International Journal of Research
Available at https://edupediapublications.org/journals
p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 04 Issue 06
May 2017

# A Novel Architecture of Cloud Computing By User Revocation

**T.HARIPRASAD[1]& N.ASHOK[2]**

[1]M-Tech Dept. of CSE Swathi Institute of Technology & Science

[2]Assistant Professor Dept. of CSE Swathi Institute of Technology & Science

**ABSTRACT**

The advent of the cloud computing makes storage outsourcing becomes a rising trend, which promotes the secure remote data auditing a hot topic that appeared in the research literature. Recently some research considers the problem of secure and efficient public data integrity auditing for shared dynamic data. However, these schemes are still not secure against the collusion of cloud storage server and revoked group users during user revocation in practical cloud storage system. Here I figure out the collusion attack in the exiting scheme and provide an efficient public integrity auditing scheme with secure group user revocation based on vector commitment and verifier-local revocation group signature. In existing system, Kallahalla et al presented a cryptographic storage system that enables secure data sharing on untrustworthy servers based on the techniques that dividing files into file groups and encrypting each file group with a file-block key. ECC is a really amazing public key cipher that uses only basic number in its description. However, whenever a new cipher appears there will be many people that test its security and whenever possible will try to break it. So far ECC has not been broken but certain bad things can happen with it if we are not careful. As well as key size is also too length. Proposed system can achieve fine-grained access control. Registered users can use the source in the cloud and revoked users cannot access the cloud. The revoked users cannot get the original data even if they conspire with the cloud, so the system can be protected from collusion attack. Proposed system is able to support dynamic groups efficiently, when a new user joins in the group or a user is revoked from the group, the private keys of the other users do not need to be recomputed and updated. The primary benefit promised by Paillier cryptosystem is a similar key size, reducing storage and transmission requirements, and it provides the same level of security afforded by an ECC-based system with a large modulus and correspondingly larger key.

**Key words**: - Cloud Server, Group manager, Group Members, Key Distribution, Access Control, Data Confidentiality.

## 1. INTRODUCTION

Cloud computing, with the characteristics of intrinsic data sharing and low maintenance,

provides a better utilisation of resources. In cloud computing, cloud accommodation providers offer an abstraction of illimitable storage space for clients to host data. It can avail clients reduce their financial overhead of data managements by migrating the local managements system into cloud servers. However, security concerns become the main constraint when outsourcing the storage of data, which is possibly sensitive, to cloud providers. To preserve data privacy, a prevalent approach is to encrypt data files afore the clients upload the encrypted data into the cloud. Infelicitously, it is arduous to design a secure and efficient data sharing scheme, especially for dynamic groups in the cloud. Kallahalla et al presented a cryptographic storage system that enables secure data sharing on untrustworthy servers predicated on the techniques that dividing files into file groups and encrypting each file group with a file-block key. However, the file-block keys need to be updated and distributed for a utilised revocation; ergo, the system had a heftily ponderous key distribution overhead. Other schemes for data sharing on untrusted servers have been proposed in. However, the intricacies of utilised participation and revocation in these schemes are linearly incrementing with the number of data owners and the revoked users. Yu et al exploited and cumulated techniques of key policy attribute-predicated encryption, proxy re-encryption and indolent re-encryption to achieve fine-grained data access control without disclosing data contents. However, the single-owner manner may obstruct the implementation of applications, where any member of the group can utilise the cloud accommodation to store and apportion data files with others. Lu et al proposed a secure provenance scheme by leveraging group signatures and ciphertext-policy attribute-predicated encryption techniques. Each utilised obtains two keys after the registration while the attribute key is utilised to decrypt the data which is encrypted by the attribute predicated encryption and the group signature key is utilised for privacy-preserving and traceability. However, the revocation is not fortified in this scheme.

## 2. RELEGATED WORK

### 2.1Existing System

The file-block keys need to be updated and distributed for a utilised revocation; ergo, the system had a cumbersomely hefty key distribution overhead. The involutions of utilised participation and revocation in these schemes are linearly incrementing with the number of data owners and the revoked users. The single-owner manner may

obstruct the implementation of applications, where any member of the group can utilise the cloud accommodation to store and apportion data files with others.

