International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 04 Issue: 05 | May -2017 www.irjet.net p-ISSN: 2395-0072

A survey on Data uploading using proxy and integrity checking in public cloud

Bhagyalaxmi Beleri

PG student, Dept. of CSE, Acharya Institute of Technology, Karnataka, India

---

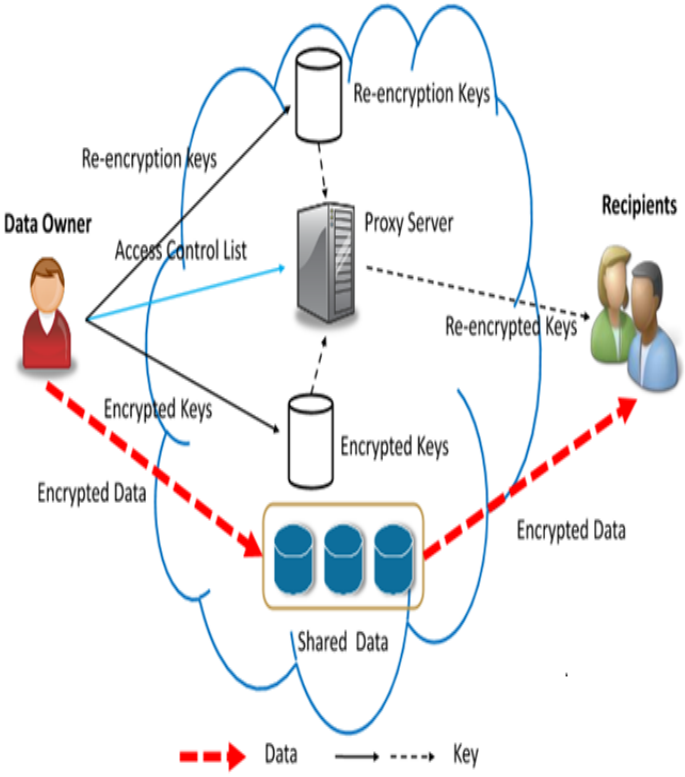
Abstract-*Alongside for distributed computing improvement, many of the customers are dependent on to storage of the information into PCS which is an open cloud server. To reach the goal of helping customers with their information, all the security issues must be settled. the privacy and security of data sharing are the two big issues. In public cloud, the user transfers his information to PCS that is responsible for the control of the information. Another important problem is semi trusted nature of PCS. Consider these issues into account and collect various methods that gives good solution to these problems. Customers limited to get public cloud server, will design some proxy to proceed his data and transfer the same to customers.*

Key Words: Cloud computing, Proxy cryptography, PCS, Proxy re-encryption, Public Cloud, Secure Data Sharing.

1. INTRODUCTION

One of the practices for using networks is the Cloud Computing. To store, process and manage the data remote servers are hosted rather than local server usage. Cloud benefits the user by providing data sharing capabilities. Several advantages of cloud can be figured such as elasticity, broad network access, low cost etc, despite of advantages it has various challenging obstacles, wherein the privacy and security is the major issue. Traditionally data is stored only in trusted servers, anyways cloud is managed and maintained by the semi-trusted third party.

In the open distributed computing, the enormous of information is being stored in remote servers. Since the control is not easy for the customers, it involves security of the information. Remote information checking uprightness is a primitive to persuade customer information. In some cases the information is proprietor is confined to appoint undertaking of information to third party i.e., the proxy. On other side checking of the information must be productive with the specific goal. In public cloud the main issue with remote data sharing is the secure data sharing, hence a different techniques being used to support security, one among which is the proxy re-encryption.



Proxy Cryptography:

In the proxy re-encryption, a proxy can change registered encryption under Alice's open key into an proposed encryption for bob. Such plan is utilized by Alice to forward messages to Bob without sending Mystery key also without knowing about the plain text. The Bob and proxy nonetheless, were not permitted for conspire, various proxy re-encryption techniques been proposed for open key encryption.

The proxy utilizes the, re-encryption keys, proxy keys, to play the interpretation without having capacity to consider plain text. Also the mystery keys of Alice and Bob does not have any data reasoned from proxy keys.

2. Related work

Duc H. Tran[1] introduced a secure framework to efficiently share data among multi-users.

