ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 9, September 2018

Improving Data Confidentiality in Cloud

[1] Masarath Begum, [2] V.S Padmini
[1][2] Assistant. Professor, Dept. Of CS&E, GNDEC college Bidar, Karnataka, India

Abstract: **- Cloud computing has become an area of discussion among users in computing field benefiting users by providing many services. The services are based on pay as you use, one of the major services include place for storage and other required resources [1, 2]. Though people believe it to be difficult area to understand but the simplest way to understand cloud computing is to consider the experience dealing with the e-mail services on the web.Cloud computing is a huge area which basically provides many services on the basis of pay as you go. One of the fundamental services provided by cloud is data storage. Cloud provides cost efficiency and an efficient solution for sharing resource among cloud users. A secure and efficient data sharing scheme for groups in cloud is not an easy task. On one hand customers are not ready to share their identity but on other hand want to enjoy the cost efficiency provided by the cloud. It needs to provide identity privacy, multiple owner and dynamic data sharing without getting effected by the number of cloud users revoked. In this paper, any member of a group can completely enjoy the data storing and sharing services by the cloud. A secure data sharing scheme for dynamic cloud users is proposed in this paper. For which it uses group signature and dynamic broadcast encryption techniques such that any user in a group can share the information in a secured manner. Additionally the permission option is proposed for the security reasons. This means the file access permissions are generated by the admin and given to the user using Role Based Access Control (RBA) algorithm. The file access permissions are read, write and delete. In this, owner can provide files with options and accepts the users using that option. The revocation of cloud user is a function generated by the Admin for security purpose. The encryption computational cost and storage overhead is not dependent on the number of users revoked. We analyze the security by proofs and produce the cloud efficiency report using cloudsim.**

General Terms
Security,storage,revocation,cloudsim,confidentiality,braodcasting.

Keywords: - Cloud computing, data sharing, data-privacy, role based access control, encryption.

I. INTRODUCTION

To access your email, you open web browser, and then login to the email client. To make this work the most important thing is to have internet access. Your email is not placed on your local system; you always need an internet connection and from anywhere at any time to access the e-mail. If you are at home or work, or n a trip, you can check your email just by having access to the internet. The working of an email client is similar to cloud computing working, but with more features than just accessing the e-mail. The cloud allows you to access information at anytime from anywhere. While a traditional computer requires you as well as the data storage device to be in the same place, this part in excluded in the cloud. The cloud removes the necessity for you to be in the physical location as the storage device. Cloud provider can provide place or house the system resources needed to run your applications. To access cloud one always needs an internet connection. This means that either by using wireless or wired internet connection you can access your data housed in the cloud. By doing this one can enjoy the services of cloud from any place and using any device. This is ubiquity characteristic of cloud. The information placed on the cloud is often considered as a great deal to individuals with malicious intent. The security measures are provided by the cloud providers, which makes it difficult for you to understand the security measures. So it is equally important for individuals to take personal precautions to secure their data. There are many questions that one can ask, but it is always better to choose a provider that takes into account data security as a major concern. Data security is a critical issue in cloud computing. The fact that users no longer physically possess their data makes it very challenging to protect data confidentiality and secure data sharing in Cloud Computing. In this paper, we will identify the challenges pertaining to the problem of securing data sharing in cloud computing. We will present our preliminary work, an encryption-based fine-grained data access control framework, that is to tackle this challenges in cloud computing. Our solution is based on a recent cryptographic scheme – group signature. Today, large scale data is stored in the cloud in order to save the maintenance cost of in-house storage by many organizations. With moving to cloud storage service, any member of a group can share their data with other members of the group. Cloud computing also has many challenges that, if not taken precaution, may obstruct its fast growth. One of the major challenges faced by cloud applications is data security and is a great concern for the cloud user when they store their sensitive data on the cloud servers. These concerns are basically originated from the fact that cloud servers are handled by third party providers who are generally outside the trusted domain. Hence, data confidential over cloud servers is required when users storages on an outsourced center in the cloud. Let us consider an example, in healthcare application scenario use, disclosure of protected information system should meet the requirements of health insurance probability and accountability. In order to provide an efficient and secure data storing and sharing by the cloud we need to firstly consider the identity privacy, second, the multiple ownership that is; any member in the group can store and share the data by the cloud and finally, dynamically storing the data without getting effected by the number of users revoked. This is achieved by using group signature and dynamic broadcast encryption technique.

