ISSN XXXX XXXX © 2018 IJESC

Research Article Volume 8 Issue No.6

# An Efficient Anti-Collusion Data Sharing Mechanism for Data Confidentiality for Dynamic Groups

Pawan Kumar Singh[1], Akash Bhardwaj[2], Abhisheka Swami[3], Aheraaz Tamboli[4], Vina M. Lomte[5]
BE Student[1, 2, 3, 4], HOD[5]
Department of Computer Engineering
RMD Sinhgad School of Engineering, Pune, India

**Abstract:**
Providing efficient as well as cost effective approach for data sharing is one of the characteristics of cloud computing. User attains less for management and maintenance cost. In public clouds when data is shared across dynamic groups, there can be rapid user revocation from one group to other. In this paper we are providing secure user revocation using key distribution among the group members. When any user revokes from one group to other, private key of the revoked user gets changed. Along with this private keys of all previous group member gets changed. Fine grained access control is achieved using three factor authentications, one through user password, second through otp at first login and third through token. System also secures when same files are uploaded and when user from one group tries to access file from another group, he is identified as a fake user and will not be able to access the application further.

**Key Words:** Access control, privacy-preserving, key distribution, cloud computing, user revocation

## 1. INTRODUCTION

Cloud computing is an Internet-based computing that provides computer-shared computer processing resources and data and other devices on demand. It is a computing style where dynamically scalable and often virtualized resources are provided as an Internet service. One of the most basic services offered by cloud providers is data storage. Let us consider a practical data application. A company allows its employees in the same group or department to archive and share files in the cloud. However, it also represents a significant risk for the confidentiality of stored files. A company allows its staff to be in the same group or department to file and share files in the cloud. However, it also represents a significant risk for the confidentiality of stored files. In particular, cloud-managed cloud servers are not trusted by users, and data files stored in the cloud can be sensitive, such as business plans. To safeguard data privacy, a basic solution is to encrypt data files and upload encrypted data to the cloud. Identity privacy is one of the most significant obstacles to the widespread implementation of cloud computing. Without the guarantee of identity privacy, users may not be willing to join cloud computing systems because their real identities could easily be revealed to cloud providers and Attackers. On the other hand, unconditional privacy of identity may result in privacy abuse. For example, the wrong staff can trick others into the company by sharing fake files without being traced. Therefore, traceability, which allows the group manager to reveal the actual identity of a user, is also highly desirable. It is recommended that all members of a group can enjoy full cloud storage and sharing services, defined as multi-owner mode. Compared to the unique owner mode, where only the group manager can store and edit data in the cloud, owner multiple mode is more flexible in practical applications. Specifically, each user in the group can not only read the data, but also modify their part of the data across the entire data file shared by the company. Finally, groups are usually dynamic in practice, for example, a new employee involvement and the current employee revocation in a company. Changing affiliates makes it very difficult to exchange data. On the one hand, the anonymous system challenges new users to know the contents of the stored data files before they participate, as it is impossible for new users to contact anonymous data owners and get their decryption keys. On the other hand, you also need an effective member revocation mechanism without updating the secret keys of remaining users to minimize the complexity of key management. Several security schemes have been proposed for data sharing and falsity servers. In these approaches, data owners store the encrypted data files in a trusted archive and distribute the corresponding decryption.

## 2. LITERATURE SURVEY

In this paper "Cryptographic cloud storage" [1], The cloud provider one of the best services is data storage the security and privacy issue have major concern for organization for utilizing such service. Cloud data storage has provided significant benefits by allowing users to store massive amount of data on demand in a cost-effective manner. To protect the privacy of data stored in the cloud, cryptographic role-based access control (RBAC) schemes have been developed to ensure that data can only be accessed by those who are allowed by access policies. However these cryptographic approaches do not address the issues of trust. In this paper, we propose trust models to reason about and improve the security for stored data in cloud storage systems that use cryptographic RBAC schemes. The trust models provide an approach for the owners and roles to determine the trustworthiness of individual roles and users respectively in the RBAC system. The proposed trust models take into account role inheritance and hierarchy in the evaluation of trustworthiness of roles. We present a design of a trust-based cloud storage system which shows how the trust models can be integrated into a system that uses cryptographic RBAC schemes. We have also considered practical application scenarios and illustrated how the trust evaluations can be used to reduce the risks and enhance the quality of decision making by data owners and roles of cloud storage service. In this paper "Sirius: Securing remote entrusted storage" [2], It is a greatest platform that provides data storage in very lesser cost and all time it should be available over the internet. The security must be important in the cloud computing. The encryption technique is commonly adopted by the cloud computing that means the encrypted data should be stored on the

