International
Journal
Of Advanced Research in Engineering & Management (IJAREM)

Privacy and Security issues in Multi Owner data sharing over cloud

D.Ramya, N.Geetha
Final Year M.Tech., Dept of CSE, KMMITS,Ramireddypalli,Tirupathi.
Assistant Professor, Dept of CSE, KMMITS,Ramireddypalli,Tirupathi.

Abstract: Cloud computing refers to manipulating, configuring and accessing the hardware and software resources remotely. It facilitates us to store data online. Without installing any software locally we can use this service. It is a service oriented architecture that reduces overhead for the end-user with a great flexibility. This paper discusses about efficient multi owner data sharing technique over cloud storage. The proposed scheme provides privacy and complexity while handling the data sharing over cloud.

Introduction

Cloud Computing makes computer infrastructure and services available "on-need" basis. The infrastructure may be hard disk, development platform, database or other software applications etc. There are specific vendors who provide these types of services and users need to use on payment basis like we are paying our electricity bill monthly. Cloud computing started with a risk-free concept: Let someone else take the ownership of setting up of IT infrastructure and let end-users tap into it, paying only for what is been used.[1]

In cloud computing, the cloud service providers (CSPs), such as Amazon, are able to deliver various services to cloud users with the help of powerful data centers.[2] By migrating the local data management systems into cloud servers, users can enjoy high-quality services and save significant investments on their local infrastructures. The primary service provided by the cloud vendor is data storage. Let us consider a simple scenario. A company allows its staffs in the same group or department to store and share files in the cloud. By utilizing the cloud, the staffs can be completely released from the troublesome local data storage and maintenance. However, it also poses a significant risk to the confidentiality of those stored files. Specifically, the cloud servers managed by cloud providers are not fully trusted by users while the data files stored in the cloud may be sensitive and confidential, such as business plans. 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.

To dealt with privacy and security many privacy techniques for data sharing on remote storage machines have been recommended[3]. In these models, the data owners store the encrypted data on un trusted remote storage. After that 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. The new data owner has to take permission from other data owners in the group before generating a decrypting key. The proposed system identified the problems during multi owner data sharing and proposed an efficient protocol and cryptographic technique for solving drawbacks in the traditional approach. It proposed an efficient and novel secure key protocol for group key generation and using these key data owners can encrypt the files. Suppose new user register into group the user need not to contact the data owner during the downloading of files and data can be encrypted with AES before uploading the data in to the cloud.

This paper first discusses about some works done on this area with few literature and then it discussed about the proposed system with few advantages. Then it discuss about the data owner, Group key manager and User revocation principles in brief and finally the paper deals with conclusion and future works with some limitations.

2. Related Work

In [1], the authors specified a secure data sharing model, Mona, for dynamic groups in a remote storage. In Mona, a data owner can share data with others in the group without announcing their identity. Moreover, Mona supports effective user repudiation and new user registration. More specially, efficient user repudiation can be attained by a public revocation list without ideating the private keys of the remaining users, and new users can directly decrypt files stored in the cloud before their presence.

In [4], Kallahalla et al. developed a cryptographic storage system that facilitates secure file sharing on untrusted servers. By breaking files into filegroups and encrypting each filegroup with a exclusive file-block key, the data owner can share the filegroups with others by handover of the corresponding lockbox key. In fact, it gives an additional load for key distribution. Apart from this, the file-block key needs to be renewed and delivered again for a userrevocation.

In [5], the contents of files placed on remote server are metadata and file data. The file metadata contains the access control data that encompass collection of encrypted keys. These metadata files are encrypted with public key of authorized users. As the file metadata should be refurbished, the user abrogation in the scheme is an uncompromising issue particularly for large-scale sharing. Nonetheless, the private key should be regenerated for each user for every new user addition into the group. This limits the application to support dynamic groups. Another issue is the encryption load enhances with the sharing scale. .

3. Proposed System

A secure multi-owner data sharing scheme is provided. It implies that any user in the group can securely share data with others by the untrusted cloud. Our proposed scheme is able to support dynamic groups efficiently. Specifically, new granted users can directly decrypt data files uploaded before their participation without contacting with data owners. User revocation can be easily achieved through a novel revocation list without updating the secret keys of the remaining users. The size and computation overhead of encryption are constant and independent with the number of revoked users. A secure and privacy-preserving access control to users, which guarantees any member in a group to anonymously utilize the cloud resource, is provided. Moreover, the real identities of data owners can be revealed by the group manager when disputes occur. A rigorous security analysis, and perform extensive simulations to demonstrate the efficiency o four scheme in terms of storage and computation overhead.

Advantages of Proposed System

- Any user in the group can store and share data files with others by the cloud.
- The encryption complexity and size of cipher texts are independent with the number of revoked users in the system.
- User revocation can be achieved without updating the private keys of the remaining users.
- A new user can directly decrypt the files stored in the cloud before his participation

3.1 Data owner

Data owner requires registration before uploading the data in to the service. Data owner can upload the data into the service after encrypting the file by the key which is generated by the group key manager. Data owner can download the content when ever required.

