A Survey on Secure Data Sharing Methods in Public Cloud Computing

Shahina K M, Deepak Lal

Abstract— **The objective of the study is to conduct a survey about secure data sharing in public clouds. Due to the high popularity of cloud computing, many organizations use the public cloud for secure data sharing and large-scale data storage. But the privacy and security of sharing data have become two major issues. In public cloud, the user transfers his data to public cloud server and PCS is responsible for the overall control of the data. The semi trusted nature of PCS is another important problem. Thus we take these issues into account and collect different methods that give better solution to these problems.**

***Index Terms*—PCS, Proxy re-encryption, Public Cloud, Secure Data Sharing**

I. Introduction

Cloud computing is the practice of using a network of remote servers hosted on the Internet to store, manage, and process data, rather than using a local server or a personal computer. Cloud is rising from recent advances in technologies such as hardware virtualization, web services, distributed computing, utility computing and system automation. Cloud systems are used to enable data sharing capabilities and this can provide many benefits to the user. It has a number of advantages such as low cost, On-demand self-service, broad network access, resource pooling and rapid elasticity. Despite of above advantages, there still remain various challenging obstacles, among which the privacy and security of user's data become two major issues.

In traditional system, the data owner stores his data in the trusted servers, which are generally controlled by a fully trusted administrator. Anyways the cloud is usually maintained and managed by a semi-trusted third party (Cloud provider). So we cannot directly apply the traditional security storage technologies into cloud storage.In public cloud secure data sharing is the main issue. So we are using different techniques to support the secure data sharing. Some of the techniques are certificate less encryption, proxy re-encryption, attribute based encryption, matrix inversion computation, enhanced TGDH scheme and so on.

Manuscript received Dec, 2015.

***Shahina K ma**, Department of Computer Science and Engineering, KMCT College of Engineering, Calicut University Calicut, India*

***Deepak Lal,** Department of Computer Science and Engineering, Calicut University, Calicut, India.*

II. LITERATURE SURVEY

There are a number of inventions for providing effective cloud computing.

Duc H. Tran[1] introduced a secure framework to efficiently share data among multi-users. This mechanism is based on proxy re-encryption scheme and which requires the encryption of data before sending it to the cloud. All the users encrypt their data by using the same public key and decrypt it by using different private keys. When a user makes a request for the data stored by another user, the proxy will pre-decrypt the data according to the requested user's private key before sending it to the requested one. A revoked user is prevented to access the data by simply avoiding the pre-decryption of data using his private key.

Among the different types of proxy re-encryption, ElGamal-based Proxy Re-encryption is used by this mechanism. A pair of private keys that is created for each user and the proxy is used. Consider a user i , desire to share data m to a group, then he first encrypts his data and send the ciphertext to the cloud. When a user j makes a request for the data from user i, proxy will convert the ciphertext from the private key of user i to the ciphertext from the private key of user j. So the user j can encrypt the data easily by using his private key.

Piotr K Tysowski and M. Anwarul Hasan[2] proposed a key management system for secure data outsourcing applications based on attribute-based re-encryption. Attribute-based encryption effectively permits authorized users to access secure content in the cloud based applications on the satisfaction of an attribute-based policy. The scheme has been modified in such a way that the data owner and a trusted authority cooperate in the key generation and encryption processes. Responsibility over key generation is divided between a mobile data owner and a trusted authority and the owner is relieved of the highest computational and messaging burdens, so mobile users can minimise their battery and wireless communication usage. Additional security is provided through a group keying mechanism were data owner controls access based on the distribution of an additional secret key, beyond possession of the required attributes. In particular, costly pairing operations are performed by the manager and cloud provider instead of the data owner. Also, the manager computes the decryption key and assists with key distribution on behalf of the owner.

A hybrid protocol is also used to allow message encryption based on a group key, allowing the user membership to be further refined for highly sensitive data. It also allows re-encryption to occur, and thus revocation become efficient without necessitating existing common remedies and their

ISSN: 2278 – 7798

limitations. Thus this method is useful for securing mobile cloud computing with very large user populations.