storage of cloud to protect the data. Encryption is no sufficient as organization obtain have to enforce fine-grained access control on data. Such control is based on the attribute that system is known as the attribute based system. For the data privacy it is important to encrypt the data and upload the encrypted data on the cloud. In cloud it is not easy to design efficient and secure data sharing scheme in multi owner system due to the following challenging issues. Identity, revocation and new member participation i.e. the changes of membership make securely data sharing extremely difficult. On the other hand an efficient member revocation without updating the secret key of remaining user to minimize the complexity of key management. Signed receipt is caused after every member revocation in group that minimizes multiple copy of encrypted file it can help to minimize computation cost. In this paper "Plutus: Scalable Secure File Sharing on Untrusted Storage" [3], Presented cryptographic storage system that enable secure data sharing. In this technique dividing file into the file group and encrypt each file group with a file block key. In this scheme at the time of user revocation the file block key need to be updated and distributed to the user therefore the system had a heavy key distribution overhead. Plutus is a cryptographic storage system that enables secure file sharing without placing much trust on the file servers. In particular, it makes novel use of cryptographic primitives to protect and share files. Plutus features highly scalable key management while allowing individual users to retain direct control over who gets access to their files. We explain the mechanisms in Plutus to reduce the number of cryptographic keys exchanged between users by using file groups, distinguish file read and write access, handle user revocation efficiently, and allow an untrusted server to authorize file writes. We have built a prototype of Plutus on OpenAFS. Measurements of this prototype show that Plutus achieves strong security with overhead comparable to systems that encrypt all network traffic. to the success of data forensics in cloud computing, yet it is still a challenging issue today. In this paper, to tackle this unexplored area in cloud computing, we 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. With the provable security techniques, we formally demonstrate the proposed scheme is secure in the standard model. In this paper "Secure Provenance: The Essential of Bread and Butter of Data Forensics in Cloud Computing"[4], Secure provenance that records ownership and process history of data objects is vital to the success of data forensics in cloud computing, yet it is still a challenging issue today. In this paper, to tackle this unexplored area in cloud computing, we 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. With the provable security techniques, we formally demonstrate the proposed scheme is secure in the standard model. In this paper "Fine Grained Two Factor Access Control for web based cloud computing Services"[5], In this paper, we introduce a new fine-grained two-factor authentication (2FA) access control system for web-based cloud computing services. Specifically, in our proposed 2FA access control system, an attribute-based access control mechanism is implemented with the necessity of both a user secret key and a lightweight security device. As a user cannot access the system if they do not hold both, the Mechanism can enhance the security of the system, especially in those scenarios where many users share the same computer for web-based cloud services. In addition, attribute-based control in the system also enables the cloud server to restrict the access to those users with the same set of attributes while preserving user privacy, i.e., the cloud server only knows that the user fulfils the required predicate, but has no idea on the exact identity of the user. Finally, we also carry out a simulation to demonstrate the practicability of our proposed 2FA system. In this paper "Optimal Coding and Allocation for perfect Secrecy in multiple cloud"[6], For user to store data in the cloud, using services provided by multiple cloud storage providers (CSPs) is a promising approach to increase the level of data availability and confidentiality, as it is unlikely that different CSPs are out of service at the same time or collude with each other to extract information of a user. This paper investigates the problem of storing data reliably and securely in multiple CSPs constrained by given budgets with minimum cost. Previous works, with variation in problem formulation typically trickle the problem by decoupling it into sub problem and solve them separately. In this paper "Circuit Cipher text- policy Attribute based Hybrid encryption with verifiable Delegation in cloud computing"[7], In the cloud, for achieving access control and keeping data confidential, the data owners could adopt attribute-based encryption to encrypt the stored data. Users with limited computing power are however more likely to delegate the mask of the decryption task to the cloud servers to reduce the computing cost. As a result, attribute-based encryption with delegation emerges. Still, there are caveats and questions remaining in the previous relevant works. For instance, during the delegation, the cloud servers could tamper or replace the delegated cipher text and respond a forged computing result with malicious intent. They may also cheat the eligible users by responding them that they are ineligible for the purpose of cost saving. Furthermore, during the encryption, the access policies may not be flexible enough as well. Since policy for general circuits enables to achieve the strongest form of access control, a construction for realizing circuit cipher text-policy attribute-based hybrid encryption with verifiable delegation has been considered in our work. In such a system, combined with verifiable computation and encrypt-then-mac mechanism, the data confidentiality, the fine-grained access control and the correctness of the delegated computing results are well guaranteed at the same time. Besides, our scheme achieves security against chosen-plaintext attacks under the k-multilinear Decisional Diffie-Hellman assumption. Moreover, an extensive simulation campaign confirms the feasibility and efficiency of the proposed solution. In this paper "Secure Data Sharing in Cloud Computing using Revocable Storage identity based encryption" [8],Cloud computing provides a flexible and convenient way for data sharing, which brings various benefits for both the society and individuals. But there exists a natural resistance for users to directly outsource the shared data to the cloud server since the data often contain valuable information. Thus, it is necessary to place cryptographically enhanced access control on the shared data. Identity-based encryption is a promising crypto graphical primitive to build a practical data sharing system. However, access control is not static. That is, when some user's authorization is expired, there should be a mechanism that can remove him/her from the system. Consequently, the revoked user cannot access both the previously and subsequently shared data. To this end, we propose a notion called revocable-storage identity-based encryption (RS-IBE), which can provide the forward/backward security of cipher text by introducing the functionalities of user revocation and cipher text update simultaneously. Furthermore, we present a concrete construction of RS-IBE, and prove its security in the defined security model. The performance comparisons indicate that the proposed RS-IBE