Proxy re-encryption scheme is used and before sending to the cloud, that needed a data encryption. for the encryption of data it uses the public key and for decryption it uses the

private keys. When a user makes a request for the data that is being stored by another user, the requested users private key before sending it to the requested one, the proxy will pre-decrypt the data. Revoked user is prevented to access the data to avoid pre-decryption of data uses the private key. There are different types of proxy re-encryption, E1 gamal-based proxy re-encryption uses this mechanism. for each user a pair of private keys are created and proxy is being used. Let's consider user i, that desire to share data m to group, the user initially encrypt his information and send its cipher text to the cloud. from the user i, a user j send request for data. When a user j makes a request for the data from user i, proxy will convert the cipher text from the private key of user i to the cipher text from the private key of user j. So the user j can encrypt the data easily by using his private key.

Kan Yang[2] introduced a Privacy-Preserving Data Publish-Subscribe Service for Cloud-based Platforms.
As privacy is critical issue in public cloud for subscription service and data publication hence a attribute based encryption is used where users attribute satisfies the policies to access the data and even for data subscription policy. The data publishers and subscribers are not trust the cloud server. To evaluate the users attribute, the existing attribute based encryption allows cloud server and user attribute satisfy the access policy. the evaluation of access policy and subscription policy will not be supported by any ABE schemes. Bio-policy ABE is the novel attribute based encryption. that supports both access and subscription policy. the data publishers defines the access policy and data subscribers defines the subscription policy.

Kaitai Liang[3] proposed a method that defines a general representation for proxy re-encryption (PRE) known as deterministic finite automata-based functional PRE (DFA-based FPRE).
In this method encryptor encrypt the index string message of arbitary length and decryptor decrypts cipher text only if secret key of him is DFA associated. This method has advantage of data confidentiality and data sharing. this scheme allows semi trusted proxy, that is used to transform encryption, that associated with arbitrary length index string to other encryption consociate with new index string by not leaking any confidential message to proxy. This method make better flexibility of sharing data and gives the guarantee about confidentiality of data.

Mohamed Nabeel , Elisa Bertino, [4] Suggested a technique for Privacy preservation through Delegated Access Control policy.
In public cloud, to avoid computation overhead Fine-grained access control mechanism is the best method . Though decomposition of Access Control Policies is a difficult task it has several advantages .the fine-grained encryption is executed by cloud. At the time of modification only external layer of the encryption is needed to modify. Only external layer is needed so it is easier to handle the changes of data. there is no transmission of data is needed between the cloud provider and data owner.

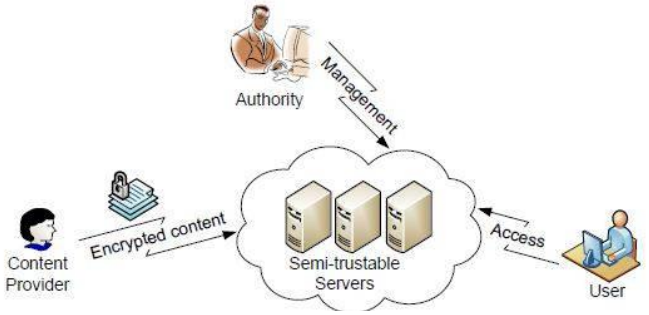
Huaqun Wang[5] introduced a proxy provable data procession technique for public cloud.
In open cloud computing, when client sends his information to cloud server he is unable to control remote data. therefore data security is one of the major issue in the public cloud. the framework proposed by this scheme is (PPDP) that is proxy provable data procession. The major importance of this method is When client is unable to perform the remote data possession checking. the bilinear pairing is used to design effective PPDP protocol. the other major issues are availability, integrity, confidentiality. The PPDP system includes 3 entities are client, proxy, Public cloud server.

W. Jia[6] suggested a secure data sharing mechanism known as secure mobile user-based data service mechanism (SDSM) to solve the problem of data secrecy and privacy in mobile cloud computing.
This scheme is based on identity based proxy re-encryption, in this method it is easier for the mobile users to implement fine-grained access control of data and gives the privacy of data in cloud. The mobile users initially encrypt their message, then forward the cipher text to cloud. at the same moment the users will assign his access control capability to the cloud. the encrypted data stored in the mobile cloud and he is trusted person to transfer cipher text encrypted with owners of data identity to one of the requesters identity. in this mechanism the communication and the updating of access policy cost is reduced. low overhead and convenient update with minimum requirement are the advantages of SDSM .