3.2 Group key manager

Group key manger receives the registration request from all the users, and generates a verification share and forwards to all the requested users for authentication purpose. Group key manager generates the key using key generation process and forwards the points to extract ion of the key from the equation generated by the verification points. For key generation protocol, Group key manager receives the verification shares and key as input to construct the Lagrange's polynomial equation f(x), which is passed, through (0, key) and verification points. After that group key manager forwards the points to data owners. Data owners again reconstruct the key from the verification points and check the authentication code which is sent by the group key manager. When a new user tries to download the file, new user need not connect with other

data owners. For decryption of the file new user connects to the group key manager then group key manager will update the group key and decrypts the files with previous key again encrypt with new key and updates the new key to all the data owners. Data owner initiate the request by sending the random challenge to the group key manager, as a response Group key manager sends a secret share. Data owner authenticates and forwards the verification share. Group key manager receives the verification shares and generates the key using Lagrange's polynomial equation and forwards the points to data owners for regenerating the key.

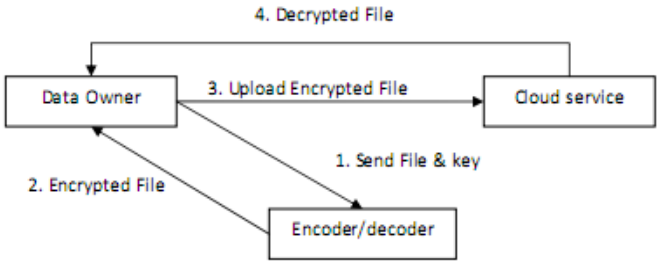

Fig.1 Initialization Process

3.3 Out sourcing of data over service

Data owner reads the required file content and encrypts the file with key, which is generated by the group key manager. For encryption of the data, the proposed system uses AES algorithm for encryption of the file and uploads in to the server. Data owner can download the file when ever required.

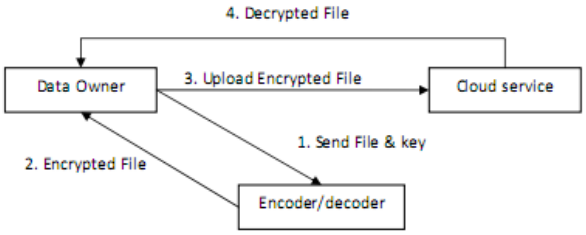

Fig.2 Outsourcing of data over service

3.4 User Revocation

Whenever new user tries to download the file, new user need not consult all the data owners. New user can be revoked by the group key manager in regular registration process. Group key manager updates the key, decrypts the data file with old key and encrypts with the new key and forwards the key to the all the related data owners.

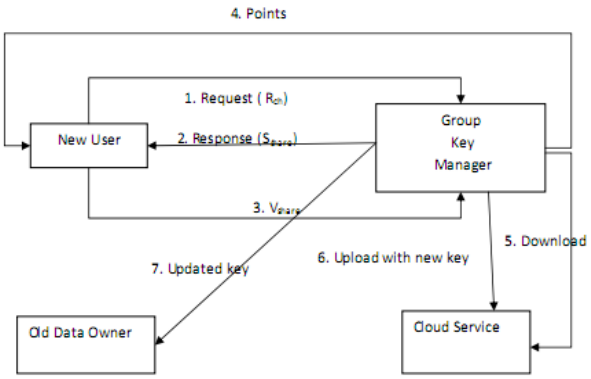

Fig.3 Revocation Process

4. Proposed Model Evaluation

In this section we present the performance report of our proposed model with the existing model. The below graph describes the performance, security and complexity attributes of the proposed model.

4.1 Performance:

The performance of proposed system is more compare to existing one, because in proposed system if new user enters into the cloud he does not depend on other users. The new user directly communicates with the group key manager and getting secret key. So the performance of the proposed system is high.

4.2 Security:

The security of proposed system is high compare to existing one. Since the group members only know the secret key. Suppose an unknown person enter into group he does not find the secret key i.e. the user enters into group confirm that he must be a group member.

4.3 Complexity:

The complexity of proposed system is low compare to existing one. Because the new user does not worry about getting the secret key i.e. the new user does not depend on the remaining group members. The new user directly communicates with group key manager and gets the secret key. The encryption and decryption of file also take less time.

4. Conclusion

In this paper, we developed a secure Multi owner Data sharing Group key protocol for an untrusted cloud. In this model, a new user can store data on the cloud storage without communicating with all the data owners. The group key manager grants the key on request to the new data owners directly. The new user revocation and registration is made simple by
allowing the user to communicate with the group key manager through the revocation policy. The storage overhead and the encryption computation cost are varied.

References

[1]. http://www.buyya.com/papers/TCC-Introduction-V1-N1-2013.pdf
[2]. http://www.ijera.com/special_issue/NCDATES/CSE/PART-1/CSE%20109-3035.pdf
[3]. M. Kallahalla, E. Riedel, R. Swaminathan, Q.Wang, and K. Fu,"Plutus: Scalable Secure File Sharing on Untrusted Storage," Proc.USENIX Conf. File and Storage Technologies, pp. 29-42, 2003.
[4]. 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.
[5]. 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.