scheme has advantages in terms of functionality and efficiency, and thus is feasible for a practical and cost-effective data-sharing system. Finally, we provide implementation results of the proposed scheme to demonstrate its practicability.

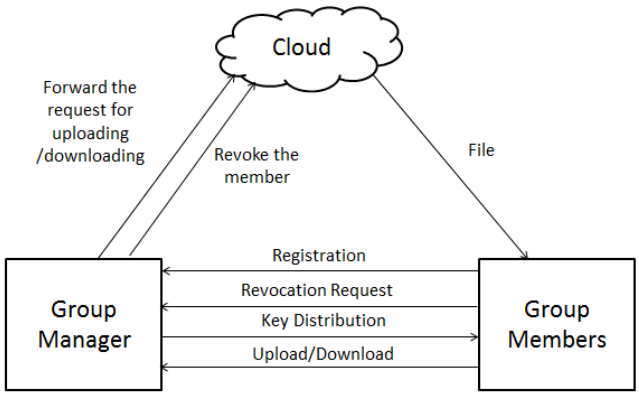
## 3. PROPOSED SYSTEM

### 3.1 Problem Definition

To provide secure as well as efficient user revocation for dynamic groups. At the same time only authenticated user should be able to get the data stored on cloud.

### 3.2 Proposed System Overview

In this system propose a secure data sharing scheme, which can achieve secure key distribution and data sharing for dynamic group. The system provides a secure way for key distribution without any secure communication channels. The users can securely obtain their private keys from group manager without any Certificate Authorities due to the verification for the public key of the user. The system can achieve fine-grained access control, with the help of the group user list, any user in the group can use the source in the cloud and revoked users cannot access the cloud again after they are revoked. Secure data sharing scheme which can be protected from collusion attack. The revoked users can not be able to get the original data files once they are revoked even if they conspire with the untruth cloud. Our scheme can achieve secure user revocation with the help of polynomial function. 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. System will provide security analysis to prove the security of our scheme.




