5.2.2. Cloud Server

Generate a native Cloud and offer plentiful storage services. The users can upload their data in the cloud. We develop this module, where the cloud storage can be made secure. By accessing cloud user can share data to each other.

5.2.3. Group Members

Group members are a set of authorized users that will store their isolated data into the cloud server and share them with others in the group. After effective connection of cloud, users must have to register with their private details like name password, email id, etc. Once the process completes admin send the signature key after preserving identity privacy.

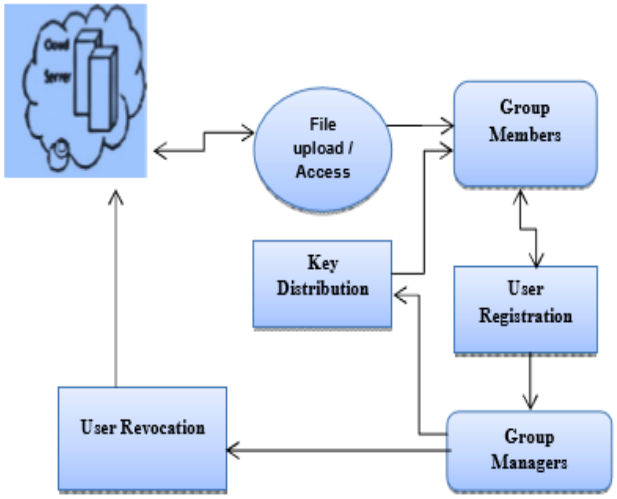

Fig.1 System Model

5.2.4. Group Manager

Group manager takes control of User registration, System constraints generation, User revocation and revealing the real identity of a argument data owner. The Group manager is the administrator. He used to store, share and manage data files stored in the cloud. He is also responsible for granting new users to access and improve cloud performance based on a request from them. The group manager is accountable for user registration and also user revocation.

5.2.5. File Security

Encrypting the data file and file stored in the cloud can be removed by either the group manager or the data owner [6]. It means that the files stored on cloud are encoded form. File can be erased by user who have file signature key. And this key should belongs only to data owners as well as group manager.

5.2.6. Key Distribution

Means of issuing secret keys by the group manager. Using public key cryptography and exchange of session keys that are effective only if the group members are not cancelled from the group. Key can be updated by creating new key from an old key.

5.2.7. User Revocation

User revocation is executed by the group manager through a public accessible revocation list (RL), based on which group members can be privacy against the revoked users. It means that if user is withdrawn then they cannot access to it. The system sustains revocation list for each attribute. Revocation is the process of removal of user.

5.3. Load Balancing

The users defer to their various claims to the Cloud Service Provider through a communication channel. The requirements from the users are queued up under the Cloud Service Providers Data Center. The sub servers are then patterned up for the minimum load with the CPU performance level of the presently executing task. The Cloud Service Provider then assigns the demanded job to the sub servers that has minimum load to process the task in a First In First Out (FIFO) manner. Thus, the User requested job will be assigned to the available sub server which contains minimum load and it is concerned to process the User requested job. The objective is to provide secure data storage, to maintain integrity of the data, to increase the user level of authentication and to improve the performance efficiently by 70-80% of balancing the load [7].

VI. DESIGN GOALS

This section describes the main design goals of the proposed scheme as follows:

6.1. Access Control

The requirement of access control is twofold. First, group members are able to use the cloud resource for data operations. Secondly, the unofficial users cannot access the cloud resource at any time, and revoked users will be incapable of using the cloud again once they are revoked.

6.2. Data confidentiality

An important and stimulating issue for data confidentiality is to sustain its accessibility for dynamic groups. Specifically, new users would decrypt the data stored in the cloud before their involvement, and cancelled users are unable to decrypt the data moved into the cloud after the revocation.

6.3. Anonymity and traceability

Anonymity assurances that group members can access the cloud without revealing the real identity. Although anonymity signifies an effective safety for user identity, it also possess a potential inside attack risk to the system.

6.4. Efficiency

The remaining users do not need to inform their isolated keys or re-encryption operations. User revocation can be attained without including the remaining users. Any group associate can store and segment data files with others in the cluster by the cloud.

VII. CONCLUSION

In this paper, introduced an efficient novel dynamic auditing protocol for secure multi-owner data sharing for dynamic groups in an untrusted cloud. In this scheme, a user is able to share data with others in the group without revealing individuality secrecy to the cloud. Efficient user cancellation can be attained through a public revocation list without updating the isolated keys of the remaining users, and new users can straightly decrypt files stored in the cloud before their contribution. The protocol permits the auditor to displays the data component meta information only that offers the abstract information of the data component. Data owner can obtain the consistent monitoring details.

VIII. REFERENCES

1. Qian Wang, Cong Wang, Kui Ren, Wenjing Lou and Jin Li, “Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing” - IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 22, NO. 5, MAY 2011.
2. Zhangjie Fu, Kui Ren, Jiangang Shu, Xingming Sun, and Fengxiao Huang, “Enabling Personalized Search over Encrypted Outsourced Data with Efficiency Improvement” - IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 27, NO. 9, SEPTEMBER 2016.
3. Cong Wang, Sherman S.M. Chow, Qian Wang, Kui Ren, and Wenjing Lou, “Privacy-Preserving Public Auditing for Secure Cloud Storage” - IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 22, NO. 5, MAY 2011.
4. Xiaofeng Chen, Jin Li, Jian Weng, Jianfeng Ma, and Wenjing Lou, “Verifiable Computation over Large Database with Incremental Updates - IEEE TRANSACTIONS ON COMPUTERS, VOL. 65, NO. 10, OCTOBER 2016.
5. Jiawei Yuan and Shucheng Yu, “Public Integrity Auditing for Dynamic Data Sharing With Multiuser Modification” - IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 10, NO. 8, AUGUST 2015.
6. Zhangjie Fu, Xinle Wu, Chaowen Guan, Xingming Sun, and Kui Ren, “Toward Efficient Multi-Keyword Fuzzy Search Over Encrypted Outsourced Data With Accuracy Improvement” - IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 11, NO. 12, DECEMBER 2016.
7. Jia-Lun Tsai and Nai-Wei Lo, “Privacy-Aware Authentication Scheme for Distributed Mobile Cloud Computing Services” - IEEE SYSTEMS JOURNAL, VOL. 9, NO. 3, SEPTEMBER 2015.