**SURVEY ON PRIVACY PRESERVING CLOUD AUDITING FOR SHARED DATA**

**ABSTRACT:**

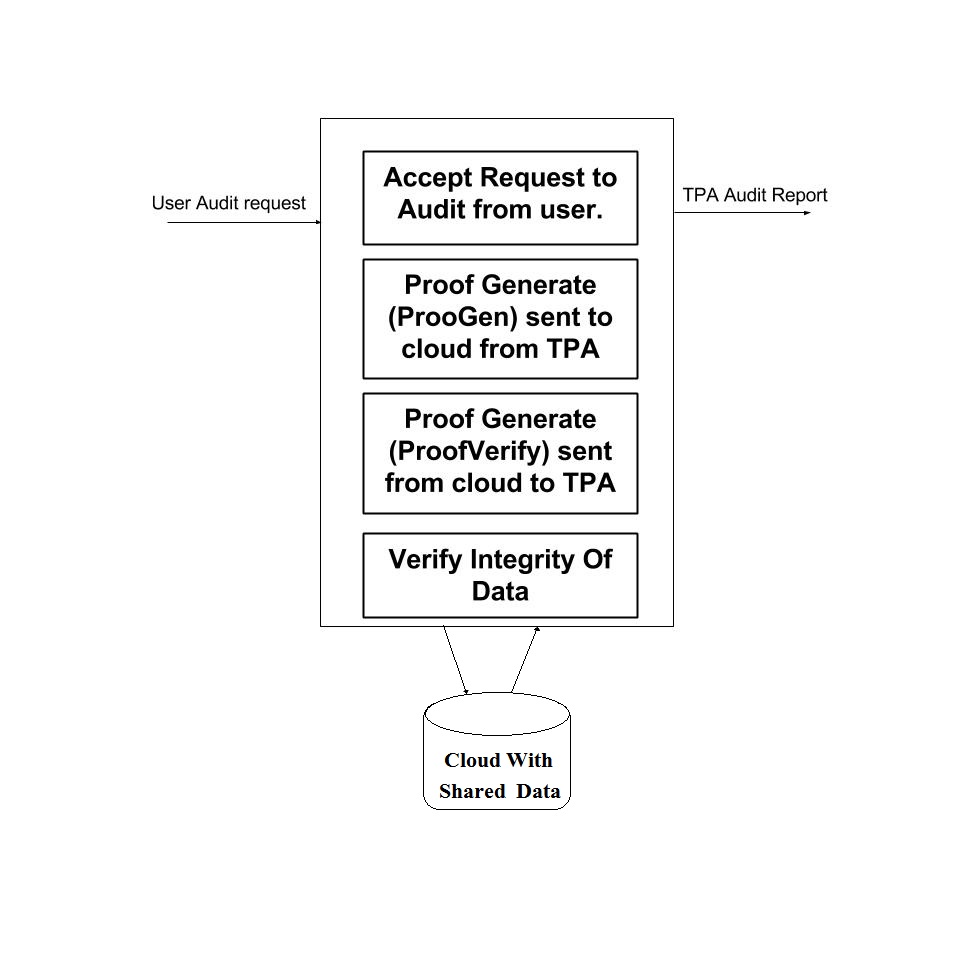
Cloud is a type of platform which helps to store the data as well as helps in sharing the data. While sharing the huge amount of data, the primary concern comes in mind is data integrity, security of the data. For the cloud server and the user it is not possible to check the integrity, consistency of stored data on cloud. Public Auditing method can help to overcome this problem. Hence the user takes help of the third party auditor (TPA) for auditing their data. Many of the techniques have been proposed by various researchers which improve upon one another. Here we have presented three landmark methodologies on Privacy preserving cloud auditing for shared data on cloud.

**INTRODUCTION:**

Cloud Computing is an upcoming new technology which provides the on-demand facility of a shared pool of resources (computing resources) (e.g., computer storage, applications and other resources), which can include rapid allocation and freedom with minimum number of efforts. Cloud computing and storage solutions provide individual users and companies with variety of capabilities to store and work on their data in data centers which are not owned by them and the location may be remote, may be across a city or across continents. Cloud computing provides sharing of resources to achieve economy of scales. The users use this cloud for sharing and the collaboration of their data with many other users in the group. Data sharing has become need in today’s world and it is provided in most of the cloud storage offerings, via Dropbox, Google.

The data integrity in cloud storage, is a subject to skepticism and inspection, as there is always this fear of data being stored in an environment where there is a chance of getting lost or corrupted[1]. The need of the Third Party Auditor (TPA) is very necessary for ensuring the integrity of the data.

Allowing public auditability for cloud storage is important so that users assign a third- party auditor (TPA) for the checking of the integrity of outsourced data and TPA offers its auditing service with more commanding computation and abilities of the communication than regular users. If we mention information, Wang et al. designed to construct a mechanism of public auditing system for cloud data, so that during public auditing process, the contents of the private data that belong to a personal user is not revealed to the third party auditor.  
 Sharing data among the multiple users is one of the features in the motivation of cloud storage. A unique problem that is introduced during the whole process of public auditing for the shared data in the cloud is how we should reserve the identity secrecy from the TPA, because the identities of each signer on shared data may show that a particular user among the group of users or special blocks in shared data is amore valuable.



