Multi Owner Data Sharing with Privacy Preserving in Cloud Security Mediator

J. Suba[1], Seenivasan[2]

[1]Jay Shriram Group of Institutions, Avinashipalayam, Tirupur-638660., India

[2]Assistant Professor, M.E, Department of Computer Science
Jay Shriram Group of Institutions, Avinashipalayam, Tirupur-638660., India

Abstract: ***Cloud computing provide a promising pattern for data security services and high-quality data services .it provides various solution for sharing data with security concerns from dynamic resources in multi pattern based on storing and sharing have several issues from the multiple data owners are involved, the aspects of membership and data sharing need to be addressed. In this paper we proposed an efficient multi owner data sharing technique over cloud storage. The proposed scheme provides privacy and complexity while handling the data sharing over cloud from authorized data holders also it user third party access rights sharing group key mechanism encryption with two round access key technique. In this technique data can be uploaded in to the server after the encryption of the content by the secret group key. When new member joined in the group, new granted users can directly decrypt data files uploaded without contacting with data owners with key accessible technique. Our security proof and performance analysis shows that Anomy Control is both secure and efficient for cloud computing environment.***

Keywords: Loud Computing, Cryptographic standards, security mediator, Data sharing

1. Introduction

Cloud computing is recognized as an alternative to traditional information technology due to its intrinsic resource-sharing and low-maintenance characteristics. One of the most fundamental services offered by cloud providers is data storage. Such cloud providers cannot be trusted to protect the confidentiality if the data. In fact, data privacy and security issues have been major concerns for many organizations utilizing such services. Data often encode sensitive information and should be protected as mandated by various organizational policies and legal regulations. Encryption is a commonly adopted approach to protect the confidentiality of the data. Encryption alone however is not sufficient as organizations often have to enforce fine-grained access control on the data. Such control is often based on the attributes of users, referred to as identity attributes, such as the roles of users in the organization, projects on which users are working and so forth. These systems, in general, are called attribute based systems. Therefore, an important requirement is to support fine-grained access control, based on policy spicier using identity attributes, over encrypted data. However, it significant risk to the confidentiality of those stored files. To preserve data privacy, a basic solution is to encrypt data files, and then upload the encrypted data into the cloud. Unfortunately, designing an efficient and secure data sharing scheme for groups in the cloud is not an easy task due to the following challenging issues. First, identity Second, it is recommended that any member in a group should be able to fully enjoy the data storing and sharing services provided by the cloud, which is defined as the multiple-owner manner. Compared with the single-owner manner, Third, member revocation and signed receipt e.g., new member participation and current member revocation in a group. The changes of membership make secure data sharing extremely difficult, it is impossible for new granted users to contact with anonymous data owners, and obtain the corresponding decryption keys. On the other hand, an efficient membership re-vocation mechanism without updating of the secret keys of the remaining users minimize the complexity of key management , signed receipt is collected after every member revocation in the group it minimizes the compound copies of encrypted file and also reduces computation cost.

Many techniques have been proposed by the researchers earlier for the development of cloud computing and security of cloud computing. Most of the methods uses encryption and decryption standards for the security of the cloud computing and security of the data transferred and authentication of data transferred in the communication. The kind of authentication protocol is assisted by the third party auditor named third party key provider. the third party key provider is responsible for the authentication of the cloud request and responsible for the security of the cloud resources. On the other hand in user perspective the selection of cloud service is a key issue. Because the same set of service may be provided by different cloud service provider, but has different time complexity, completeness and quality. So that there must be a concrete solution to select the service based on different metrics, also the solution should provide rigid security and the authentication should be a light weight one. The proposed system should reduce overall response time, latency, and network overhead. We propose a set of methods for the selection, ranking and composition of cloud services to be accessed securely in the cloud environment.

2. Data Centers

Data centers are the storage area where the server data are stored. There may be number of servers grouped in a large room and the servers can be accessed through internet. Using virtualization you can have much number of servers for a single instance of server in a physical layer but accessed to a single server. This reduces the installation of many servers for the same data center. One of the most distinguishing characteristics of cloud computing architecture is its close dependency on the hardware

components. An online application is just a simple application that could be launched in different servers but when the application is considered with cloud computing, it will require massive data centers that will ensure the processes are done as expected and timely.

