© 2016 IJSRSET | Volume 2 | Issue 4 | Print ISSN: 2395-1990 | Online ISSN : 2394-4099
Themed Section: Engineering and Technology

Enhancing the Security for Multi-Owner Data Sharing (MODS) Groups in the Cloud with Improved Dynamism

Dr. D .Ravindran, S. Sahaya Nirmala Daisy

School of Computer Science, St. Joseph's College, Trichirapalli-2, Tamil Nadu, India

ABSTRACT

Cloud Computing is a developing technology that uses the internet and central remote servers to maintain data and applications. Cloud computing permitscustomers and businesses to use requests without connection and access their private files at any system with internet access. This technology permits for much well organized computing by unifying data storage, processing and band width. The important service provided by the Cloud computing is Data Storage that is progressively more customers. But the regular changes of the membership sharing data in multi-owner manner become a very challenging task. Therefore, in this paper propose the group signature and dynamic broadcast encryption techniques, any cloud user can in secret share data on to others. Meanwhile, the storage above and encryption calculation cost of our scheme are free with the number of revoked users. In addition, a random password is generated by the web service and sent to the mail id of the user to view, edit and delete the file from the system.

Keywords : Cloud Computing, Data Sharing, Privacy-Preserving, Access Control, Dynamic Groups, Web Service, Random Keygeneration.

I. INTRODUCTION

1.1 Cloud computing

Cloud Computing declared to both the applications data delivered as services over the Internet and the hardware and system software in the datacenters that send those services. The cloud services themselves have long been mentioned to as Software as a Service (SaaS). The datacenter system hardware and Computer software is what we will call a Cloud. When a Cloud is completely accessible in a pay-as-you-go way to the general public, we call it a Public Cloud; the service being sold is Usefulness Computing.

Mobile Cloud Computing (MCC) is the grouping of cloud computing, mobile computing and wireless networks to transport rich computational resources to mobile users, network operators, as well as cloud computing providers. The final goal of MCC is to enable implementation of rich mobile applications on an overabundance of mobile devices, with a rich user experience. MCC delivers business chances for mobile network operators as well as cloud providers.[1] More comprehensively, MCC can be distinct as "a ironic mobile computing technology that leverages unified elastic resources of diverse clouds and network technologies toclear functionality, storage, and mobility to serve a multitude of mobile plans anywhere, anytime through the station of Ethernet or Internet irrespective of heterogeneous environments and platforms based on the pay-as-you-use principle".

One of the important services obtainable by cloud providers is data storage. A company permits its staff in the same group or unit to store and share files in the cloud. By using the cloud, the staff can be completely free from the worrying local data storage and maintenance. However, it also attitude so important risk to the privacy of those stored files. Cloud offers huge chance for new novelty, and even disturbance of whole industries. Cloud computing is the long fantasized vision of calculating as a usefulness, where data owners can remotely store their data in the cloud to like on request high-quality applications and services from a common pool of configurable computing resources. Individuality privacy is one of the most important problems for the wide placement of cloud computing. Without the assurance of individualityconfidentiality, users might be reluctant to join in cloud computing schemes because their real individualities could be easily exposed to cloud workers and attackers. For example, a disobeyed staff can cuckold others in the company by distribution false files without being visible. Preserving the integrity of data plays a vital role in the founding of trust between data subject and service provider. Although intended as a talented service platform for the Internet, the new data storage example in "Cloud" brings about many stimulating design issues which have deepeffect on the security and presentation of the total system. One of the biggest anxieties with cloud data storage is that of data integrity confirmation at untrusted servers.

Some security systems for data sharing on untrusted servers have been proposed. In these methods, data owners store the encrypted cipher data files in untrusted storage and distribute the consistent decryption secretes keys lone to authorized users. Thus, unauthorized users or attackers as well as storage servers cannot study the content of the data files because they have no information of the decryption keys.

In this work propose a secure multi-owner data sharing scheme using web service. It suggests that any user in the group can securely share data with others by the untrusted cloud. The proposed arrangement is able to support dynamic groups professionally. Exactly, new decided users can directly decrypt cipher data files uploaded before their contribution without communicating with data owners.

User cancelation can be easily attained through a novel cancelation list without updating the secret keys of the remaining users. The size and calculation above of encryption are constant and self-governing with the number of revoked users. The deliver secure and privacy-preserving access control to users, which assurances any member in a group to secretly utilize the cloud resource. Furthermore, the real individualities of data owners can be exposed by the group manager when arguments happen. Here provides hard security analysis, and perform wide imitations to prove the efficiency of our scheme in terms of storage and calculation overhead.

