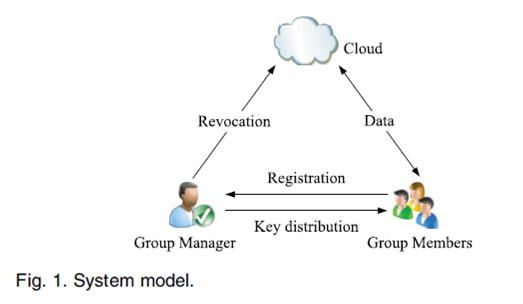
**Mona: Secure Multi-Owner Data Sharing for Dynamic Groups in the Cloud**

**ABSTRACT:**

With the character of low maintenance, cloud computing provides an economical and efficient solution for sharing group resource among cloud users. Unfortunately, sharing data in a multi-owner manner while preserving data and identity privacy from an untrusted cloud is still a challenging issue, due to the frequent change of the membership. In this paper, we propose a secure multiowner data sharing scheme, named Mona, for dynamic groups in the cloud. By leveraging group signature and dynamic broadcast encryption techniques, any cloud user can anonymously share data with others. Meanwhile, the storage overhead and encryption computation cost of our scheme are independent with the number of revoked users. In addition, we analyze the security of our scheme with rigorous proofs, and demonstrate the efficiency of our scheme in experiments.

**Architecture:**



**EXISTING SYSTEM:**

To preserve data privacy, a basic solution is to encrypt data files, and then upload the encrypted data into the cloud. Unfortunately, designing an efficient and secure data sharing scheme for groups in the cloud is not an easy task.In the existing System data owners store the encrypted data files in untrusted storage and distribute the corresponding decryption keys only to authorized users. Thus, unauthorized users as well as storage servers cannot learn the content of the data files because they have no knowledge of the decryption keys. However, the complexities of user participation and revocation in these schemes are linearly increasing with the number of data owners and the number of revoked users, respectively.

**DISADVANTAGES OF EXISTING SYSTEM:**

1. In the existing Systems, identity privacy is one of the most significant obstacles for the wide deployment of cloud computing. Without the guarantee of identity privacy, users may be unwilling to join in cloud computing systems because their real identities could be easily disclosed to cloud providers and attackers.
2. On the other hand, unconditional identity privacy may incur the abuse of privacy. For example, a misbehaved staff can deceive others in the company by sharing false files without being traceable.
3. Only the group manager can store and modify data in the cloud
4. The changes of membership make secure data sharing extremely difficult the issue of user revocation is not addressed

**PROPOSED SYSTEM:**

We propose a secure multi-owner data sharing scheme. It implies that any user in the group can securely share data with others by the untrusted cloud. Our proposed scheme is able to support dynamic groups efficiently. Specifically, new granted users can directly decrypt data files uploaded before their participation without contacting with data owners. User revocation can be easily achieved through a novel revocation list without updating the secret keys of the remaining users. The size and computation overhead of encryption are constant and independent with the number of revoked users. We provide secure and privacy-preserving access control to users, which guarantees any member in a group to anonymously utilize the cloud resource. Moreover, the real identities of data owners can be revealed by the group manager when disputes occur. We provide rigorous security analysis, and perform extensive simulations to demonstrate the efficiency of our scheme in terms of storage and computation overhead.

**ADVANTAGES OF PROPOSED SYSTEM:**

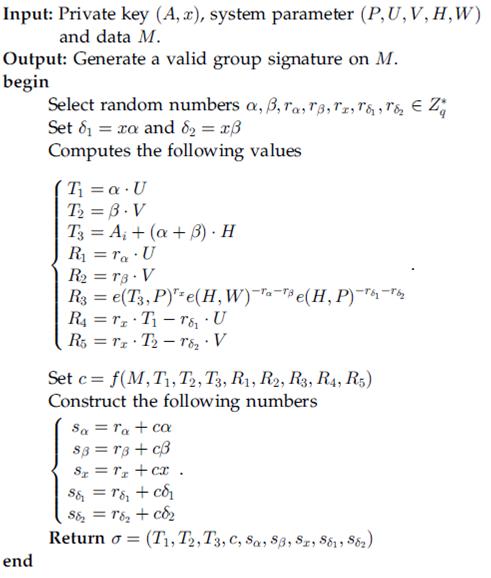
1. Any user in the group can store and share data files with others by the cloud.
2. The encryption complexity and size of cipher texts are independent with the number of revoked users in the system.
3. User revocation can be achieved without updating the private keys of the remaining users.
4. A new user can directly decrypt the files stored in the cloud before his participation.

**Modules :**

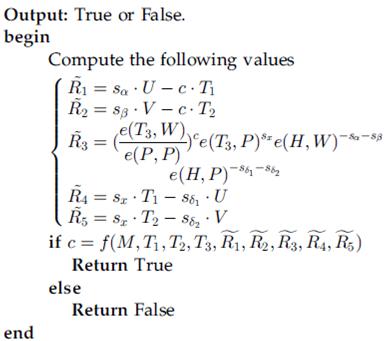
* Signature Generation (Algorithm used)
* Signature Verification (Algorithm used)
* Revocation Verification (Algorithm used)

**ALGORITHMS DESCRIPTION:**

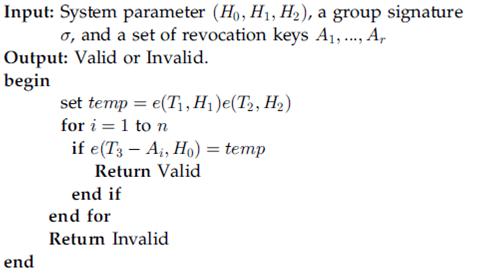
**Signature Generation**



**Signature Verification:**



**Revocation Verification**



**SYSTEM REQUIREMENTS:**

**HARDWARE REQUIREMENTS:**

* System : Pentium IV 2.4 GHz.
* Hard Disk : 40 GB.
* Monitor : 15 inch VGA Colour.
* Mouse : Logitech Mouse.
* Ram : 512 MB
* Keyboard : Standard Keyboard

**SOFTWARE REQUIREMENTS:**

* Operating System : Windows XP.
* Coding Language : ASP.NET, C#.Net.
* Database : SQL Server 2005

**REFERENCE:**

Xuefeng Liu, Yuqing Zhang, Boyang Wang, and Jingbo Yan, “Mona: Secure Multi-Owner Data Sharing for Dynamic Groups in the Cloud”, IEEE