II. DATA SHARING IN CLOUD

Securing the data as well as identity privacy while, sharing data among users in an untrusted cloud is a challenging issue, due to the continuously change of the user in a group. Here, we propose a secure data sharing scheme, for active groups in the cloud. Here active means dynamic. By using dynamic broadcast encryption group signature techniques, any customer can share data with others in a group. Simultaneously, the encryption computation cost and storage overhead of this scheme are independent of the revoked users. Our project has the following features:

- Any member of the group can store and share data with other members by the cloud.
- The encryption computation complexity and size of ciphertexts are not dependent with the number of revoked users in the system.
- The users can be revoked without updating the keys of the remaining users.

We propose a technique in which multiple owners can securely share their data among the other members of the group in an unsecure cloud. The proposal is able to support active groups efficiently. New registered users can straight away decrypt data uploaded before their participation without knowledge of data owners. User revocation can be done without modifying the secret keys of the other users in the group. The encryption computation overhead and size remains same and independent of revoked users. This secure scheme is built using cipher text-policy attribute-based encryption and group signatures techniques.

In our scheme, the keys are generated with the help of the group signature and these keys are sent to the each user via the e-mails. By using the received key and password the user enter into the cloud system. Admin can generate these keys and send to each user involved in the group. And also the admin can generate the file access permission and then the revoke function for security purpose. The file access permissions are provided to the user using RBA based algorithm. The access permissions are read, write and delete permission. The revoke function is enabling the user to access the file which means the authorized person can only access the file. Finally, in our proposed scheme the files share between the dynamic users in the cloud in secure manner.

III. SECURITY ISSUES IN CLOUD AND THEIR DEFENSES

3.1 Cryptographic Cloud Storage

S. Kamara et al. [2] proposed a cryptographic security scheme for customers to save and share their sensitive data in the cloud storage. It aims to provide security of private cloud and the functionality and cost savings of public cloud. However, the revocation function in the cryptographic access control system is a performance degrader. To maximize the revocation method, they present an efficient revocation function which is efficient, and secure. In this scheme, initially the data is fragmented into n number of fixed fragments, and then stored to the cloud. For the revocation process, which is handled by the owner who just needs to download the fragment, encrypt again and then put back into the cloud. Thus, the revocation process is accelerated by affecting only one slice instead of the whole data. They have applied the efficient revocation scheme to the cipher text-policy attribute-based encryption based cryptographic cloud storage.

3.2 Achieving Secure, Scalable, and Fine-Grained Data Access Control in Cloud Computing

In [3] S. Yu et al. aimed on many challenges for access control security of data when users transfer their sensitive data on the cloud servers. This scheme uses cryptographic method to keep sensitive data confidential and only the authorized users get the data decryption key. However, the problem of concurrently achieving fine-grained, data confidentiality and scalability of access control still remains unsolved. This scheme addresses challenging issue by enforcing access policies based on data attributes, and allows the data owner to do most of the computation tasks involved in data access control cloud servers without revealing the data contents. In this technique the data owner used a random key to encrypt the data file. Using a set of attributes this random key is again encrypted. And a group manager assigns an access structure and its corresponding secret key to authorized user, such that if the data file attributes satisfy the access structure provided by the manager then only the user can decrypt the ciphertext.

3.3 Plutus: Scalable Secure File Sharing on Untrusted Storage

In [4], Kallahalla et al. proposed a secure file sharing on untrusted server, named Plutus. Generally, the files are divided into filegroups and each group is encrypted with an exclusive file block key. Due to which there is heavy key distribution and more over the file block key has to be modified and distributed again each time the user is revoked. However, for any large-scale file sharing it causes a heavy key distribution overhead. Additionally, there is always need for updating and distributing the file-block key each time a user is revoked.

3.4 Sirius: Securing Remote Untrusted Storage

E. Goh, H. Shacham, N. Modadugu, and D. Boneh [8] introduced SiRiUS. The use of it is done in situations where users don’t have control over the file server (like Yahoo!). They believe that this is the most secure scheme than an existing network file system (NFS) without changing the protocol or file server. SiRiUS uses hash tree constructions for file system. It supports multi-user file systems. All the users maintain two keys. But has the problem of file metadata updating for each revocation.

3.5 Revocation and Tracing Schemes for Stateless Receivers

In [12], the files saved in an untrusted server include two things: file data and file metadata. The file metadata has the access control information which includes a series of key blocks. Each key is encrypted using the authorized user’s public key. Thus, as the number of users are revoked the size of metadata to vary with this respect. For large-scale sharing revocation of user is an intractable issue, since the file metadata has to be modified. There is an extension version to this, the NNL construction which is used for key revocation efficiently. However, whenever there is a new comer in the group then each user’s private key needs to be computed again in an NNL system. This may limit the application for active groups. Moreover, as the sharing scale’s, there is linear rise in the overhead computation of encryption.