**2.2Proposed System**

In this system, a secure data sharing scheme is proposed, which can achieve secure key distribution and data sharing for a dynamic group. A secure way for key distribution without any secure communication channels is provided. The users can securely obtain their private keys from group manager without any Certificate Ascendant entities due to the verification for the public key of the utilizer. Proposed scheme can achieve fine-grained access control, with the avail of the group utilizer list, any utilizer in the group can utilise the source in the cloud and revoked users cannot access the cloud again after they are revoked. A secure data sharing scheme which can be bulwarked from collusion assailant is proposed. The revoked users can not be able to get the pristine data files once they are revoked even if they conspire with the un trusted cloud. Proposed scheme can achieve secure utilizer revocation with the avail of the polynomial function. Proposed scheme is able to fortify dynamic groups efficiently when an incipient utilizer joins in the group or a utilizer is revoked from the group, the private keys of the other users do not require to be recomputed and updated. Security analysis to prove the security of our scheme is provided by me.

**3. IMPLEMENTATION**

**3.1Cloud:**

The cloud, maintained by the cloud service providers, provides storage space for hosting data files in a pay-as-you-go manner.

**3.2 Group manager:**

Group manager takes charge of system parameters generation, user registration, and user revocation. In the practical applications, the group manager usually is the leader of the group.

**3.3 Group members:**

Group members(users) are a set of registered users that will store their own data into the cloud and share them with others.

**3.4 Key Distribution:**

The requirement of key distribution is that users can securely obtain their private keys from the group manager without any Certificate Authorities. In other existing schemes, this goal is achieved by assuming that the communication channel is secure, however, in proposed scheme, it is achieved without this strong assumption.

**3.5Access control:**

First, group members are able to use the cloud resource for data storage and data sharing. Second, unauthorized users cannot access the cloud resource at any time, and revoked users will be incapable of using the cloud resource again once they are revoked.

**3.6Data confidentiality:**

Data confidentiality requires that unauthorized users including the cloud are incapable of learning the content of the stored data. To maintain the availability of data confidentiality for dynamic groups is still an important and challenging issue. Specifically, revoked users are unable to decrypt the stored data file after the revocation.

**3.7Efficiency:**

Any group member can store and share data files with others in the cloud. User revocation can be achieved without involving the others; this means the remaining users do not need to update their private keys.