1.2 AES Algorithm

AES is a symmetric block cipher that uses the same key for together encryption and decryption. Though, AES is quite different from DES in different ways. The algorithm Rijndaellets for a variety of block and key sizes and not just the 64 and 56 bits of DES' block and key size. The block and key can be chosen autonomously from 128, 160, 192, 224, 256 bits and need not be the same. However, the AES standard defines that the algorithm can only accept a block size of 128 bits. Depending on which version is used, the name of the normal is adapted to AES-128, AES-192 or AES- 256 respectively. As well as these alterations AES varies from DES in that it is not a feistel structure. Recall that in a feistel structure, half of the data block is used to adapt the other partial of the data block and then the halves are swapped. In this case the complete data block is managed in parallel during each round using replacements and transformations. A number of AES parameters depend on the key length. For instance, if the key size rummage-sale is 128 then the number of rounds is 10 while it is 12 and 14 for 192 and 256 bits correspondingly. At current the most common key size probable to be rummage-sale is the 128 bit key. This description of the AES algorithm therefore describes this particular implementation. Rijndael was designed to have the following characteristics:

- Resistance in contradiction of all known attacks.
- Speed and code density on a wide range of platforms.
- Design Simplicity.

II. METHODS AND MATERIAL

LITERATURE SURVEY

Literature survey is the most important step in software improvement process. Following is the literature survey of some existing method for cloud.

1. Plutus : Accessible Secure File Sharing on Untrusted Storage. M. Kallahalla et al. [2] proposed cryptographic storing system which is known as Plutus. Plutus enables protected file sharing on untrusted server by using client based key delivery. Plutus allow client to grip all the key management and delivery operations. As associate to client, Server incurs very little cryptographic above because Plutus does not place much trust on server, it removes almost all requirement of server faith. Plutus divide files into file groups and enable data owner to share the file groups with others by encrypting each file group with unique file-block key that can defend data. There is some restriction identified in the Plutus such as a) A heavy key delivery overhead for large-scale file sharing. b) The file block key needs to be updated and dispersed again for a user cancelation. Thus Plutus provides end-to-end security for group sharing system with lazy revocation.
2. Sirius: Securing Remote Untrusted Storage. E. Goh et al. [3] proposed a SiRiUS, Securing Remote Untrusted Storage. A SiRiUS is calculated to handle secure multi user file system over unconfident network using cryptographic processes. SiRiUS implement cryptographic read-write access controller for file sharing without use of a block server. Also it is likely for SiRiUS to implement large scale group sharing using the NNL key revocation construction. Key management and revocation is simple with negligible out-of-band communication. SiRiUS provides secure NFS without changing the file server. SiRiUS has some control in case of user revocation and dynamic groups. The user revocation is problematic for large scale distribution. Private key of every group member must be updated while connection of new user in the group.

3. Improved Proxy Re-Encryption Schemes with Applications to Secure Distributed Storage. Ateniese et al. [4] proposed proxy re-encryptions technique to add the entrée control to the secure file system and distributed storage. Blocks of contented are encrypted with unique and symmetric content keys by the data owner. The resultant encrypted content keys are extra encrypted under a master public key. Additionally, to grant a user's public key, the suitable content keys from the master public key is straight re-encrypt using proxy cryptography which helps in preserving the access controller and development of security. To manage access to encrypted content stored on distributed untrusted replicas, this system makes use of central access control server. The main assistances of this scheme are that they are unidirectional and only aincomplete amount of trust is placed in the proxy. However, a conspiracy attack can occur between any cancelled malicious user and untrusted server permitting them to discovery out the decryption keys of all the encrypted blocks of contented.
4. Achieving Secure, Scalable, and Fine-Grained Data Access Control in Cloud Computing. Yu et al. [5] offered a scalable and fine-grained data access controllersystem by defining access polices based on data attributes and KP-ABE technique. The grouping of attribute-based encryption (ABE), proxy re-encryption and idle re encryption certification the data owner to assign the addition tasks to untrusted server without revealing the essential contents of data. Data files are encrypted using random key by data owner. By means of key policy attribute based encryption (KP-ABE), the random key is additional encrypted with a set of features. Then the authorized users are allocated an access structure and matching secret key by the group manager. Thus, only the group user with data file attributes that content the access structure can decrypt a cipher text. This scheme has some limitation such as multiple-owner way is not reinforced by this system so that those single owner manners make it less supple as only group manager are responsible for modifying the data file shared. And user secret key needed to be efficient after individually revocation.
5. Efficient Revocation in CP-ABE Based Cryptographic Cloud Storage. Yong CHENG [7] proposed a security for clients to store and shares their complex data in the cryptographic cloud storage. It delivers a basic encryption and decryption for providing the security and data privacy. However, the cryptographic cloud storage still has some inadequacies in its presentation. Firstly, it is incompetent for data owner to allocate the symmetric keys one by one, particularly when there are a number of files shared online. Next, the access policy cancelation is exclusive, because data owner has to recuperate the data, and re-

encrypt and re-publish it. The first problem can be determined by using cipher text policy attribute-based encryption algorithm(CP-ABE). To improve the revocation procedure, they existing a new effectivecancelationsystem. In this scheme, the originaldata are first alienated into a number of slices, and then published to the cloud storage. When a cancelation occurs, the data owner wants only to save one slice, and reencrypt and re-publish it. Thus, the termination process is pretentious by only one slice in its place of the whole data.