3.6 Improved Proxy Re-Encryption Schemes with Applications to Secure Distributed Storage

Ateniese et al. [5] strengthens proxy reencryptions for securing distributed storage. In this scheme the data owner uses exclusive and symmetric content keys for data, which is further encrypted using master public key. The server uses proxy cryptography for access control to directly encrypt again the suitable content key(s) from the public key to a authorized user's key. Unfortunately, between any revoked user and untrusted server a collusion attack may occur, which may help to know the encrypted blocks key to decrypt it.

3.7 Broadcast Encryption

A.Fiat et al.[9] introduces a framework system on multicast communication, where different occurrences of security risk were there. As a result construction of secure multicast communication that safeguard users from snooping and invasion. In this paper, they propose an efficient key distribution method for a secure dynamic group communication. By using IP multicast method for shortest rekeying time so that it can reduce conflicting effect on the communication. Additionally, they provide proxy technique for replies from group members to the group manager in order to minimize traffic came by rekeying.

3.8 Secure Provenance: The Essential of Bread and Butter of Data Forensics in Cloud Computing

In [6], Lu et al. introduces a secure provenance scheme based on the bilinear pairing techniques. The proposal is characterized by providing the information confidentiality on sensitive documents stored in cloud, anonymous authentication on user access, and provenance tracking on disputed documents. This scheme is based on group signatures and ciphertext policy attribute based encryption. In which each user is provided with two keys group signature key and attribute key. Unfortunately, user revocation is not supported. Goyal et al. developed a cryptosystem for fine-grained sharing of encrypted data that we call Key-Policy Attribute-Based Encryption (KP-ABE). In this cryptosystem, cipher texts are labeled with sets of properties and the access structures associates with private keys that control which cipher texts a user is able to decrypt. Wang et al. utilize and uniquely combine the public key based homo morphed authenticator with random masking to achieve the privacy-preserving public cloud data auditing system, which meets all above requirements.

3.9 Secure Multi-Owner Data Sharing for Dynamic Groups in the Cloud

In [1], Xuefeng Liu et al. introduces One of the most fundamental services offered by cloud providers is data storage. Let us consider a practical data application. 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.

IV. CONCLUSIONS

In this paper, we carried out a survey of various security issues in cloud computing, the multiple users are sharing the file in cloud environment in secure manner. But, the user having the fear about loss of their data and then they need more privacy about our data. In this scheme, multiple user in a same group can store and sharing the data in secure manner. This system first creates the groups for users. After that, generate signature for each user. Once users login into the cloud environment, the signature verification process is performed for each user. The signature may be in the form of keys. We then surveyed the work carried out till now in discovering various security issues in data transfer and their proposed solutions. The Admin can also handle the Access control and revocation function. The Access control is based upon the role of user. This system uses RBA concept to access the file present in the cloud. There are three different kinds of file access permissions are given to the user. There are read file, write file and then the delete file. The revocation function is used to find whether the file access by the user is authorized person or not. And the files are downloaded and then shared between the same groups in multiple users. Finally, we provided some insight on what future work can be done in order to reach the secure transmission in the cloud across dynamic groups.

V. ACKNOWLEDGMENTS

The satisfaction and euphoria that accompany the successful completion of any task would be incomplete without the mention of the people who make it possible, whose Constant guidance and encouragement crown all the efforts with Success. I consider it my privilege to express our gratitude and respect all those who guided, inspired and helped us in writing paper, the expression in the papert belongs to those below. I would like to express our deep sense of gratitude to our guide Dr.Mohammed Abdul Waheed for providing us the necessary facility in order to complete the paper successfully.

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] S. Kamara and K. Lauter, “Cryptographic Cloud Storage,” Proc.Int’l Conf. Financial Cryptography and Data Security (FC), pp. 136-149, Jan. 2010.

[3] 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.

[4] 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.

[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.

[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.

[7] C. Delerablee, P. Paillier, and D. Pointcheval, Fully Collusion Secure Dynamic Broadcast Encryption with Constant-Size Ciphertexts or Decryption Keys, Proc. First Intl Conf. Pairing-Based Cryptography, pp. 39-59, 2007.

[8] 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.

[9] A. Fiat and M. Naor Broadcast Encryption, Proc. Intl Cryptology Conf. Advancesin Cryptology (CRYPTO), pp. 480-491, 1993.

[10] Mary Campione, Alison Huml, Kathy Walrath, “On the Road to Understanding Java,” http://www.informit.com/articles/article.aspx?p=31940, Jun, 2003.