3. Encryption schemas

There are many different encryption schemes that have been proposed to address the security issues for data sharing inside cloud
A. Attribute Based Data Sharing Scheme
Yu, Shucheng, Cong Wang, Kui Ren, and Wenjing Lou.[7] proposed a method of encryption which is Cipher text-Policy Attribute Based Encryption (CP-ABE) provides fine-grained access control. All user have set of attributes and encryption is taken place by the access structure on attribute. the attribute satisfies the cipher text access structure, in the case of cipher text decryption. Therefore the possible attacks to sensible data is protected by security model and it is effective. and at any time enables revocation of attribute data.fig1 shows method of data sharing. the revocation of attribute of data sharing is one of the main problem. it is easier to solve by using this method for the limited instances. there is a master key component in this cryptography method that defines secret and public key for the users .these keys are belongs to user attribute. In the case of attribute based systems ,[7]This method efficiently handles problems of attribute revocation. it can be

implemented in semi trustable proxy servers for attribute revocation support. it places minimum load on authority, on these revocation events. the chosen plain text attack is secured by combining proxy re-encryption with CP-ABE technique.
The main drawback of this scheme is, it doesn't avoid the key escrow problem and the Proxy servers not have the provision to update secret key without disclose the attribute data.



B. Content Dissemination for Privacy preserving in cloud
Shang, Ning, Mohamed Nabeel, Federica Paci, and Elisa Bertino[8] proposed a Privacy preserving scheme which is a group key management scheme. This method is used in the selective distribution of documents ,which are encoded and preserves the document where it has been delivered .this is broad casting approach and it is based on access control of users policies, that can access the documents. the broadcast document is segmented into different sub documents that is based on access control policies and it is encrypted by different key. user identity attributes is based on the modern attribute-based access control. the policies have special advantages to the user's identity. in access control policies, the users had permission to access the documents and sub documents which have the access of their document publishers identity attributes. the document publisher not only learn users identity attributes but also users verify the policy conditions. The inferences of the values of attributes identity will be prevented. there is no need of sending decryption keys and encrypted document. bases on the subscription data users get the privacy to rebuild the key to decrypt authorized person. this scheme handled new and revocation subscriptions.
. The main disadvantage is, instead of enabling the Privacy protection to users and creates some transparent rekey to users but it is not supports expressive access control policies and clustering subscribers are not supported.

C. DFA based Proxy re-encryption scheme in cloud
Liang and Kaitai[9] proposed a DFA based encryption scheme in cloud, In this method a Proxy Re-Encryption (PRE), is also known as Deterministic Finite Automata Based Functional PRE (DFA-based FPRE).DFA-based FPRE system has a new technique. Every message has arbitrary length string associated with index and cipher text to it. the decryption will be carried if only the DFA has his/her secret key which take the string. the semi trusted proxy gives Re-encryption key. In semi trusted proxy the encryption gives the permission to transfer another cipher text that is join with the new string. the proxy will not give the access gain to plain text. the new primitives increases the flexibility. this method gives the permission for the encryption that is associated with the arbitrary length index string. by using the secret key we can recover the plain text. If the key receives the string that is tagged by DFA, then only this operation will be carried out. it gives the permission for semi trusted proxy to transform encryption.
There are some drawbacks, in this method the weaker re-encryption will occur, then proxy possesses the keys of both parties at the same time .decryption of plain text and encryption takes place in the another side. For the secure encryption it is not ideal method.

D. Group sharing framework in cloud storage
For the protection of data in the public cloud, [10] this scheme provides effective and secure group sharing framework that gives the security against the third party servers and attackers. this technique involves proxy re-encryption, proxy signature scheme, and enhanced group data sharing altogether creates a protocol. The members of the group will get access by group leader. at the same time the group leader will efficiently manage the more members of the group. Many operations, which computationally intensive will be designated without disclosing any secret data to cloud. The updating of group key while joining and leaving of the members of group will takes place that is supported by this scheme. Without the leakage of data of the users ,this scheme helps to transfer computational complexity and communication overhead. The group management privilege can be get by the any specific member and also at any time it can be revoked. The group members are not online and the group members are offline then also they can perform group synchronization. There will be a certificate problem because framework of group sharing.