**1. Group Member or User Module :**

Every user needs to register with corresponding group for getting access permission using signature key. They can get access permission. They can upload files to cloud. Members from same group can view the content of file over simultaneously they can download the file as well

**2. Group Manager Module:**

Responsible for providing and denying access permission to the members of various groups. Manager has the main access permission for maintaining the files over cloud. Manager can navigate through the group as well. Manager can view the log details of activities carried on cloud file storage.

### 3.2 Algorithm

**Algorithm 1: AES Algorithm**

AES (advanced encryption standard).It is symmetric algorithm. It used to convert plain text into cipher text. The need for coming with this algorithm is weakness in DES. The 56 bit key of des is no longer safe against attacks based on exhaustive key searches and 64-bit block also consider as weak. AES was to be used128-bit block with128-bit keys.Rijendeal was founder. In this drop we are using it to encrypt the data owner file.

Input:
128_bit /192 bit/256 bit input (0,1)
Secret key (128_bit)+plain text(128_bit).
Process:
10/12/14-rounds for-128_bit /192 bit/256 bit input
XOR state block (i/p)
Final round: 10, 12, 14
Each round consists: sub byte, shift byte, mix columns, add round key.
Output:
Cipher text (128 bit)

**Algorithm 2: Blowfish Algorithm**

It is having a function to iterate 16 times of network. Each round consists of key-dependent permutation and a key and data-dependent substitution. All operations are XORs and additions on 32-bit words. The only additional operations are four indexed array data lookup tables for each round.
Divide x into two 32-bit halves: xL, xR
For i = 1to 16:
xL = XL XOR Pi
xR = F(XL) XOR xR
Swap XL and xR
Swap XL and xR (Undo the last swap.)
xR = xR XOR P17
xL = xL XOR P18
Recombine xL and xR

### 3.3 Mathematical Model

Input: File Upload F
Process: -

$S=\{s, e, X, Y, \Phi\}$
Where,
s = Start of the program.
1. Log in with webpage.
2. Load Files on cloud.
e = End of the program.
Retrieve the file from cloud storage system.
X = Input of the program.
Input should be File.
Y = Output of the program.
File will be first uploaded then search and send key and download the file

$X, Y \in U$
Let U be the Set of System.
U= {GM,GU, S, G, D}
Where GM, GU , F, S, T, M, D are the elements of the set.
GM=Group Manager
GU=Group User
S=Search keyword
G=Get key from user
D=Download file using key
Output: Get File f from Group

## 4. RESULTS AND DISCUSSION

### 4.1 Experimental Setup

The Introduction of software requirements speciation provides an overview of all software used in Projects which used the operating system window 7,8,10. The Language used to implementation is java which required the JDK (Java SE Development kit) JDK have many version such as the 1.2, 1.3 and up to 1.7. Platform which used for JDK is eclipse, eclipse have lots of the version. To run the code in eclipse required the Server as the Apache tomcat 7.Data base used is MYSQL version 5.

