MONA: SECURE MULTI -OWNER DATA SHARING FOR DYNAMIC GROUPS IN THE CLOUD

V Gokula Krishnan[1], J Gowtham Kumar[2], I Kalyyanasundar[3], R Sanjay[4]

Associate Professor[1], Department of Computer Science and Engineering, Panimalar Institute of Technology, Chennai, Tamil Nadu, India
UG Scholars[2], Department of Computer Science and Engineering, Panimalar Institute of Technology, Chennai, Tamil Nadu, India
UG Scholars[3], Department of Computer Science and Engineering, Panimalar Institute of Technology, Chennai, Tamil Nadu, India
UG Scholars[4], Department of Computer Science and Engineering, Panimalar Institute of Technology, Chennai, Tamil Nadu, India

ABSTRACT

The genuine function of this strategy is a secure multi-proprietor data sharing arrangement. It derives that any user at intervals the social affair can firmly offer data to others by the untrusted cloud. This arrangement can support dynamic social occasions. Profitably, especially, new permissible customers can clearly unscramble data archives modified before their backing whereas not coming to with data proprietors. User revocations are typically successfully sensible through a novel foreswearing list whereas not modification the puzzle Keys of notwithstanding remains of the purchasers. The dimensions and count overhead of secret writing are steady and freelance with the amount of revoked user. We gift a secure and security guaranteeing access management to customers, which guarantee any half in a very event to anonymously utilize the cloud resource. The veritable identities of information proprietors will be disclosed by the get-together government once open deliberation happen. We have a tendency to offer careful security examination, and perform expansive generations to point out the adequacy of our arrangement to the extent limit and estimation overhead. Disseminated calculation provides a traditionalist and paying response for sharing event resource among cloud customers. Sharing knowledge an exceedingly multi-proprietor means shielding knowledge and identity security from an untrusted cloud continues to be a testing issue.

Keyword: - *Encryption, Cloud Computing, Dynamic Broadcast, Servers, Data Sharing, Privacy Preserving, Access Control, Multi Owner, User Revocation*

1. INTRODUCTION

Cloud computing, with the characteristic of intrinsic information sharing and low maintenance, provides a stronger utilization of resources. In cloud computing, cloud service suppliers provide an abstraction of infinite space for storing for clients to host information. It will facilitate clients scale back their money overhead of information managements by migrating the native managements system into cloud servers. However, security considerations become the most constraint as we have a tendency to currently source the storage of information, which is probably sensitive, to cloud providers. To preserve information privacy, a standard approach is to encode information files before the clients transfer the encrypted information into the cloud. Unfortunately, it's tough to style a secure and more efficient information sharing scheme, particularly for dynamic clusters within the cloud.
Cloud computing is the use of computing resources (hardware and software) that are delivered as a service over a network (typically the Internet). As an abstraction for the difficult infrastructure it contains in system diagrams, the name comes from the common use of a cloud-shaped symbol. Cloud computing entrusts remote services with a user's information, computer code and computation. Cloud computing is recognized as an alternate to ancient info technology because of its intrinsic resource-sharing and low-maintenance characteristics. In cloud computing, the

cloud service suppliers (CSPs), like Amazon, are ready to deliver numerous services to cloud users with the assistance of powerful datacentres. By migrating, the native information management systems into cloud servers, users will get pleasure from high-quality services and save important investments on their native infrastructures.

2. RELATED WORK

[1] Anmin Fu, Shui Yu, Yuqing Zhang, Huaqun Wang, and Chanying Huang recommend to make sure the integrity of the shared information, some schemes are designed to permit public verifiers (i.e., third party auditors) to with efficiency audit information integrity while not retrieving the whole users' information from cloud. In contrast to the present solutions, our theme needs a minimum of cluster managers to recover a trace key hand in glove, that eliminates the abuse of single-authority power and provides non-frameability. Moreover, our theme ensures that cluster users will trace information changes through selected binary tree; and might recover the most recent correct information block once the present information block is broken. Additionally, the formal security analysis and experimental results indicate that our theme is demonstrably secure and economical during this paper, NPP: A New Privacy-Aware Public Auditing Scheme for Cloud Data Sharing with Group Users (2017).