**IMPLEMENTATION DETAILS:**

Oruta is constructed, using the method of HARS and its properties. Using Oruta, the TPA is able to verify the data without retrieving all of them and still maintaining the identity privacy of the users who signed them includes five algorithms:

1. KeyGen: for generating a user's public and private key
2. SigGen : invalid user i.e a member of the group or the original owner of the data can sign a data block which is a combination of its own private key and all other user’s public key.
3. Modify: evaluation is a can add delete or modify data and computer new signature on that data
4. ProofGen : used by both the TPA as well as the cloud server to generate a proof possession of shared data.
5. ProofVerify: the cloud sent this proof of procession to the TPA and the TPA verifies it.

*Solution To Other Problems Proposed in ORUTA:*

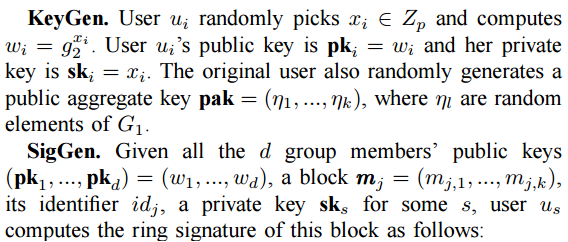
The size of the Ring signature is an issue which is solved in this paper by using an aggregate block that is aggregate of many other data packs.

Another issue which is solved in this paper is the dynamic changes in the data by valid users. This was achieved by the use of hashing techniques.  
Advantages:

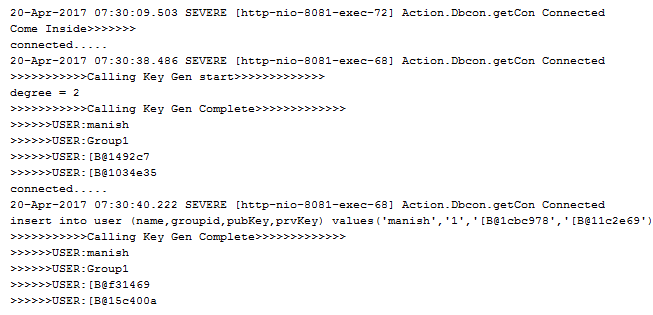
1. Preserves data from third party auditor and achieves data security.
2. Solves the problem of large storage space required for ring signatures.
3. Solves the problem of dynamic operations on data by Hash indexing.
4. Preserves user identity from third party auditor.

Disadvantages:

1. An unsolved challenge in Oruta remains that the groups need to be predefined. Dynamic changes in the group like addition or deletion or modification of user keys and changing the private information of users is not allowed. This remains the future scope of this paper.

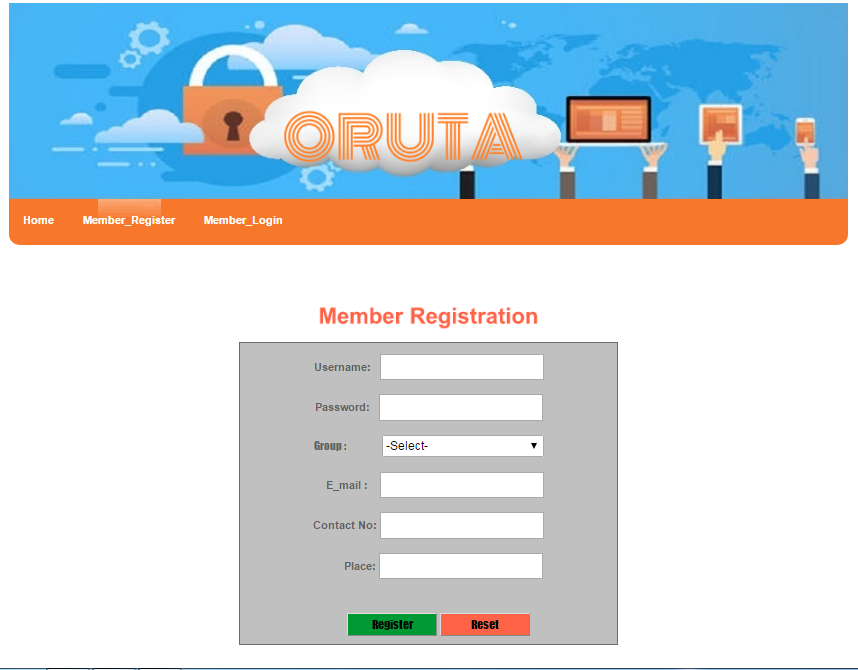


**RESULT:**



**SNAPSHOT:**







**CONCLUSION:**

After these techniques are understood, algorithms will be given code form. But

the implementation of basic UI will be started during the understanding of the techniques is going on. Netbeans is used for development as we have unanimously decided to implement Oruta in JSP, so as to increase its productivity by implementing it on web platform and also use the power of Java.

**REFERENCES:**

1. Boyang Wang, Student Member, IEEE, Baochun Li, Senior Member, IEEE, and Hui Li, Member, IEEE(IEEE TRANSACTIONS ON CLOUD COMPUTING, VOL. 2, NO. 1, JANUARY-MARCH 2014)
2. Ms.Madhuri B.Patil -M.Tech(CSE),Department CSE,MLRIT,Hyderabad & Mr. N. Aravind Kumar- Assistant Professor,Department of CSE, MLRIT,Hyderabad International Research Journal of Computer Science (IRJCS) ISSN: 2393-9842 Issue 6, Volume 2 (June 2015)