ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Monthly Peer Reviewed Open Access International e-Journal

# Multi-Owner Data Sharing by using Three-dimensional security pattern in cloud computing

**P T Satya Narayana Murthy**
M.Tech Student,
Department of CSE,
Srinivasa Institute of Engineering and Technology.

**V.Venkanna**
Assistant Professor,
Department of CSE,
Srinivasa Institute of Engineering and Technology.

## ABSTRACT:

Cloud computing provides different services economically and efficiently to share many resources among cloud users with low maintenance cost. But unfortunately, during this sharing process data preservation and data integration became a challenging issue for the researcher.

This paper, we proposes a secure mona protocol for data sharing in un-trusted cloud called Mona, for dynamic cloud groups by introducing group signature and dynamic broadcast encryption techniques. This technique helps all the cloud user to share data with others. This presents an efficient result to support the authors claim that it gives an best result as compare to the existing encryption technique.

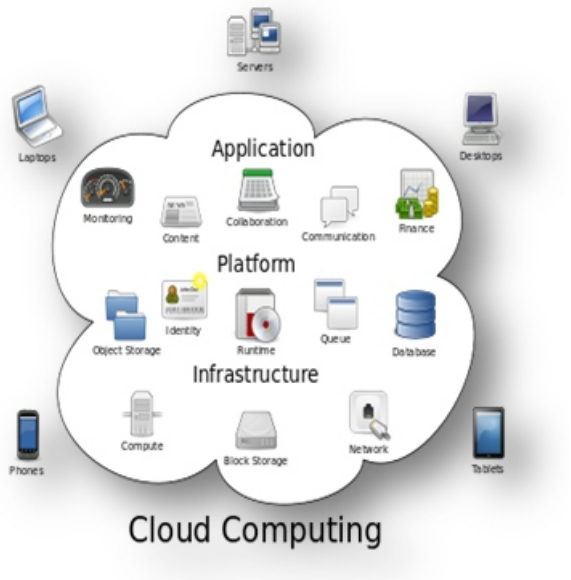
## Key words:
Mona, multiowner data sharing, group signature.

## 1.INTRODUCTION:

Cloud computing is the anthology of user assets that are useful to offer services over a network particularly over the internet. Cloud computing found remote services with a user's data, software and computation. These services normally provide access to a enormous data and many software applications with high-end networks of server computers [1].

The aim of cloud computing is to pertain conventional supercomputing, or high-performance computing power, normally used by military and research facilities, to perform more computations per second, in consumer-oriented applications such as financial portfolios, to deliver personalized information, to provide data storage or to power large, immersive computer games.[2].

The cloud computing uses networks of large groups of servers normally running low-cost end user PC technology with expert connections to broaden data-processing chores across them. System which is shared with a large pools of systems that are linked together [3,4].




Structure of cloud computing

## Characteristics and Services Models:

The most important characteristics of cloud computing is based on the definitions of it provided by many authors [5,6,7]:

- **On-demand self-service:**
- **Broad network access:**
- **Resource pooling:**
- **Rapid elasticity:**

**Measured service**

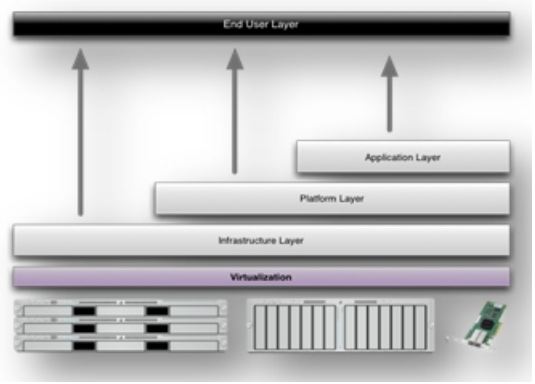
ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Monthly Peer Reviewed Open Access International e-Journal


Characteristics of cloud computing

## Services Models:

Cloud Computing comprises three different service models, namely Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), and Software-as-a-Service (SaaS).

These three service models are completed by an end user layer that encapsulates the end user point of view on cloud services. The model is shown in figure below [8, 9, 10].




Structure of service models

Many researchers has developed many secured storage system like M. Kallahalla et al [11] has introduced a cryptographic storage system called Plutus that enables secure file sharing without placing much trust on the file servers. E. Goh et al [12] presents SiRiUS, a secure file system designed to be layered over insecure network and P2P file systems such as NFS, CIFS, OceanStore, and Yahoo! Briefcase.

Ateniese, Giuseppe, et al [13] predict that fast and secure re-encryption will become increasingly popular as a method for managing encrypted file systems. Although efficiently computable, the wide-spread adoption of BBS re-encryption has been hindered by considerable security risks.

R. Lu, X. Lin et al [14] proposed a new secure provenance scheme based on the bilinear pairing techniques. As the essential bread and butter of data forensics and post investigation in cloud computing, the proposed scheme is characterized by providing the information confidentiality on sensitive documents stored in cloud, anonymous authentication on user access, and provenance tracking on disputed documents.

B. Waters et al [15] present a new methodology for realizing Ciphertext-Policy Attribute Encryption (CP-ABE) under concrete and noninteractive cryptographic assumptions in the standard model.

## 2.SYSTEM ANALYSIS AND DESIGN:

To safeguard the privacy in data , 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 un trusted storage and allocate the corresponding decryption keys only to authorized users.

Thus, unauthorized users as well as storage servers cannot find out 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.

