# Effective user management with high strength crypto –key in dynamic group environment in cloud

To cite this article: P J Kumar *et al* 2017 *IOP Conf. Ser.: Mater. Sci. Eng.* **263** 042044

# Effective user management with high strength crypto –key in dynamic group environment in cloud

**P J Kumar, P Suganya, and G Karthik**
VIT University, Vellore-632014, Tamilnadu, India.
Email: pjkumar@vit.ac.in

**Abstract.** Cloud Clusters consists of various collections of files which are being accessed by multiple users of Cloud. The users are managed as a group and the association of the user to a particular group is dynamic in nature. Every group has a manager who handles the membership of a user to a particular group by issuing keys for encryption and decryption. Due to the dynamic nature of a user he/she may leave the group very frequently. But an attempt can be made by the user who has recently left the group to access a file maintained by that group. Key distribution becomes a critical issue while the behavior of the user is dynamic. Existing techniques to manage the users of group in terms of security and key distribution has been investigated so that to arrive at an objective to identify the scopes to increase security and key management scheme in cloud. The usage of various key combinations to measure the strength of security and efficiency of user management in dynamic cloud environment has been investigated.

## 1. Introduction

Several works have discussed the architecture of data protection, key generation and distribution in the cloud or distributed environment [1-7]. The main criteria of the framework are to give secure way to deal with sharing of data between remarkable social occasion premises. With no ensured channels of correspondence we set free most secure game plan for delivering particular keys. There were couple of difficulties in the present one, just it produces single key which is extremely difficult for encryption. A revoked member can attempt to access the data maintained within the group, even after the membership has been revoked for that particular group. The existing system fails to deliver data to the genuine members even the keys are refreshed periodically. Our proposed system ensures data integrity and privacy in presence of members whose privileges to a particular group has been revoked.

## 2. Scope of the Work

We propose an ensured data sharing arrangement, which can fulfill secure key spread and data sharing for dynamic social environment in cloud. We give an ensured way to deal with key allocation with no protected correspondence channels. The key distribution to the existing group members is performed effectively so it enables only the genuine members to access data securely while thwarting the revoked members from accessing the data.

## 3. Literature Survey

**Paper Title: "**Achieving Scalable, Secure and Fine grained control access data in cloud computing"

**Authors:** Shucheng Yu, Kui Ren, Cong Wang, Weijing Lou

**Years:** 2010

**Survey:**

Accessing the resource in distributed manner in the cloud is an important characteristic. Several users can access the data maintained in the cloud proving their credentials. The credentials acquired over a data may vary dynamically. In this wander similarly as discussed before there were numerous troubles like threats on data secure and get the chance to control. To keep up protection for data out residence they ordinarily use methodologies for cryptographic by uncovering the keys of unscrambling just to the premises who are endorsed. There has been various issues like overhead of retaliation on data developed out by parasite [6]. Still various problems remain unsolved like flexibility, mystery.

**Paper Title: "**Mona: Multiple Owners sharing data for dynamic groups"

**Authors :** Yuqing Zhang, Xuefeng Liu, Boyang Wang, & Yang

**Years : 2013**

**Survey:**

Here in this article they recommended that in any scheming cloud users can share data securely. Once the malicious users acquire the credentials for a file kept in cloud , they may attempt to the scramble the contents of the file [8].

**Paper Title: "**For Group Of Multi Parasite secured data is stocked in cloud".

**Authors:** R Sarvanan, S Ramamoorthy

**Years:** 2014

**Survey:**

The work proposed user management scheme to maintain data secrecy and integrity among the users of cloud.[9]

**Paper Title: "**Securely role Based on Access control data in cloud paradigm."

**Authors:** R Pavithra, Dr.Joshi, V.Sathya priya

**Years:** 2011

**Survey:**

The proposed work discusses about maintaining key confidentiality among users to protect data from various threats.[10]

**Paper Title: "**Hierarchical identity based encryption with cipher text with size constant"

**Authors:** X Boyen, E Goh, D boneh

**Years:** 2005

**Survey:**

In HIBE [11] technique, has gathering of 3 components and to unscramble particular data it require retributions of two bilinear. This is in oracle model and it is full secured.