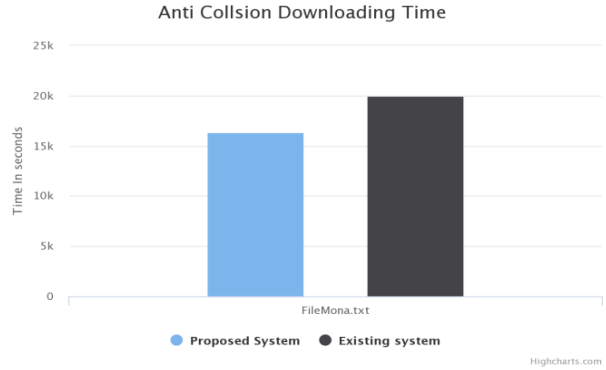
### 4.2 Expected Result

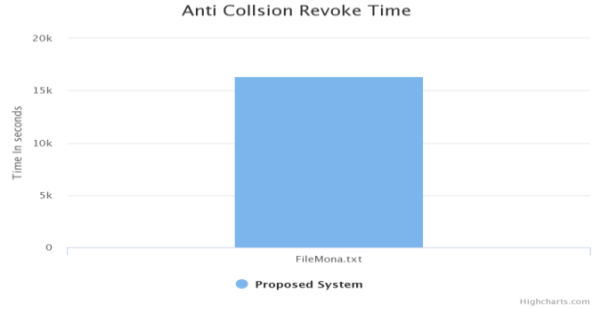
We expect the comparison of some Security parameter OBBE, Mona and Our Scheme. It is obviously observed that computation cost for members in our scheme is irrelevant to number of revoked users.

### 4.3 Comparisons

| Schemes | Secure Key distribution | Access control | user re-vocation | Anti-collusion attack | Data confi-dentiality |
|---|---|---|---|---|---|
| Mona | - | Yes | - | - | - |
| ODBE | - | Yes | Yes | Yes | - |
| Re-Encryption(Prosed scheme) | Yes | Yes | Yes | Yes | Yes |

| Number | Factor | AES | Blowfish |
|---|---|---|---|
| 1. | Key Length | AES accepts keys of 128, 192 or 256 bits (128 bits is already very unbreakable), uses 128-bit blocks | Blowfish is 64 bits. Blowfish is efficient in software, at least on some software platforms (it uses key-dependent lookup tables, hence performance depends on how the platform handles memory and caches). |
| 2. | Cipher Type | Symmetric Block cipher | Symmetric Block Algorithms |
| 3. | Round | 10,12 and 14 resp. | 16 |




## 5. CONCLUSION AND FUTURE SCOPE

Overhead of key distribution can managed more efficiently with some other mechanism. For creation of digital signature we used RSA and SHA algorithm but using this algorithm it increases the key computation. So to reduce key management process we will use Two Fish algorithm in future.


## 6. ACKNOWLEDGEMENT

It is my privilege to acknowledge with deep sense of gratefulness to my guide Prof. Vina M. Lomte, Head of the Department, RMDSSOE(Computer Science) for her kind cooperation, valuable suggestions and capable guidance and timely help given to me in completion of my paper.


## 7. REFERENCES


[1].S.Kamara and K. Lauter, "Cryptographic cloud storage," in Proc. Int. Conf. Financial Cryptography Data Security, Jan. 2010, pp. 136–149.

[2].E. Goh, H. Shacham, N. Modadugu, and D. Boneh, "Sirius: Securing remote entrusted storage," in Proc. Netw. Distrib. Syst. Security Symp., 2003, pp. 131–145.

[3].M. Kallahalla, E. Riedel, R. Swaminathan, Q. Wang, and K. Fu, "Plutus: Scalable secure file sharing on untrusted storage," in Proc. USENIX Conf. File Storage Technol., 2003, pp. 29–42.

[4].R. Lu, X. Lin, X. Liang, and X. Shen, "Secure provenance: The essential of bread and butter of data forensics in cloud computing," in Proc. ACM Symp. Inf., Comput. Commun. Security, 2010, pp. 282–292.

[5].Joseph K. Liu, Man Ho Au, Xinyi Huang, Rongxing Lu, Jin Li,"Fine Grained Two Factor Access Control for web based cloud computing Services"

[6].Ping Hu, Chi Wan Sung ,Siu-Wai Ho,Terence H. Chan, "Optimal Coding and Allocation for perfect Secrecy in multiple cloud"

[7]. Jie Xu, Qiaoyan Wen, Wenmin Li, Zhengping Jin, "Circuit Ciphertext-Policy Attribute-Based Hybrid Encryption with Verifiable Delegation in Cloud Computing Sign In or Purchase"

[8].Jianghong Wei, Wenfen Liu, Xuexian Hu, "Secure Data Sharing in Cloud Computing using Revocable Storage identity based encryption"