Kan Yang[3] introduced a Privacy-Preserving Data Publish-Subscribe Service for Cloud-based Platforms. In public cloud, privacy issue becomes much more critical for data publication and subscription service, as the cloud server cannot be fully trusted by both data publishers and data subscribers. Existing Attribute Based encryption allows the cloud server to evaluate whether user's attributes can satisfy the access policy. However none of the ABE schemes support the evaluation of both access policy and subscription policy. But the novel attribute based encryption known as Bi-Policy ABE supports both access and subscription policy. Were access policy is defined by data publishers and the subscription policy is defined by data subscribers. Access policy is constructed by the use of attributes and the subscription policy is constructed with data tags.

BP-ABE employs two encryption secrets s1 and s2 in the encryption algorithm instead of only one in traditional ABE. Both s1 and s2 are shared according to the access policy defined by data subscriber and embedded into ciphertext components, while s2 is also used to generate data tags. To support privacy-preserving bi-policy matching, cloud server will do the access policy evaluation and pre-decryption with a transformed secret key.

Kaitai Liang[4] proposed a method that defines a general representation for proxy re-encryption (PRE) known as deterministic finite automata-based functional PRE (DFA-based FPRE).This is the first and concrete DFA-based FPRE system. In this method the message is encrypted with an arbitrary length index string and the decryptor can decrypt the ciphertext if and only if a DFA associated with his secret key accepts the string. This scheme permits a semi-trusted proxy to transform an encryption associated with an arbitrary length index string to another encryption associated with a new index string without leaking any useful message information to the proxy. This method enhances the flexibility of data sharing and also guarantees the confidentiality of data.

Mohamed Nabeel , Elisa Bertino, [5] Suggested a technique for Privacy preservation through Delegated Access Control policy. In public cloud, the data owners suffer high communication and computation overhead. Fine-grained access control mechanism is the best method to avoid this issue. The proposed scheme is based on Two Layers of Encryption (TLE) to address these requirements. Were the data owner accomplish a coarse-grained encryption, in contrast the cloud executes a fine-grained encryption on top of the owner encrypted data.

The decomposition of Access Control policies (ACP's) is a difficult task. This method has a number of advantages. It is easy to handle changes to the data because only the external layer of the encryption needs to be modified during modification. So no data transmission is required between the data owner and the cloud provider for modification purposes. This scheme uses two optimal algorithms, namely Subset-cover algorithm and complete sub tree algorithm for resolving the problem of decomposition of ACP.

Xinyu Lei, Xiaofeng Liao[6] Suggested a mechanism based on Matrix Inversion Computation (MIC).MIC is a general scientific and engineering task. Cloud Computing helps the clients to outsource their large computation workloads to a cloud server with huge computational power. Input or output privacy and result verification are the two major problems in cloud. The main approach is to preserve the privacy by transforming original matrix into an encrypted matrix and which is sent to the cloud and then re-encrypting the result to get the original matrix. The proposed scheme suggest Monte Carlo verification algorithm for result verification.

Huaqun Wang[7] introduced a proxy provable data procession technique for public cloud. In Public cloud computing, the client sends his data to cloud server and he is not able to control the remote data. So information security is an issue in public cloud storage. The other issues are confidentiality, integrity and availability. Here they proposed a framework called proxy Provable data Procession (PPDP). This method has high importance when the client cannot perform the remote data possession checking. In this method an efficient PPDP protocol is designed using bilinear pairing technique. The three network entities Client PCS and Proxy are included in this PPDP system.

Lan Zhou, Vijay Varadharajan [8] proposed the Role Based Access Control (RBAC) mechanism to prevent the unauthorized access of data. This provides flexible control and management by having two mappings, users to roles and roles to privileges on data objects. This system develops a role-based encryption (RBE) scheme that integrates the cryptographic techniques with RBAC. Also a secure RBE-based hybrid cloud storage architecture is designed and which allows an organization to store data securely in a public cloud, while maintaining the sensitive information related to the organization's structure in a private cloud.