[4] Jia Yu, Kui Ren, Cong Wang,and Vijay Varadharajan, recommend to investigate a way to scale back the harm of the client's key exposure in cloud storage auditing, and provides the primary sensible resolution for this new downside setting. We have a tendency to formalize the definition and also the security model of auditing protocol with key-exposure resilience and propose such a protocol. In our style, we have a tendency to use the binary tree structure and also the pre-order traversal technique to update the key keys for the shopper. We have a tendency to conjointly develop a unique appraiser construction to support the forward security and also the property of blockless verifiability. The protection evidence and furthermore the performance analysis demonstrate that our anticipated protocol is secure and economical all through this paper, Enabling Cloud Storage Auditing with Key-Exposure Resistance (2015).

[6] Boyang Wang, Baochun Li and Hui Li recommend to exploiting a ring signature to calculate the verification data required to audit the integrity of shared information. With our mechanism, the identity of the signer on every block in shared information is unbroken non-public from a 3rd party auditor (TPA), WHO continues to be ready to publically verify the integrity of shared information while not retrieving the whole file. Our experimental results demonstrate the effectiveness and potency of our projected mechanism once auditing shared information during this paper, Oruta: Privacy-Preserving Public Auditing for Shared data in the Cloud (2014).

[7] Boyang Wang, Baochun Li, and Hui Li Investigate to propose a unique public auditing mechanism for the integrity of shared information with economical user revocation in mind. By utilizing the thought of proxy re-signatures, we have a tendency to enable the cloud to re-sign blocks on behalf of existing users throughout user revocation, in order that existing users don't have to be compelled to transfer and re-sign blocks by themselves. Additionally, a public booster is usually ready to audit the integrity of shared information while not retrieving the whole information from the cloud, albeit some a part of shared information has been re-signed by the cloud. Moreover, our mechanism is ready to support batch auditing by verificatory multiple auditing tasks at the same time. Experimental results show that our mechanism will considerably improve the potency of user revocation throughout this paper, Panda: Public auditing for Shared data with Efficient User Revocation in the Cloud (2015).

[9] Tao Jiang, Xiaofeng bird genus, and Jianfeng Ma recommend to analyze sand predict QoS performance, and adaptively assign applicable wireless metric to accommodate extra multimedia sessions whereas not QoS degradation. it'll indicate that the joint vogue is in an exceedingly position to intelligently assign resources supported QoS demands resource-constrained home M2M networks throughout this paper, Public Integrity Auditing for Shared Dynamic Cloud Data with Group User Revocation (2015).

[10] H. Wang recommend to provide a unique remote information integrity checking model in multi-cloud storage. The formal system model and security model are given. Supported the linear pairings, a concrete ID-DPDP protocol is intended. The projected ID-DPDP protocol is demonstrably secure beneath the hardness assumption of the quality CDH (computational Diffie-Hellman) downside. Additionally to the structural advantage of elimination of certificate management, our ID-DPDP protocol is additionally economical and versatile. During this paper, Identity-Based Distributed Provable Data Possession in Multi-Cloud Storage (2015), non-public verification, delegated verification and public verification will understood by Supported the client's authorization, the projected ID-DPDP protocol.

3. PROBLEM DEFINITION

This paper presents a Secure Multi owner data sharing scheme, Named Mona, for dynamic clusters within the cloud. Any cloud user will anonymously share information with others by investing Group Signature and dynamic broadcast encoding techniques. The Main aim of the MONA is to provide solutions for three issues. One is to create a combined solution for Quality of Service (QOS) issues in cloud. Second is to provide the solution for Security for Dynamic Group users by the Un-trusted Cloud. Third is to provide a way to find the un-trusted users in the dynamic groups and to revoke the users from that group.