## 4. Architecture

Fig. 1 illustrates the proposed architecture. After each denial of parasite keys of record piece ought to be refreshed and henceforth prompting substantial dissemination of keys. In the above engineering, prior parasite qualifications are confirmed from the database and if the parasite accreditations are checked no one but parasite can get to the application and next it ventures into exchange administration. Exchange administration comprise of two levels in particular encryption and unscrambling. At prior parasite transfers data into the cloud server and for each document transferred by the parasite a key is created and later that record is scrambled, next at the collector segment encoded data is received and that data is decoded and the key is produced. Revocated parasites by the administrator can't get to these records in the gathering after once they are renounced.

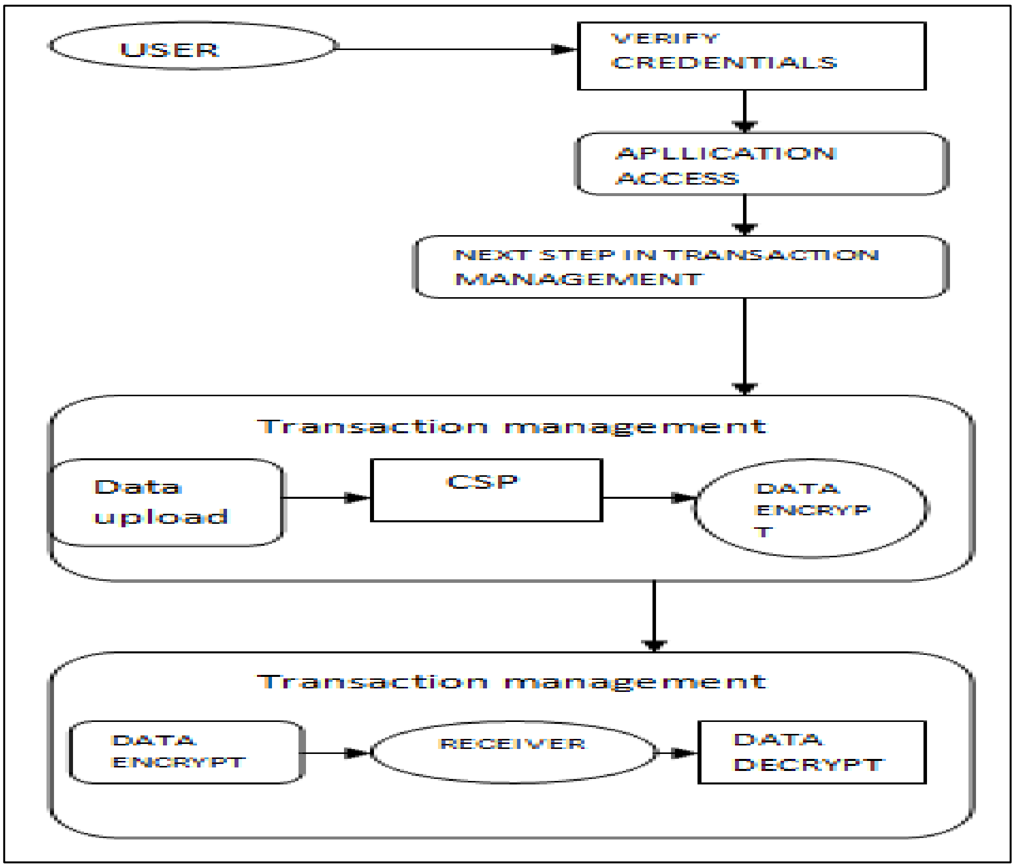

**Fig. 1.** System Architecture

### 4.1 Functional Modules

There are different modules used in the process, they are:

- User interaction
- Message Transmission
- Key Distribution
- User access control
- Confidentiality of data

### 4.2 User Interaction

This plan is the prior in our module. The fundamental part and goal is to move login screen to move to parasite window. We have made this for surety concern. JSP is utilized for outlining. Here prior parasite will enter their points of interest then our plan will check their accreditations in the database of the server and certifications coordinated then just it will be signed in , this is an extraordinary secure in our framework. In the event that certifications don't coordinate it will indicate mistake message.

### 4.3 Message Transmission

This module causes us in sending records over capacity of cloud. We can utilize many cloud specialist organization and utilize the cloud and we can pay as we go. Means we can pay just for our use in cloud. Here parasites can stock their data in cloud and can impart them to others securely with no issue. Client ship of gathering is changed progressively because of each time new enlistment happens and furthermore renouncement of parasite. Here parasites can stock their documents either private or openly as their comfort. After encryption records are protected in the nodes of cloud. For each private record and open document transferred a remarkable key is produced and along these lines giving more secure to our data subcontract.

