IOSR Journal of Engineering (IOSRJEN) **www.iosrjen.org**
ISSN (e): 2250-3021, ISSN (p): 2278-8719
PP 15-19

Secure Multi Owner Data Sharing For Dynamic Groups In The Cloud

S.Seethalakshmi[1], S. Saraswathi[2], Dr.V.Raji[3]
[1,2]Deptofcomputerscienceandengineering,SKPEngineeringCollege, Tiruvannamalai
[3]Assistant Professor, Dept of computer science and engineering , SKP Engineering College, Tiruvannamalai
Corresponding author: S.Seethalakshmi[1]

Abstract: The main purpose of our paper is to share the data in the cloud. In this paper, we shown that how to share information securely, efficiently and flexibly with others on cloud storage. For this, we propose key aggregate cryptosystem, which creates a standard size cyber text, which can assign them to such encryption rights. By combining a secret key, we can create a small single key. By using this compact key, we can send others or save in a much less secure storage. First, setting up the next general layout of the data owner The KeyGen algorithm creates a general or master / secret key. By using this key, a user can convert simple text to speech. The next user will give input as the primary secret key through the extract function; It produces output as the overall cryptographic force. The main created this is sent to the secure recipient. Then the user can encrypt the encryption with a full keyboard and the user encryption function. The proper security analysis of our plans is provided in the standard plan. We also describe other applications of our plans. In particular, our programs provide the first public key patient control code for a flexible step, which is not yet known. Cloud Storage has recently gained popularity. In enterprise systems, we find data increases the need for data outsourcing to help enterprise data management. It is also used as a key technology behind.
Keywords: Data Sharing, Dynamic Groups, Cloud, Cryptosystem.

I. Introduction

The CLOUD System provides an excellent utility for resources, with internal data sharing and minimal maintenance properties.Thecloud[1]service providers a infinite storage space to provide customers with data. Moving local admin settings on client servers helps to reduce customer data management. However, by now outsourcing storage of more information, it becomes a safe and important security feature. To protect data privacy, data encryption is a common approach before the client uploads the encrypted data[2] in the client. Unfortunately, it is difficult to design a secure[3] and efficient data sharing program, especially for dynamic groups in the cloud. Cloud Computing is the hardware and software application offered as a service on a network. This name comes from the general use of a cloud-shaped code for complex infrastructure in system diagrams. Cloud computing enters remote services[4] with a user's data, software, and accounting. Hardware and software sources available on the Internet in cloud computing are managed by third-party services. These services generally provide access to top networks of advanced software applications and server systems. In Cloud Computing, Cloud Service Providers (Additional Service Providers) can offer various services to cloud users with the help of powerful data centre such as Amazon. By changing local data management systems to cloud servers, users can enjoy high quality services and save substantial investments in their local infrastructure.

II. Literature Survey

[6] This paper had openness issues and access principles which are based on data attributes. Another challenge is the data control of calculation are involving well-calculated data. The data owner allows access to basic data contents without access to control clouds. Our proposed program has the security of user access privilege and has the key features of the key properties and user's secret.

[7] This document uses the novel of cryptographic standards used for the safety of the safe storage in the presence of trusted servers and the desire for a major distribution managed by the owner. The server believes that the server trusts the basis of a safe saving system in the hands of the owner of the personal data (and so we can detect if we do not need to destroy the data today - and so we can detect if they do) and keep key supplies (and therefore access control) Protect and share data.