4. EXISTING SYSTEM

Several security schemes for information sharing on untrusted servers are planned. In these approaches, information owners store the encrypted information files in untrusted storage and distribute the corresponding decoding keys solely to licensed users. As a result of no information of the decoding keys, Storage servers as well as unauthorized users are unable to learn the content of the information files. The complexities of user participation and revocation in these schemes are linearly increasing with the information owners and also the number of revoked users.

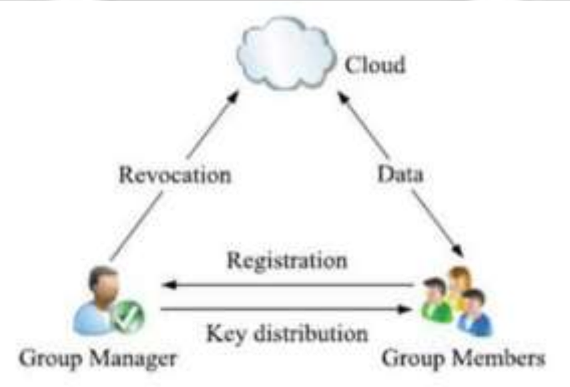


Fig-1: Working of Existing System

By setting a bunch with one attribute, Lu et al. planned a secure provenance scheme based on the cipher text-policy attribute-based encoding technique, which permits any member in a very cluster to share information with others. However, the difficulty of user revocation isn't addressed in their scheme. A Presented scalable and fine-grained information access control scheme in cloud computing is predicated on the key policy attribute-based encoding (KP-ABE) technique. Sadly, the only owner manner hinders the adoption of their scheme into the case wherever any user is granted to store and share information.

4.1Disadvantages

- It doesn't give security for sharing the data among the teams.
- It doesn't give privacy protective access management to the users**.**

5. DESIGN GOALS

5.1 Access control

Initial, licensed cluster members are able to access the cloud information. Second, unauthorized users cannot access the cloud information at any time, and revoked users won't be capable of accessing the cloud once they're revoked.

5.2 Data confidentiality

Data confidentiality needs that unauthorized users aren't capable to access the content of the stored information and difficult issue for information confidentiality for dynamic clusters. Specifically, new users ought to access the information stored within the cloud before their participation, and revoked users are unable to access the information once the revocation. Data owner can store the information on the cloud and share among the cluster members and data owner can modify the information and delete the information within the cloud.

5.3 Anonymity and Traceability

Anonymity guarantees that cluster members will access the cloud without revealing the real identity. Though anonymity is an efficient protection for user’s identity, it additionally poses a potential within attack risk to the system. For instance, an internal attacker might store and share a malicious data to get the necessary data. Thus, to get rid of the within attack, the cluster manager ought to have the power to verify the important identities or members of information owners. If the one cluster member access the information and delete or modify the information by different cluster members data may be simply traceable within the cloud.

5.4 Efficiency

Any cluster member will store and share information files with others within the cluster by the cloud. User revocation is achieved by without involving the remaining users. The remaining users don't have to be compelled to update their private keys or re-encryption operations. New cluster member will access all the content information files stored on cloud before his participation without contacting with the information owner.

6. PROPOSED SYSTEM

Our Scheme has a tendency to propose a secure multi owner information sharing scheme, named Mona, for dynamic clusters within the cloud. Any cloud user will anonymously share information with others by leverage cluster signature and dynamic broadcast encoding techniques.