### 4.4 Key Distribution

Compared to the existing techniques to distribute the key to the users of the group, we take keys which consist of large numbers of diverse elements and which undergoes several permutations and combinations. By increasing the size of the key, it increases the number of unique keys that can be generated for different user which would avoid the repetition. We include in the key a field to identify the current validity of the user to a particular group. When the user is no longer a member to a group , the field in the key is invalidated which makes the user not to access the file available in the group.

### 4.5 User Access Control

Here premises of gathering can transfer records and it is checked and after that it is changed over to scramble arrange. Parasites can reclaim data by giving the keys given and data is decoded and download to nodes which are eligible. Archives which are freely transferred can decode by open keys and the other way around for private documents with private keys.

### 4.6 Confidentiality of Data

In this venture parasites repudiated can't have the capacity to decode the records of their premises in gathering. Along these lines outsourced data are kept secret and furthermore secure at the same time.

## 5. Results and Discussion

| | Key distribution securely | Control access | User revocation | Anti-collusion attack | Confidentiality of data |
|---|---|---|---|---|---|
| ODBE | | Y | Y | Y | |
| RBAC method | | Y | | | |
| MONA | | Y | | | |
| Our method | Y(with more key strengh) | Y | Y | Y | Y |

### 5.1 Performance Comparison

Here from the above table we can see that our framework is more reasonable and moreover more definitive and we satisfy this in more secure way. We have demonstrated examination between various plans like RBAC, MONA, ODBE and we can see that our strategy is more beneficial and bringing many components at one place.

## 6. Conclusion and Future Work

Various user management schemes available in the literature have been studied to effectively handle the user mobility. Several key based user handling mechanism have been proposed in the literature. The validity of a user to a particular group in the cloud is handled effectively when the user leaves. Modifications are done to key exchanging process and the field in the key to handle user effectively with more security. A specific field in the key identifies the current validity of a user to a particular group and automatically denies access to the group if the user had left the group recently. As part of future work, it is planned to test the proposed approach in Cloud Simulation environment.

## 7. References

[1] M. Armbrust, A.D. Joseph, A. Fox, R. Katz, A. Konwinski, R. Griffith, G. Lee, A. Rabkin, D. Patterson, I. Stoica and M. Zaharia. (2010 ), “CLOUD COMPUTING VIEW,” , ACM, .**53**, no.4, 50-58.

[2] S. Kamara and K. Lauter (2010), “cloud storage cryptographic”, Proc. Intl conf. Data surety & financial cryptographic (FC), 136-149.

[3] M. kallahalla, R. Swaminathan, E.Riedel, K. Fu, Q. Wang (2003), “Plutus: Secure Scalable sharing file on storage on untrusted storage” , Proc.UNENIX Conf.Storage and file Technologies, 29-42,

[4] H. Shacham, D. Boneh, N. Modadugu, E. Goh (2003), “Sirius: Securing Remote Untrusted storage” Proc. Network and systems which is distributed surety symp. (NDSS), 131-145.

[5] K. Fu, S. Hohenberger, G. Ateniese, M. Green (2005), “Improved proxy re encryption schemes with applications to secure distributed storage,” proc.Network and distributed systems surety symp, (NDSS), 29-43.

[6] Cong Wang, Kui Ren, Shucheng Yu, Weijing Lou (2010), “Achieving Secure, Scalable, And Fine grained data access control in cloud computing”, Proc. ACM symp. Information, Comm & computer surety, 282-292.

[7] A. Sahai, B. Waters, V. Goyal, O. pandey (2006), “Attribute based encryption for fine grained access control of encrypted data,” Proc. ACM conf. Comm. & computer surety, (css) pg: 89-98, 2006.

[8] Jingbo Yang, Xuefeng Liu, Boyang Wang, Yuging Zhang (2013), “Mona: Secure multi owner data sharing for dynamic groups in the cloud” IEEE transactions on distributed and parallel systems, Vol. **24**, no 6, 1182-1191.

[9] R. Saravanan, S. Ramamoorthy (2014) , “for group of multi parasite secured data is stockd in cloud”, 49-56

[10] R. Pavithra, Dr. Joshi, V. Sathya priya (2011), “securely role based on access control data in cloud paradigm” , 89-95.

[11] E. Goh, D. Boneh, X. Boyen (2005), “Hierarchical identity based encryption with cipher text with size constant” , 112-119.