[8] This article includes SiRiUS, Secure File System, Unsafe Network and NFS, CIFS, Seafood Store and Yahoo! Designed to lay out the P2P file systems. SiRiUS is unreliable to network storage and provides its own read-write encryption access control for file system sharing. Key management and withdrawal are at least out-of-the-band communication. The file system supports freshness warranties SiRiUS hash using tree structures. SiRiUS features a new method for performing system file system operation in an encryption file without the use of the volume server.
[9] This paper is anonymous authorization for user access, and tracking controversial documents by providing information confidentiality in important documents that are stored in the cloud in the proposed program. With a proven security technique, we guarantee the proposed project to be secured in a stable model.
[10] This paper presents a new method of realizing the cyber text under the concrete and interactive encryption assumptions in the standard model of Policy Attributation (Communist Abbey). Our solutions allow us to specify access control indicators on the basis of any accessibility on the system's properties. In our most sacred manner, linear mode with the complexity of the ciphertext size, encryption and encryption method access formula. The only previous task to achieve these parameters was just a source of the general group model.
[11] This paper provides important information that is shared and stored by third-party sites on the website, and is required to encrypt the data stored on these sites. Encryption data is a disadvantage, it can only be selected at a rustful level (ie, give your personal key to another party). We create a new encryption method for encrypted data encrypted partitions, and we call main policy attribute-based encryption (KP-ABE). Our cryptography, siftaretes attributes and private key boxes access structures are labeled cipher tags which can be a user decrypt controlling. We demonstrate the use of our construction to share the censorship-record information and broadcast encryption.
[5] This paper is a "divided property." Any subset-coating that does not require this mechanism can be integrated with the project. The length of a traitor that does not extend the range, and range of traitors that a general traitor gives a general traitor to track the mechanism.

III. System Design

3.1Existing System:

Some security plans have been proposed to participate in various meetings in cloud unreliable servers. These methods, the communication owners are surrounded by coding keys that are only relevant to customers who have secured and disconnect the disclosed information documents with reliable information. Within these lines, unauthorized customers in cloud and efficient servers can't take the goods in documents, although they do not contain information on encryption keys, however, the customer support and disavowal's problems directly expand in these projects. Information owners and the number of individually abandoned customers. By setting up a unique group. A safe product plan was proposed to consider the characteristic coding system of the simulated content arrangement to implement any part of a meeting to provide information to others.

Disadvantages of existing system:

- It does not provide security for sharing the data within the groups.
- It does not provide privacy preserving access control to the users.

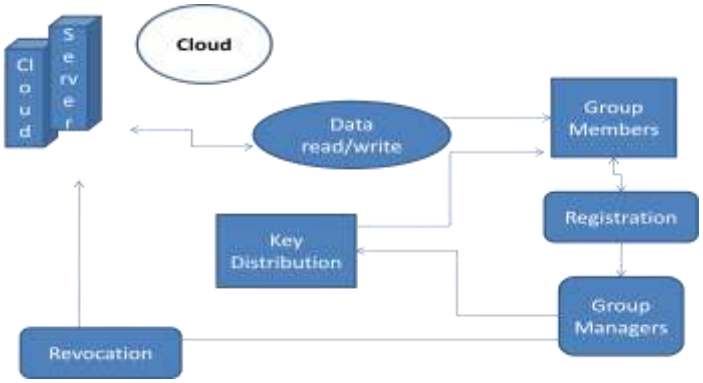
3.2 Proposedsystem:

This paper, we propose a secure multiowner data sharing scheme, said to be Mona, for dynamic groups in the cloud. Using cloud signature and dynamic encryption methods, any cloud client can provide information securely to other clients. Meanwhile, the storage overhead and encryption computation cost of our scheme are independent with the number of revoked users. Furthermore, we break the security of cloud in further verification information, and we demonstrate the efficiencies of our dynamic meetings taking tests.

Advantages of 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.
- Cloud clients provide security and security access controls, which ensure that any part of a dynamic collection is secretly used by the Cloud Asset.

System Architecture:



Group Member should register to join in the group. In the registration form group member should enter the valid Email Id. Group Manager will send a 16bit Private key by using SMTP protocol through the registered Email. Now a group member can access the cloud by Data read and write into the cloud. Group Managers can revocate the group member.

IV. High-level description of the algorithm

Step 1: Key Expansion—round keys are derived from the cipher key using Rijndael's key scheduleInitial Round.
Step 2: AddRoundKey—each byte of the state is combined with the round key using bitwise xorRounds
Step 3: SubBytes—a non-linear substitution step where each byte is replaced with another according to lookup.
Step 4: ShiftRows—a transposition step where each row of the state is shifted cyclically a certain number of steps.
Step 5: MixColumns—a mixing operation which operates on the columns of the state, combining the four bytes in each column.
Step 6: AddRoundKey
Step 7: Final Round (no MixColumns)
Step 8: SubBytes
Step 9: ShiftRows
Step 10: AddRoundKey

V. Implementation:

The implementation stage consists ofplanning,investigation of the existing system and implementing proposed system in the evalution of change over method

5.1 Module Description

5.1.1 User Registration:

For the registration of user with identity ID the groupmanager randomly selects a number. Then the group manager adds into thegroup user list which will be used in the traceability phase. After the registration, user obtains a private keywhich will be used for group signature generation and file decryption.