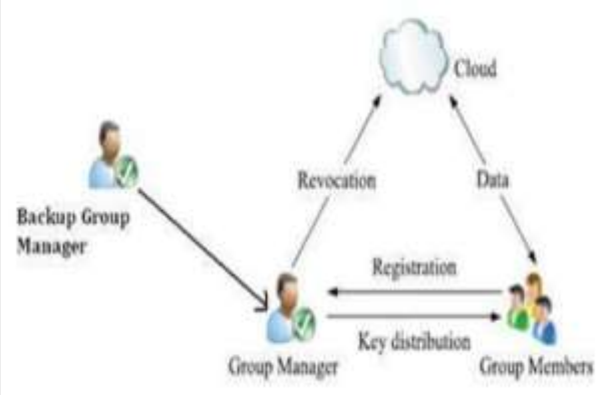


Fig-2: Working of Proposed System

A quantity of revoked users is directly proportional to the storage overhead and encoding computation price of our scheme. Additionally, we have a tendency to analyze the protection of our scheme with rigorous proofs, and demonstrate the potency of our scheme in experiments.

6.1 ADVANTAGES

- Secure multi-owner information sharing scheme proposed by us implies that any information shared by any user within the cluster will be firmly shared with others in public cloud.
- We can guarantees any member during a cluster to anonymously utilize the cloud resource by giving secure and privacy-preserving access control to users.

7. SYSTEM ARCHITECTURE

The architecture model consists of 3 main completely different entities: The Cloud Server, group Manager and a large range of cluster Members.

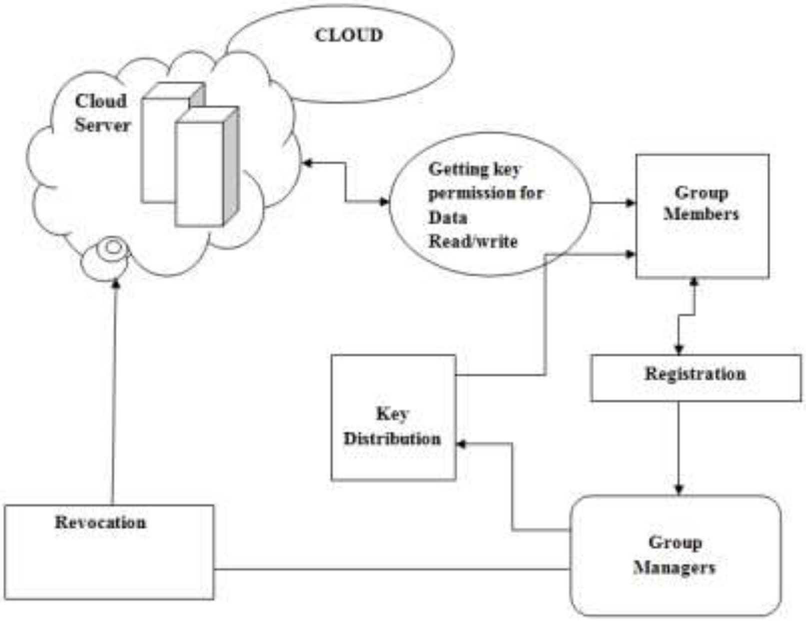


Fig-3: Block Diagram of Mona

7.1 Cloud Server

Cloud is the massive repository of resources. Cloud is accountable for storing all user information and granting access to the file among a cluster to different cluster members based on public revocation list which is maintained by group manager. We have a tendency to assume that the cloud server is honest but curious. That is, the cloud server will not maliciously delete or modify user information, but can attempt to learn the content of the stored information.

7.2 Group Manager

The group manager is acted by the administrator of the company. The group manager is completely trusted by the other parties group manager perform various operations like generation of encoding key by bilinear mapping, system parameters generation, user registration, creation of cluster, assign cluster signature, and also assigning resources to a requested user, maintaining revocation list and migrate this list into cloud for public use, and traceability.

7.3 Group Members

Group members are a collection of registered users that may store their private information into the cloud server and share them with others within the group.

8. MODULES DESCRIPTION

8.1 User Registration

For the registration of user with identity ID the group manager arbitrarily selects a number. Then the group manager adds into the group user list which is able to be utilized in the traceability section. Once the registration, user obtains encryption key which is able to be used for group signature generation and file decoding.