W. Jia[9] 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 method is based on identity based proxy re-encryption scheme , which make mobile users easily implement fine-grained access control of data and also guarantee the data privacy in the cloud. Here mobile users will encrypt their data first and then forward the ciphertext to the cloud servers. At the same time the mobile user also delegates his access control capability to the cloud. Then the mobile cloud stores the encrypted data, and he is responsible to transform the ciphertext encrypted with the data owner's identity to the one with the requester's identity. The cost of updating of access policy and communication is also reduced in this mechanism. The main idea of SDSM is that SDSM outsources not only the data but also the security management to the mobile cloud in a trust way .The SDSM has many advantages such as low overhead, convenient update with minimum requirement.

III. A DYNAMIC SECURE GROUP SHARING FRAMEWORK FOR PUBLIC CLOUD COMPUTING

Public cloud provides an efficient platform for group data sharing. But ensuring privacy and security of group data stored in public cloud without exposing the private data into the semi trusted cloud provider or attacker is an important problem in cloud. Therefore a new framework is introduced, and this framework combines proxy signature, enhanced TGDH and proxy re-encryption together. This frame work effectively take advantages of cloud server's help without exposing any sensitive data to attackers or the cloud providers.

This scheme supports the updation of group key pair during group member's joining or leaving operation and which transfers most of the computational complexity and communication overhead to cloud servers without exposing sensitive data. Also the privilege of group management is granted to some of the group members. Enhanced TGDH scheme enables the group to negotiate and update the group key pairs when some of group members are offline.

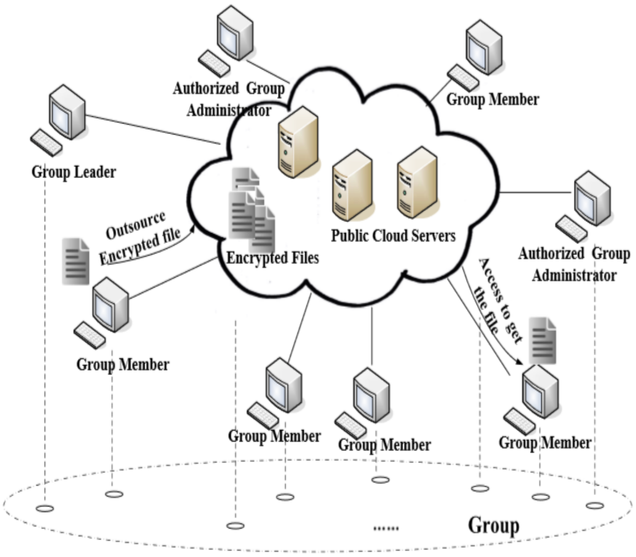

Fig 1. An example for secure group sharing

The novel framework consists of mainly six phases

- Group Initialization
- Group Administration Privilege Management.
- Data Sharing Management
- Group Member Joining
- group Member Leaving
- Key Synchronizing

A. Group Initialization

In the initialization group leader generates a shortest binary tree with n leaf nodes. GL chooses a random security key for each node and computed the blind key. For each group member M_i, GL encrypts $Index_{Mi}$, K_{Mi} and a timestamp value T with PuK_{Mi}. Then GL uploads tree structure and related information to the cloud.

B. Group Administration Privilege Management

GL can authorize and revoke the administration privilege to/from specific group members using proxy signature.And GAs help the GL to manage the group. Also the GL authorizes a group member GM_j to be GA, GL first sets the combination of some semantic information as the warrant information (m_{wMj})and then proxy signature is created.

C. Data Sharing Management

Before uploading data, owner gives the semantic description of the file: DESCRIPTION.Then symmetrically encrypts the file with randomly chosen session key. Data owner also uploads a digital envelope, which is asymmetrically encrypted with group public key.