6. Knox: Privacy-Preserving Auditing for Shared Data with Large Groups in the Cloud B. Wang et al. [8] absorbed on cloud computing and storing services, data is not only stored in the cloud, but frequently shared amongst a large number of users in a group. In this paper, they suggest Knox, a privacy-preserving auditing mechanism for data stored in the cloud and collective among a large number of users in a group. In specific, the develop group signatures to concept authenticators,homomorphicso that a third party auditor (TPA) is able to confirm the integrity of shared data. In the meantime, the identity of the signer on each block in shared data is reserved private from the TPA.

3. Existing System Model

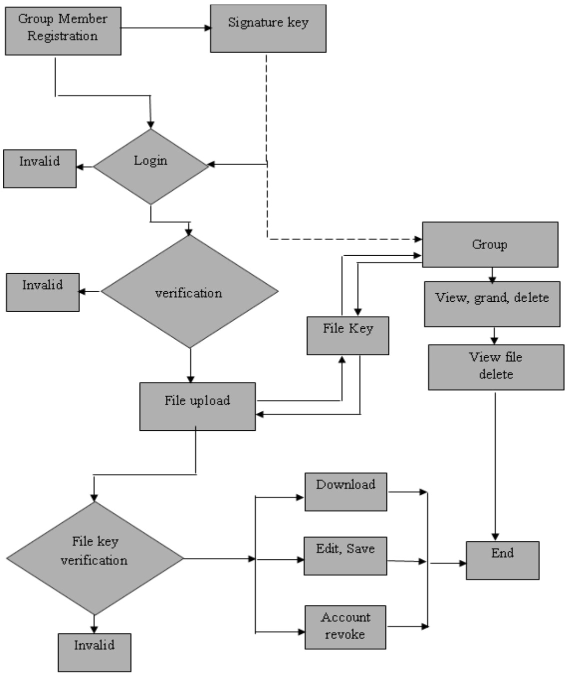


Figure 1. Existing System Model

4. Proposed System Model

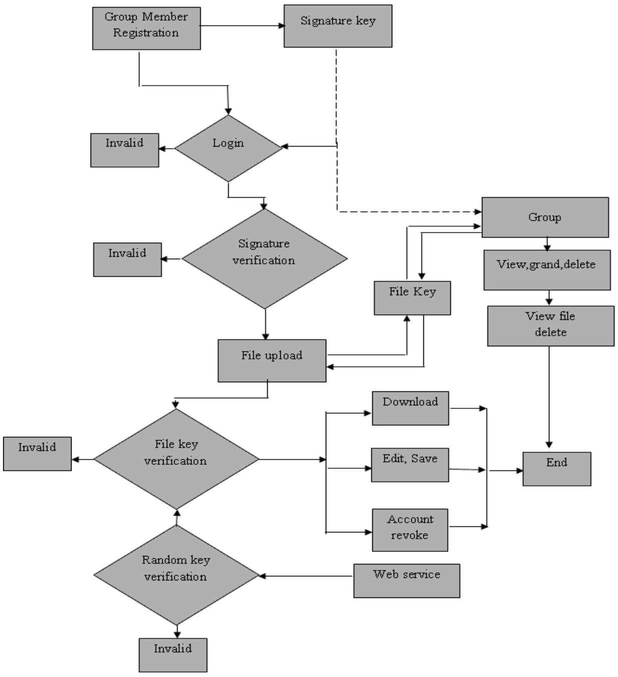


Figure 2. Proposed System Model

III. RESULTS AND DISCUSSION

Proposed System

Researchers have proposed various methods for defensive data sharing in cloud computing, though most methods failed to attain the well-organized as well as secure technique for data sharing for groups. In all of these methods, the encrypted data cipher files are stored in untrusted storage and distribute the consistent decryption keys only to group authorized users by the data owners. Therefore, the difficulties of user contribution and cancelation in these arrangements are linearly cumulative with the number of data owners and the number of revoked users, respectively.

To overcome these problems, the secure data sharing scheme for dynamic groups in an untrusted cloud by combining group signature and broadcast encryption techniques. In this method we are presenting how to manage risk in securely sharing data among multiple group members using key regeneration techniques. Compared to existing work our proposed system provides some unique features such as

a) Any group member able to store and share data files with others within a group.

b) This system supports dynamic group professionally. It implies that new user joining and user revocation are easily achieved without involving remaining users.
c) A random password is generated by the web service and sent to the mail id of the user to view, edit and delete the file from the system.
d) This system delivers rigorous security using AES encryption technique.