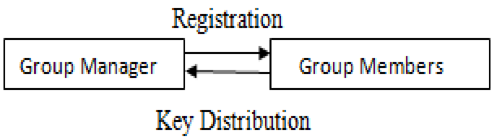


Fig-4: User Registration

8.2 User Revocation

User revocation is performed by the group manager via a public available. Revocation List, based on which group members will encode their information files and make sure the confidentiality against the revoked users. Group manger update the revocation list on a daily basis even no user has being revoked within the day. In alternative words, the others will verify the freshness of the revocation list from the contained current date.

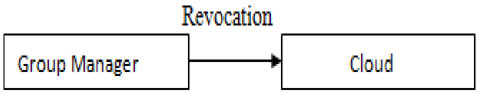


Fig-5: User Revocation

8.3 File Generation and Deletions

To store and share the information enter the cloud, a group member performs to obtaining the revocation list from the cloud. During this step, the member sends the group identity ID group as an invitation to the cloud for verifying the validity of the received revocation list. File stored within the cloud will be deleted by either the group manager or the information owner.

8.4 File Access and Traceability

To access the cloud, a user has to compute a group signature for his/her authentication. The utilized group signature scheme will be considered a variant of the short group signature which inherits the inherent enforceability property, anonymous authentication, and following capability. Once an information dispute happens, the tracing operation is performed by the group manager to spot the important identity of the information owner.

9. EXPERIMENTAL RESULTS

The below displayed are the results of the module implementation. These screenshots show the User Interface through which the modules are being developed.

User Registration Form is form which is used to register a new user in any group. After registration of new user, 16-bit secret code is generated for this new user and secret code will be sent to new registered user (Figure6).

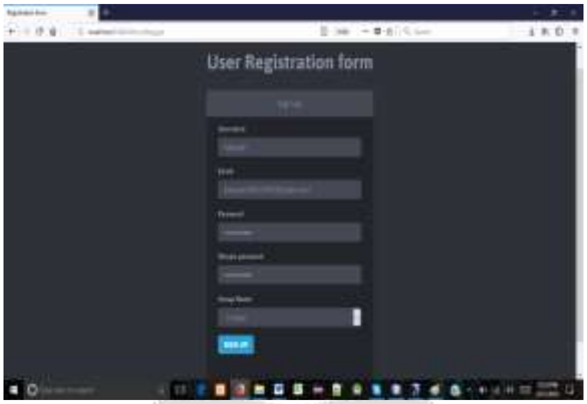


Fig-6: Creating a new member in the Group 1

File Upload Page is used to share a user's file among other same group users while other user of same group can be access the file by using their secret key (Figure7).A uploaded file which will be stored in the cloud. Owner can be access it by its storage location.

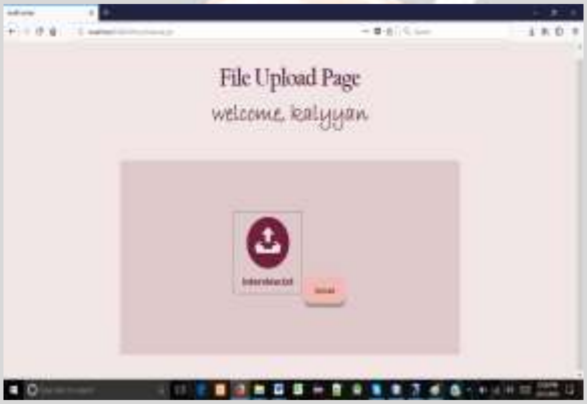


Fig-7: Uploading a new file in the Group 1 by one of its Group Member.

If someone from different group user want to access your file, then that user want to request access of any particular file to own user (Figure8).There is no other ways to access a file from different groups.