3. Distributed Server

The servers are not grouped or placed in a same location, but located in different geographical location and make the system more secure and providing service in a flexible manner. This makes the system as easy recoverable one and need not bother about the location failure or disaster and increases the service availability at any point of situation.

3.1 Third Party Auditor

The third party auditor works to generate **primary key** or **public key** to authenticated user and checking user to whether ***authorized or unauthorized*** person during user process. Suppose if unauthorized user enter into a system and it terminate that unauthorized entry into a system. This third party auditor can be used to checking that original user with respect to public key. And this process should be performed during encryption process as well as decryption process.

Third Party Auditor: an entity, which has knowledge and capabilities that clients do not have, is trusted to assess and represents risk of cloud storage services on behalf of the clients upon request. In the cloud paradigm, by putting the large data files on the remote servers, the clients can be relieved of the load of storage and computation. As clients no longer acquire their data locally, it is of critical importance for the clients to ensure that their data are being correctly stored and maintained. That is, clients should be equipped with certain security means so that they can periodically verify the correctness of the remote data even without the existence of local copies. In case those clients do not necessarily have the time, feasibility or resources to monitor their time and data, they can delegate the monitoring task to a trusted third party key provider. In this paper, we only consider verification schemes with public audit ability: any in control of the public key can act as a verifier. We assume that third party key provider is unbiased while the server is entrusted. For application purposes, the clients may interact with the cloud servers via CSP to access or retrieve their presorted data.

4. Related Work

Many privacy techniques for data sharing on remote storage machines have been recommended [1], in these models, the data owners store the encrypted data on un-trusted remote storage. After this, they will share the respective decryption keys with the authorized users. This prevent the cloud service providers and intruders to access the encrypted data, as they don't have the decrypting keys. However the new data owner registration in the above said models reveals the identity of the new data owner to the others in the group [1]. The new data owner has to take permission from other data owners in the group before generating a decrypting key.

Using the security mediator (SEM), this is able to generate verification metadata (i.e., signatures) on outsourced data for data owners [2]. Our approach decouples the anonymity protection mechanism from the PDP. Thus, an organization can employ its own anonymous authentication mechanism, and the cloud is oblivious to that since it only deals with typical PDP-metadata, therefore, there is no extra storage overhead when compared with existing non-anonymous PDP solutions. The distinctive features of our scheme also include data privacy, such that the SEM does not learn anything about the data to be uploaded to the cloud at all, which is able to minimize the requirement of trust on the SEM [2]. In addition, we can also extend our scheme to work with the multi-SEM model, which can avoid the potential single point of failure existing in the single-SEM scenario. Security analyses prove our scheme is secure, and experiment results demonstrate our scheme is efficient.

A cryptographic storage system that enables secure file sharing a entrusted servers. By dividing file into file groups and encrypting each file group with a unique lock group key [3], the data owner can share the file groups with others through delivering the corresponding group key, where the lock group-key is used to encrypt the lock-group keys [3]. However, it brings about a heavy key distribution overhead for large-scale file sharing [3]. Furthermore, the Lock group key needs to be updated and spread again for a user revocation.

Entrusted server has two parts of files to be stored file metadata and file data. The file meta-data implies the access control information that includes a series of encrypted key blocks, each of which is encrypted under the symmetric key of authorized users [3]. It is proportional to the number of authorized users. The user revocation in the scheme is an intractable issue especially for large-scale sharing, since the file metadata needs to be updated.

The establishment jointly computes a system-wide public key, and individually computes their master keys at the initialization phase. The public key is used for all operations within the method, and the master keys are used by each attribute authority when degenerates private keys for Data Consumers. A Data Owner achieves public key from any one of the authorities, and he uses the public key to encrypt the data file before outsourcing it to the Cloud Servers [4]. The Cloud Server, who is assumed to have sufficient storage capacity, does nothing but store them. Newly joined Data Consumers request private keys from all of the authorities, and they do not know which attributes are controlled by the system. On the other hand, authorities do not know which Data Consumers are interacting with them because each of them knows only a part of Data Consumers' attributes [4]. When the Data Consumers request their private keys from the authorities, authorities jointly create corresponding private key and send it to them.