D. Group Member Joining

When a group member joins, he will send a joining request to GA_j. Then GA_j tries to find a leaf node. At the same time new member randomly select a security key and get the BK of all sibling node from cloud provider. Then he will set the version of his node and parent node to zero, add one to the version of other internal nodes in the path. Send all BKs from his node to the root node to GA_j. After receiving all BKs from the new member, GA_j uploads all this BKs to the Cloud Server. Then Cloud provider updates the tree structure and the corresponding BKs.

E. group Member Leaving

When a group member leaves, one GA should mandate leaving group member's position in the binary tree and act as a sponsor to implement the group member leaving process. GA_j computes the proxy re-encryption key by combining old group private key with new group public key. Then cloud provider updates all existing digital envelopes and thus ensures backward secrecy.

F. Key Synchronizing

An offline should implement the key synchronizing process to get the current group key pair at the time he is online. M_i gives index of his associated node and version to the CLP. CLP founds the new position and the updated BKs of sibling nodes.

IV. Conclusion

Public clouds are very popular for mass storage and retrieval of the user's information. But there are various issues exist in cloud computing. So this paper analyses a number of invention of various schemes for secure data sharing in cloud computing .Among which Dynamic Secure Group Sharing Framework in Public Cloud Computing[10] is outperformed. This scheme combines three techniques known as Enhanced TGDH scheme, proxy re-encryption and proxy signature. Were Enhanced TGDH scheme is used for dynamic updation of group key pair during group member leaving or group member joining operation. Forward secrecy and backward secrecy is ensured by using proxy re-encryption. And group management privilege can be granted to some specific members based on proxy signature. It has an advantage of providing better security, efficiency and performance to group communication.

ACKNOWLEDGMENT

I am thankful to my project guide Mr. Deepak Lal ,assistant professor of KMCT College of Engineering and Head of the Department Prof. Mary Linda P.A for their support, remarks, and suggestions . I am also grateful to all the staff members of the Department of Information Technology and Computer Science & Engineering of KMCT College of Engineering and Technology, Calicut for their assistance in improving the review paper significantly.

REFERENCES

[1] D.H.Tran,H.-L.Nguyen,W.Zha,andW.K.Ng,“Towardssecurity 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] P. Tysowski and M. Hasan, “Hybrid attribute-and re-encryptionbased key management for secure and scalable mobile applications in clouds,” IEEE Transactions on Cloud Computing, vol. 1, no. 2, pp. 172–186, 2013.

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

[4] 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 .

[5] 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.

[6] Xinyu Lei ,Xiaofeng Liao,“ Outsourcing Large Matrix Inversion”.

[7] Huaqun Wang, “Proxy Provable Data Possession in Public Clouds” IEEE Transactions On Services Computing, Vol. 6, No. 4, OctoberDecember 2013 .

[8] Lan Zhou, Vijay Varadharajan,, " Achieving Secure Role-Based Access Control on Encrypted Data in Cloud Storage ", IEEE Transactions On Information Forensics And Security, Vol. 8, No. 12, December 2013.

[9] 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

[10] Kaiping Xue ,Peilin Hong, “A Dynamic Secure Group Sharing Framework in Public Cloud Computing”, IEEE Transactions on Cloud Computing (2014)Mohamed Nabeel, Ning Shang, “Privacy Preserving Policy - Based

Shahina K M, received her B.Tech Degree in Computer Science & Engineering, in year 2014, from UKF, College of Engineering, Kerala University. Currently she is pursuing her Masters of Technology in Computer Science & Engineering from KMCT College of Engineering, affiliated to Calicut University.

Deepak Lal, Asst. Professor, Did his BE(Computer Science & Engineering) in year 2010, and M.Tech(Computer Science) in year 2014 from KMCT, College of Engineering, Kerala. Presently he is a faculty of Computer Science & Engineering at KMCT, College of Engineering Kerala.