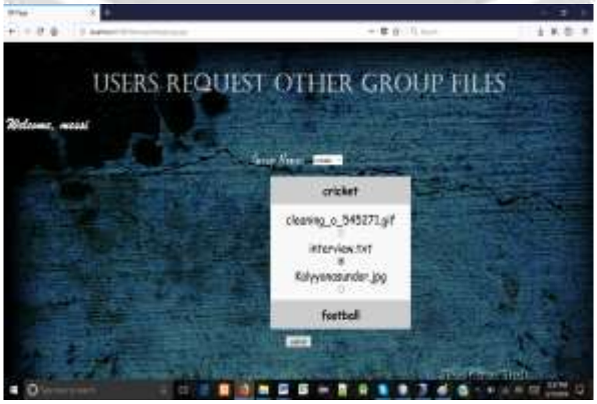
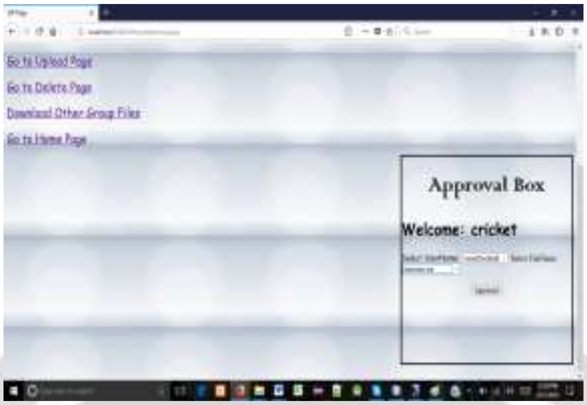


Fig-8: Requesting a file of Group 1 by one of the Group Member of Group 2.

Approval Box consists of list of request from different user of different groups to access your file. Approval Box is used to approve the other user's request of accessing yours file. If unwanted request, then owner can block that user or group respectively (Figure9).



Go to Upload Page

Go to Delete Page

Download Other Group Files

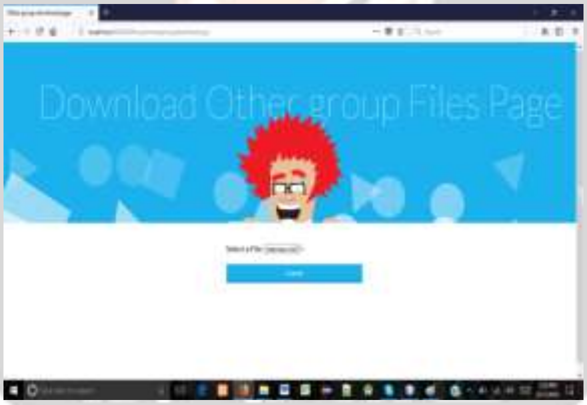
Go to Home Page

Approval Box

Welcome: cricket

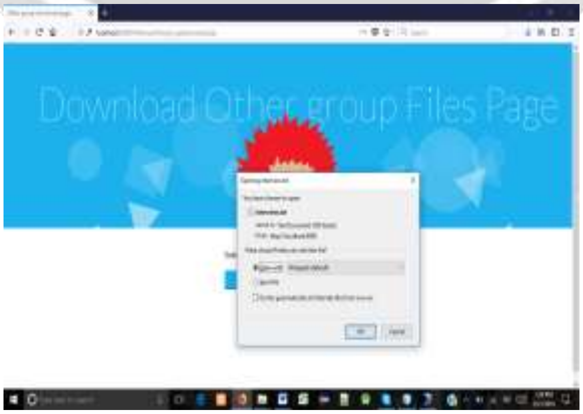
Fig-9: Approving Request from the Group Member of Group 2 by the one of the Group Member of Group 1.

It is the gateway to access or download the other owner file of different group if owner of that file have accepted your proposal of accessing their own file (Figure10 & Figure11).If suppose owner of the file didn't accept your request, then you are not able to see the file name to download it or view it.