So we propose a secure mona protocol for data sharing in un-trusted cloud.in the proposing system ,called mona protocol for data sharing in dynamic groups by using group signature verification and file key verification. As new granted members can easily access securely.Don't required any knowledge of the decryption technique. Additionally, Mona supports efficient user revocation and new user joining. More specially, 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. Moreover, the storage overhead and the encryption computation cost are constant. Extensive analyses show that our proposed scheme satisfies the desired security requirements and guarantees efficiency as well.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Monthly Peer Reviewed Open Access International e-Journal


System model

## MPLEMENTATION:

## MODULES:

1.Cloud Module
2.Group Manager Module
3.Group Member Module
4.File Security Module
5.Group Signature Module
6. User Revocation Module.

## MODULES DESCRIPTION:

### 1.Cloud Module :

In this module, we create a local Cloud and provide priced abundant storage services. The users can upload their data in the cloud. We develop this module, where the cloud storage can be made secure.

However, the cloud is not fully trusted by users since the CSPs are very likely to be outside of the cloud users' trusted domain. Similar to we assume that the cloud server is honest but curious.

That is, the cloud server will not maliciously delete or modify user data due to the protection of data auditing schemes, but will try to learn the content of the stored data and the identities of cloud users.

### 2.Group Manager Module :

Group manager takes charge of followings,
1. System parameters generation,
2. User registration,
3. User revocation, and
4. Revealing the real identity of a dispute data owner.
Therefore, we assume that the group manager is fully trusted by the other parties. The Group manager is the admin. The group manager has the logs of each and every process in the cloud. The group manager is responsible for user registration and also user revocation too.

### 3.Group Member Module :

Group members are a set of registered users that will
1.store their private data into the cloud server and
2.Share them with others in the group.

Note that, the group membership is dynamically changed, due to the staff resignation and new employee participation in the company.

The group member has the ownership of changing the files in the group. Whoever in the group can view the files which are uploaded in their group and also modify it. The group meme

### 4.File Security Module :

1. Encrypting the data file.
2. File stored in the cloud can be deleted by either the group manager or the data owner.(i.e., the member who uploaded the file into the server).

### 5.Group Signature Module :

A group signature scheme allows any member of the group to sign messages while keeping the identity secret from verifiers. Besides, the designated group manager can reveal the identity of the signature's originator when a dispute occurs, which is denoted as traceability.

### 6. User Revocation Module :

User revocation is performed by the group manager via a public available revocation list (RL), based on which group members can encrypt their data files and ensure the confidentiality against the revoked users.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Monthly Peer Reviewed Open Access International e-Journal

## CONCLUSION:

In this paper, we design a secure mona protocol for data sharing in un-trusted scheme, Mona protocol for dynamic groups in an untrusted cloud. In Mona, a user is able to share data with others in the group without revealing identity privacy to the cloud. Additionally, Mona supports efficient user revocation and new user joining. More specially, 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. Moreover, the storage overhead and the encryption computation cost are constant. Extensive analyses show that our proposed scheme satisfies the desired security requirements and guarantees efficiency as well.

## Futher extension

A new type authentication system, which is highly secure, has been proposed in this paper. This system is also more users friendly. This system will definitely help thwarting Shoulder attack, Tempest attack and Brute-force attack at the client side. Though 3-dimensional Security system is a time consuming approach, it will provide strong security where the need to store and maintain crucial and confidential data secure. Such systems provide a secure channel of communication between the communicating entities.We can concentrate on preserving identity privacy for its enhancement. Interaction between the group manager and the group member should be improved.

## REFERENCES:

[1] 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.

[2] S. Kamara and K. Lauter, "Cryptographic Cloud Storage," Proc. Int'l Conf. Financial Cryptography and Data Security (FC), pp. 136-149, Jan. 2010.

[3] 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.

[4] M. Kallahalla, E. Riedel, R. Swaminathan, Q. Wang, and K. Fu, "Plutus: Scalable Secure File Sharing on Untrusted Storage," Proc. USENIX Conf. File and Storage Technologies, pp. 29-42, 2003.

[5] E. Goh, H. Shacham, N. Modadugu, and D. Boneh, "Sirius: Securing Remote Untrusted Storage," Proc. Network and Distributed Systems Security Symp. (NDSS), pp. 131-145, 2003.

[6] G. Ateniese, K. Fu, M. Green, and S. Hohenberger, "Improved Proxy Re-Encryption Schemes with Applications to Secure Distributed Storage," Proc. Network and Distributed Systems Security Symp. (NDSS), pp. 29-43, 2005.

[7] 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.

[8] B. Waters, "Ciphertext-Policy Attribute-Based Encryption: An Expressive, Efficient, and Provably Secure Realization," Proc. Int'l Conf. Practice and Theory in Public Key Cryptography Conf. Public Key Cryptography, http://eprint.iacr.org/2008/290.pdf, 2008.

[9] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data," Proc. ACM Conf. Computer and Comm. Security (CCS), pp. 89-98, 2006.

[10] D. Naor, M. Naor, and J.B. Lotspiech, "Revocation and Tracing Schemes for Stateless Receivers," Proc. Ann. Int'l Cryptology Conf. Advances in Cryptology (CRYPTO), pp. 41-62, 2001.

[11] Kallahalla, Mahesh, et al. "Plutus: Scalable Secure File Sharing on Untrusted Storage." Fast. Vol. 3. 2003.

[12] Goh, Eu-Jin, et al. "SiRiUS: Securing Remote Untrusted Storage." NDSS. Vol. 3. 2003.

[13] Ateniese, Giuseppe, et al. "Improved proxy re-encryption schemes with applications to secure distributed storage." ACM Transactions on Information and System Security (TISSEC) 9.1 (2006): 1-30.

[14] Li, Jin, et al. "Digital provenance: Enabling secure data forensics in cloud computing." Future Generation Computer Systems 37 (2014): 259-266.

[15] Waters, Brent. "Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization." Public Key Cryptography–PKC 2011. Springer Berlin Heidelberg, 2011. 53-70.