## 4. EXPERIMENTAL RESULTS

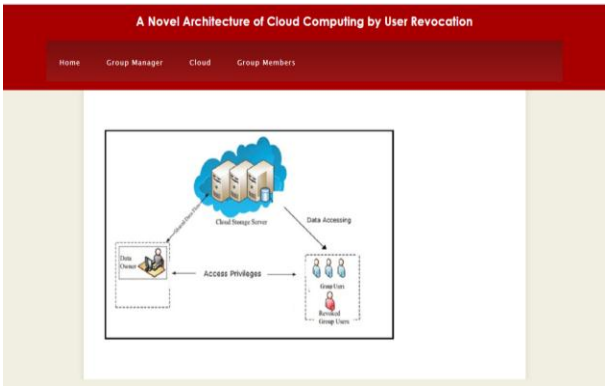


**Fig 1 Architecture Diagram**

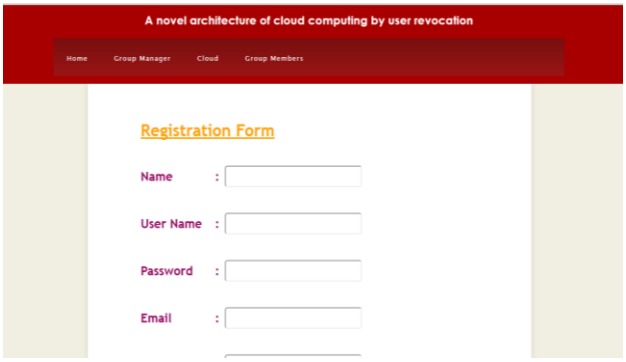


**Fig 2 Registration Page**

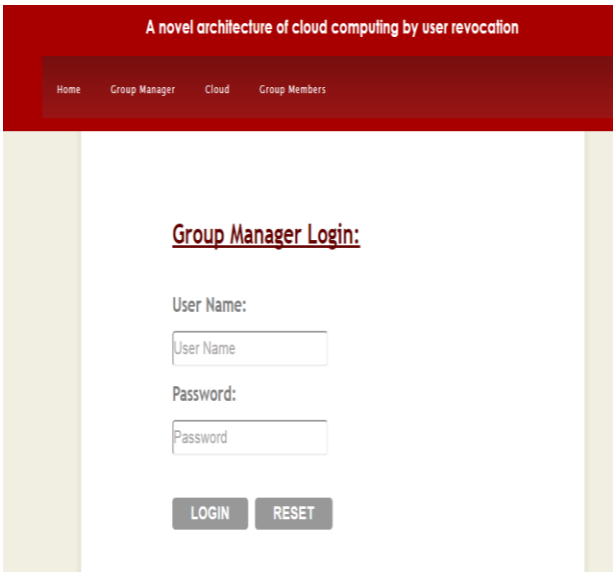


**Fig 3 Login Page**

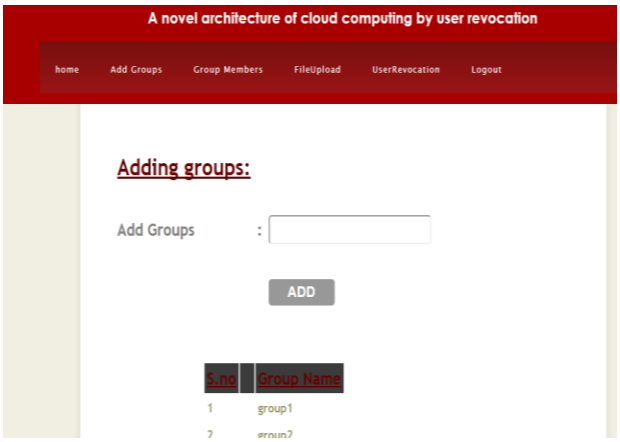


**Fig 4 Adding Groups**

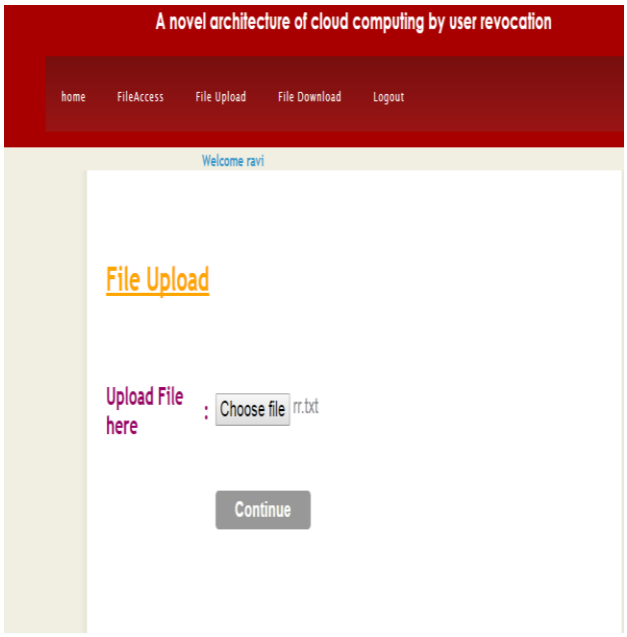


**Fig 5 File Uploading Page**

## 5. CONCLUSION

In proposed system, a secure anti-collusion data sharing scheme is designed for dynamic groups in the cloud. In proposed scheme, the users can securely obtain their private keys from group manager Certificate Authorities and secure communication channels. Also, proposed scheme is able to support dynamic groups efficiently, when a new user joins in the group or a user is revoked from the group, the private keys of the other users do not need to be recomputed and updated. Moreover, proposed scheme can achieve secure user revocation; the revoked users can not be able to get the original data files once they are revoked even if they conspire with the entrusted cloud. This project is very efficient in its execution. Although, there still exists scope for the improvement of this project in future. This project has been developed mainly by taking the example of the environment of the company. This project can be extended to the fields such as education, entertainment, various social networks and other wider areas. For example, this project can be employed in the universities to maintain the database of the students which can be used by the groups of lecturers. Here lecturer becomes the group member and the head of the department becomes the group manager. Further enhancement in the security of the data uploaded by the members can be done. This project can be enhanced by concentrating on creating subgroups in the groups and also concentrating on preserving identity privacy. Interaction between the group manager and the group member should be improved.

## 6. REFERENCE

[1] "A secure anti collusion data sharing scheme for dynamic groups in the cloud" by Zhongma Zhu , Rui Jiang, 2013.

[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] 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.

[4] 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.

[5] 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.

[6] Shucheng Yu, Cong Wang, Kui Ren, and Weijing Lou, "Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing," Proc. ACM Symp. Information, Computer and Comm. Security, pp. 282-292, 2010.

[7] 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

[8] 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.

[9] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, and M. Zaharia. "A View of Cloud Computing," Comm. ACM, vol. 53, no. 4, pp. 50-58, Apr.2010.