Download Other group Files Page

Fig-10: Selection of approved other group file.



Download Other group Files Page

Fig-11: Download of approved other group file.

10. CONCLUSION

Cloud computing is extremely engaging surroundings for business world in term of providing needed services in an exceedingly very price effective approach. However, reassuring and enhancing security and privacy practices can attract a lot of enterprises to world of cloud computing. Therefore to realize the reliability and scalability in Mona, during this paper we tend to are measure the new framework for Mona. For dynamic teams in a not trustable cloud, In Mona, a user is ready to share knowledge with others within the cluster while not revealing identity privacy to the cloud. To boot, Mona supports economical user revocation and new user change of integrity. a lot of specially, economical user revocation is achieved through a public revocation list while not change the personal keys of the remaining users, and new users will directly decode files keep within the cloud before their participation. Moreover, the storage overhead and also the coding computation price are constant and length of the signature and also the period of the signing algorithmic rule are freelance of the quantity of cluster members. Intensive analyses show that our planned theme satisfies the required security needs and guarantees potency furthermore.

REFERENCES

[1]. Anmin Fu, Shui Yu, Yuqing Zhang, Huaqun Wang, and Chanying Huang “NPP: A New Privacy-Aware Public Auditing Scheme for Cloud Data Sharing with Group Users” IEEE Transactions on Big Data, Volume: PP, Issue: 99, pp.1-10, 05 May 2017.

[2]. C. Wang, Q. Wang, K. Ren, et al, “Privacy Preserving Public Auditing for Secure Cloud Storage,” IEEE Transactions on Computers, Volume: 62, Issue: 2, pp.362-375, February 2013.

[3]. Boyang Wang, Sherman S.M. Chow, Ming Li, and Hui Li, “Storing Shared Data on the Cloud via Security-Mediator” Distributed Computing Systems (ICDCS), 2013 IEEE International Conference on Collaboration and Internet Computing, pp.124-133, 12 December 2013.

[4]. Jia Yu, Kui Ren, Cong Wang, and Vijay Varadharajan, “Enabling Cloud Storage Auditing with Key-Exposure Resistance” IEEE Transactions on Information Forensics and Security, Volume: 10, Issue: 6, pp. 1167-1179, 05 February 2015.

[5]. 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, Volume: 22, Issue: 5, pp. 847-859, May 2011.

[6]. B. Wang, B. Li, and H. Li, “Oruta: Privacy Preserving Public Auditing for Shared Data in the Cloud,” IEEE Transactions on Cloud Computing, Volume: 2, Issue: 1, pp.43-56, 13 January 2014.

[7]. B. Wang, B. Li, and H. Li, “Panda: Public Auditing for Shared Data with Efficient User Revocation in the Cloud” IEEE Transactions on Services Computing, Volume: 8, Issue: 1, pp. 92-106, January 2015.

[8]. C. Liu, J. Chen, L. Yang, et al, “Authorized Public Auditing of Dynamic Big Data Storage on Cloud with Efficient Verifiable Fine Grained Updates” IEEE Transactions on Parallel and Distributed Systems, Volume: 25, Issue: 9, pp.2234-2244, September 2014.

[9]. T. Jiang, X. Chen, and J. Ma, “Public Integrity Auditing for Shared Dynamic Cloud Data with Group User Revocation” IEEE Transactions on Computers, Volume: 65, Issue: 8, pp.2363-2373, 01 August 2016.

[10]. H. Wang, “Identity Based Distributed Provable Data Possession in Multi Cloud Storage” IEEE Transactions on Services Computing, Volume: 8, Issue: 2, pp.328-340, March 2015.

[11]. S. Yu, C. Wang, K. Ren, et al, “Achieving Secure, Scalable and Fine Grained Data Access control in cloud computing,” Proceedings of IEEE INFOCOM, pp.1-9, 06 May 2010.