E. Security Mediated Certificateless Cryptography
Security-mediated certificateless (SMC) cryptography is a version of mediated cryptography. [11] It is light weight scheme. to maintain the keys of revocation and instantaneous revocation this scheme is applicable. this technique solves the key escrow problem in comparison with existing encryption algorithm. when security methods will fail to handle at that time, this technique will effectively handles fully-adaptive chosen cipher text attacker. the algorithm in this technique is based on bilinear pairing. This technique supports distributed security mediators.
Some of the disadvantages are expensive pairing operations in mediated Certificateless-PKE scheme. the data owner needs the data to download for the attack of decryption and with help of new keys it perform the re-encryption.the data owner do not have any copies of data that is inefficient.

CONCLUSION

To retrieve users information and for storing mass data public cloud are generally used. But in cloud computing several issues do exists, to avoid such this papers surveys on Number of schemes. Among which the Proxy re-encryption scheme is found to be more effective. The proxy re-encryption ensures both forward and backward secrecy. Also the proxy signature method in it is used to grant privilege of group management only to the specific members. Hence having an advantage of better efficiency, security and even good performance to group communication. The proxy method provides added advantage to honesty of remote data privacy checking. However there is a lot of future work to be carried for open remote honesty checking and its uprightness.

REFERENCES

[1] D.H.Tran,H.L.Nguyen,W.Zha,andW.K.Ng,"Towards se curity in sharing data on cloud-based social networks", in ICICS 2011: Proc. 8th International Conference on Information, Communications and Signal Processing. IEEE CS, 2011.

[2] Kan Yang, Xiaohua Jia "Privacy-Preserving Data Publish-Subscribe Service on Cloud-based Platform", IEEE Trans. Parallel Distrib. Syst., vol. 24, no. 1, pp. 131–143, Jan. 2013

[3] Kaitai Liang, Man Ho Au, "A DFA-Based Functional Proxy ReEncryption Scheme for Secure Public Cloud Data Sharing", IEEE Transactions on Information Forensics and Security, vol. 9, no. 10, October 2014 .

[4] Mohamed Nabeel , Elisa Bertino, "Privacy Preserving Delegated Access Control in Public Clouds", IEEE Transactions On Knowledge And Data Engineering, Vol. 26, No. 9, September 2014.

[5] Huaqun Wang, "Proxy Provable Data Possession in Public Clouds", IEEE Transactions On Services Computing, Vol. 6, No. 4, October December 2013 .

[6] W. Jia, H. Zhu, Z. Cao, L. Wei, and X. Lin, "SDSM: A secure data service mechanism in mobile cloud computing", in WKSHPS 2011: Proc. 2011 IEEE Conference on Computer Communications Workshops. IEEE CS, 2011, pp. 1060–1065

[7] Yu, Shucheng, Cong Wang, Kui Ren, and Wenjing Lou. "Attribute based data sharing with attribute revocation."InProceedings of the 5th ACM Symposium on Information, Computer and Communications Security, pp. 261-270. ACM, 2010.

[8] Shang, Ning, Mohamed Nabeel, Federica Paci, and Elisa Bertino."A privacy-preserving approach to policy-based content dissemination." In-Data Engineering (ICDE), 2010 IEEE 26th International Conference on, pp. 944-955. IEEE, 2010.

[9] Liang, Kaitai, et al."A DFA-based functional proxy re-encryption scheme for secure public cloud data sharing."Information Forensics and Security, IEEE Transactions on9.10 (2014): 1667-1680.

[10] Xue, Kaiping, and Peilin Hong."A Dynamic Secure Group Sharing Framework in Public Cloud Computing."Cloud Computing, IEEE Transactions on2.4 (2014): 459-470.

[11] Chow, Sherman SM, Colin Boyd, and Juan Manuel Gonzlez Nieto."Security-mediated certificateless cryptography."Public Key Cryptography-PKC 2006. Springer Berlin Heidelberg, 2013. 508-524.