The system model consists of three different entities:

- Group Member
- Group manager
- Web service key generation
- File Security model
- User Revocation Module

Group members

Group members are a set of registered users that will upload their private data file into the cloud server and share them with others in the group. In this example, the groups play the part of group members. Note that, the group membership is animatedly changed, due to the group resignation and new member participation in the company.

This module is used for registering any valuable member. Here details like name, address, email id, password, phone number, date of birth is filled. If all particulars about that member is right, then the member is registered in cloud. After registration a mail the key is made and directed to that member mail id that the member registration is ongoing or not. It is accountability of manager to add the member into any group and beginning of member.

Group members are registered users that will
1. Upload their private file into the cloud server with cipher using AES algorithm and
2. Part them with others in the group. The group members are the proprietors of changing the files in the group and they are modifying or deleting it.

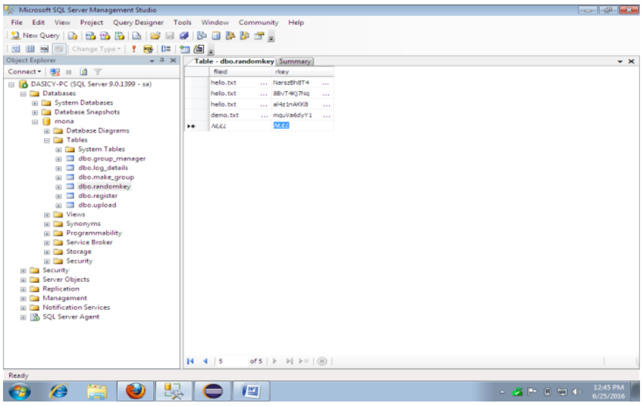
Group Manager

This module is for activating group member request. When any member attempts to register and if all details are correct then a request is sent to manager and manager has expert to accept the request. If the request is putative, then a mail is generated the key and sent to the member gmail id. In that mail generated key is directed and using that key the member can view any uploaded cipher text file. This Group manager module is for login purpose of manager. Here manager user name and his password is entered and if all details are correct then the manager is logged in successfully.

A group name scheme allows any member of the group to sign messages while keeping the identity clandestine from verifiers. Important to a group signature arrangement is a group manager, who is in charge of adding group members and has the aptitude to disclose the original signer in the occasion of disputes. A group signature scheme must content correctness, which guarantees that honestly-generated signatures confirm and trace correctly.

Web Service Key generation

In fig.3 the web service is a collection of open protocols and values used for exchanging random generated key data between applications or systems. The generated key in various programming languages and running on manystages can use web services to exchange data finished computer networks like the Internet in a wayparallel to inter-process communication on a single computer.



fileid	rkey
hello.txt	NarszBh8T4
hello.txt	8BvT4KJ7Nq
hello.txt	al4z1nAKK8
demo.txt	mquVa6dyY1
NULL	NULL

Figure 3. List of Security key Generated

File Security Module

1. Encrypting the data file using AES algorithm.
2. File upload and store in the cloud can be deleted by either the group manager or the data owner (The member who uploaded the file into the server).

User Revocation Module

User revocation is done by the group manager by revocation list (RL), based on which group members can encrypt their data files and ensure the privacy against the revoked users.

IV. CONCLUSION

In this work, to design a secure data sharing scheme MODS, for dynamic groups in an untrusted cloud. In Mods, a user is talented to part data with others in the group without insufficient individuality privacy to the cloud. Moreover, Mona ropes efficient user cancellation and new user connection. More particularly, well-organized user cancellation can be attained through a public cancellation list of without informing the private keys of the residual users, and new users can straight decrypt files stored in the cloud beforehand their contribution. Moreover, the storing overhead and the encryption calculation cost are continuous. Wide examines show that our proposed systems content the desired security supplies and guarantees capability as well.

V. FUTURE ENHANCEMENT

The above storage and the encryption calculation cost are continuous. Extensive examines show that the proposed arrangement content and desired security supply and guarantees capability as well. But here when the file is efficient by the group members. When Signature key and file key is same after the informing the web site then you can allow to accesses your data. In future the file key updating is also important to refining the security.

VI. REFERENCES

[1] Xuefeng Liu, Yuqing Zhang, Boyang Wang, and Jingbo Yan, "Mona: Secure Multi-Owner Data Sharing for Dynamic Groups in the Cloud", IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL.24, NO. 6, JUNE 2013

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

[3] 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

[4] 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

[5] 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.

[6] 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