5. Proposed Work

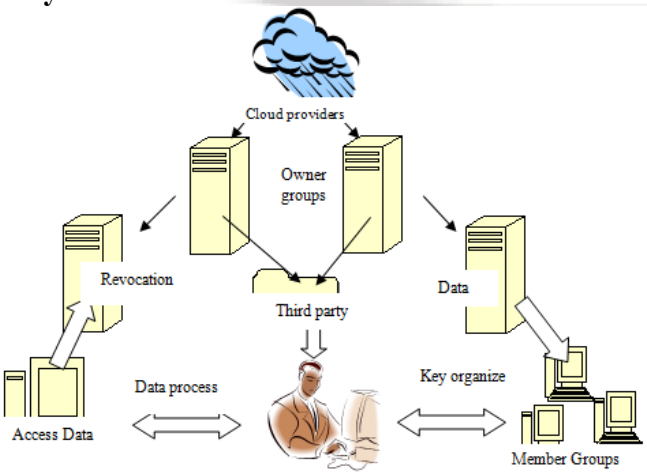
The existing system used to a security mechanism for cloud computing environment based on private key mechanism presented. Users will know neither the exact location of their data nor the other sources of the data collectively stored with the cloud. The data can find in a cloud ranges from public

sources which have minimal security concerns to private data containing which has highly sensitive information. We can implement TRA in our proposed planning. And it's main scope of third party auditor to generate primary key or public key for authenticated user. Suppose if unauthorized user enter into a system and it terminate that unauthorized entry into a system. Hence, further unauthorized person can't able to continue his process in a system. This third party auditor can be used to checking that original user with respect to public key. And this process should be performed during encryption as well as decryption of information.

The main contributions of this paper are:

1) The proposed scheme is able to protect user's privacy against each single authority of key.
2) The planned scheme is tolerant against authority compromise, and compromising authorities does not bring the whole system down.
3) We provide detailed analysis on security and performance to show feasibility of our system.
4) We first implement the real toolkit of multi-authority based encryption scheme.

6. System Model



A Data Owner achieves public key from any one of the authorities, and he uses the public key to encrypt the data file before outsourcing with third party it to the Cloud Servers. The Cloud Server, who is assumed to have adequate storage capacity, does nothing but store them. Newly joined Data Consumers request private keys from all of the authorities, and they do not know which attributes are controlled by the authorities. On the other hand, authorities do not know which Data Consumers are interacting with the Re-encryption is omitted because it is barely a composition of Decryption and Encryption. Interestingly, in a series of the experiment, the run time of encryption and decryption was independent of the tree structure. There is two round searchable key which is provide authentication to the third party permissions to access the data, the computation complexity of encryption and decryption depends only on the key providence of data owners.

7. System Implementation

This component generates dynamic agent for each service request and the agent is composed of service parameters and user identity details etc. once the agent is created it communicates with the Third party auditor which is residing in remote location. The third party auditor maintains the user identity and verifies the identity of the user whenever service request arises. The third party key provider extracts the user identity details from the agent request and verifies its signature. If the verification process is successful or it passes the verification process then the agent can access further services. Every agent will be assigned by an agent identification code and it will be updated with the Cloud service providers. The third party key provider maintains the identity of the user; it maintains the public and private keys generated for each user in the cloud by the cloud service provider. Whenever a user registers to the cloud service provider, it generates both public and private keys using which the user identity is computed. It uploads the key generated to the third party auditor and user. Upon receiving request from the user it receives the public and private keys from the user and it computes the signature for the key and verifies the signature. If the user signature verification passes, then the user will be allowed to access the service. Upon successful of signature verification, it assigns an agent identification code and same will be sent to the cloud service provider also. The agent identification code will be used to identify the agent by the cloud service provider**.**

7.1 Threats Model

Presuppose the Cloud Servers are untrusted, who behave properly in most of time but may collude with malicious Data Consumers or Data Owners to harvest others' file contents to gain illegal profits. But they are also assumed to gain legal benefit when users' requests are correctly processed, which means they will follow the protocol in general. In addition, even if the Cloud Server illegally modifies data files for sake of monetary benefits (e.g. deleting rarely accessed files to save the storage), whether the data is intact can be detected by the Third technique introduced. The authorities are assumed to be semi-honest. That is, they will follow our proposed protocol in general, but try to find out as much information as possible individually. More specifically, we assume they are interested in users' attributes to achieve the identities, but they will never collude with any user or authority to harvest file contents even if it is highly beneficial.