Fig 1: User Registration form

5.1.2.User Revocation:

User revocation is performed by the group manager via apublic available. Revocation list, based on which groupmembers can encrypt their data files and ensure theconfidentiality against the revoked users. Group manger update therevocation list each day even no user has being revoked inthe day. In other words, the others can verify the freshnessof the revocation list from the contained current date.

Fig2: User Revocation

5.1.3File Generation and Deletions:

To store and share a data file in the cloud, a group memberperforms to getting the revocation list from the cloud. In thisstep, the member sends the group identity ID group asa request to the cloudVerifying the validity of the received revocation list.File stored in the cloud can be deleted by either the groupmanager or the data owner.

Fig3: FileGeneration

Fig3.1:FileDeletion

5.1.4 File Access and Traceability:

To access the cloud, a user needs to compute a groupsignature for his/her authentication. The employedgroup signature scheme can be regarded as a variant ofthe short group signature which inherits the inherentenforceability property, anonymous authentication, andtracking capability. When a data dispute occurs, the tracing operation isperformed by the group manager to identify the realidentity of the data owner.

Fig 4: File Access and Traceability

VI. Conclusion:

In this paper, we build the key-management cryptosis for scalable data sharing in cloud strokes. In Mona, a client can provide information to others in the collection without finding out the cloud privacy. Additionally, the strong client isdeniedto join with the administrator in powerful gathering. Customers can reinstall customers' private keys with an ineligible client list with an invalid client denial, and new clients can specifically target the logs recorded in the cloud prior to their cooperation. In addition, the efficiency of the cloud and coding cost is increasing. The vast experiment demonstrates that our proposed conspiracy meets the requirements of the security and confirms productivity. An encryption manual framework was proposed for the safe record sharing of Plutus in unreliable servers. Divide documents into folders and mark each file group with a square, and share the lock key with the owner of the information owner, which is used to make the document lock key to the lock key. However, it feels considerable significant displacement for extensive document sharing. Furthermore, the registration piece should be rearranged and the customer will be rediscovered for denial.

References:

[1]. 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," Commun. ACM, vol. 53, no. 4,pp. 50–58, Apr. 2010.

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

[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]. E. Goh, H. Shacham, N. Modadugu, and D. Boneh, "Sirius: Securingremote untrusted storage," in Proc. Netw. Distrib. Syst. SecuritySymp., 2003, pp. 131–145.

[5]. G. Ateniese, K. Fu, M. Green, and S. Hohenberger, "Improvedproxy re-encryption schemes with applications to secure distributedstorage," in Proc. Netw. Distrib. Syst. Security Symp., 2005,pp. 29–43.

[6]. Shucheng Yu_, Cong Wang, KuiRen, and Wenjing Lou, "Achieving Secure, Scalable, and Fine-grained DataAccess Control in Cloud Computing",

[7]. MaheshSan Francisco," Plutus: Scalable secure file sharing on untrusted storage" March 31–April 2, 2003

[8]. Eu-Jin Goh, HovavShacham, NagendraModadugu, Dan Boneh, "SiRiUS: Securing Remote Untrusted Storage",

[9]. Rongxing Lu, Xiaodong Lin, Xiaohui Liang, and Xuemin (Sherman) Shen, "Secure Provenance: The Essential of Bread and Butter of Data Forensics in Cloud Computing",

[10]. Brent Waters, "Ciphertext-Policy Attribute-Based Encryption:An Expressive, E_cient, and Provably Secure Realization"

[11]. VipulGoyal, Omkant Pandeyy,Amit Sahaiz Brent, Waters, " Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data"