7.2 Design Goal

Our goal is to help Data Owners securely distribute their data with Data Consumers, where fine-grained privilege control is achievable, and to guarantee the privacy of Data Consumers' identity information by decomposing a center authority to multiple ones while preserving tolerance to concession attacks on the authorities. We assume the identity information is not disclosed by the underlying network.

7.3 Experimental Result

The transactions data cloud computing we compare the security level of our proposed system with the comparison of existing system. Cloud computing has been envisioned as the next generation architecture of it enterprise. in this private key used to encrypt for the data to be transferred

from the third party key provider and them should be stored in the database. Those data to be watermarking and data coloring used to transfer the data in the cloud server decrypt the data after that the data will be viewing the authorized persons. The third party key provider cannot change the data, those authorized persons only can modify and delete for them. in this data to be transferred, provided to the security key after that them to be transferred from another cloud server.

8. Conclusion

In this paper, we introduce what we believe is the right approach to achieve anonymity in storing data to the cloud with publicly-verifiable data-integrity in mind. Our approach decouples the anonymous protection mechanism from the provable data possession mechanism via the use of security mediator. Our solution not only minimizes the computation and key requirement of this mediator, but also minimizes the trust placed on it in terms of data privacy and identity privacy. The efficiency of our system is also empirically established.

Reference

[1] A Novel Multi owner Data sharing Group key protocol K.U.V.Padma, J.Anitha, K.Balaji
[2] Final year MTech , Dept of CSE, DIET, Anakapalli. Associate Professor, Dept of CSE, DIET, Anakapall.
[3] Storing Shared Data on the Cloud via Security-Mediator Boyang Wang †,‡, Sherman S.M. Chow §, Ming Li ‡, and Hui Li † † State Key Laboratory of Integrated Service Networks, Xidian University, Xi'an, China § Department of Information Engineering, Chinese University of Hong Kong, Hong Kong
[4] Secure Policy Based Data Sharing for Dynamic Groups in the Cloud M. Kavitha Margret
[5] International Journal of Advanced Research in Computer Engineering and Technology (IJARCET)Volume 2, Issue 6, June 2013 [4]. Privacy Preserving Cloud Data Access With Multi-Authorities Taeho Jung§, Xiang-Yang Li§, Zhiguo Wan† and Meng Wan
[6] 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.
[7] 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.
[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] B. Waters, "Ciphertext-olicy Attribute-Based Encryption: An Expressive, Efficient, and Provably Secure Realization," Proc. Int'l Conf. Practice and Theory in Public Key Cryptography Conf. Public Key Cryptography, http://eprint.iacr.org/2008/290.pdf, 2008.
[10] 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),
[11] pp. 89-98, 2006.
[12] D. Naor, M. Naor, and J.B. Lotspiech, "Revocation and Tracing Schemes for Stateless Receivers," Proc. Ann. Int'l Cryptology Conf. Advances in Cryptology (CRYPTO), pp. 41-62, 2001.
[13] D. Boneh and M. Franklin, "Identity-Based Encryption from the Weil Pairing," Proc. Int'l Cryptology Conf. Advances in Cryptology (CRYPTO), pp. 213-229, 2001.
[14] D. Boneh, X. Boyen, and H. Shacham, "Short Group Signature," Proc. Int'l Cryptology Conf. Advances in Cryptology (CRYPTO), pp. 41-55, 2004.
[15] D. Boneh, X. Boyen, and E. Goh, "Hierarchical Identity Based Encryption with Constant Size Ciphertext," Proc. Ann. Int'l Conf. Theory and Applications of Cryptographic Techniques (EUROCRYPT), pp. 440-456, 2005.
[16] C. Delerablee, P. Paillier, and D. Pointcheval, "Fully Collusion Secure Dynamic Broadcast Encryption with Constant-Size Ciphertexts or Decryption Keys," Proc. First Int'l Conf. Pairing-Based Cryptography, pp. 39-59, 2007.
[17] D. Chaum and E. van Heyst, "Group Signatures," Proc. Int'l Conf. Theory and Applications of Cryptographic Techniques (EUROCRYPT), pp. 257-265, 1991.