ISSN 2348 – 9928
IJAICT Volume 4, Issue 7, July 2017 Doi:01.0401/ijaict.2014.08.06 Published on 05 (7) 2017

AN ASSESSMENT ON VARIOUS SECURE DATA SHARING METHODS IN PUBLIC CLOUD

Mr. S. I. Shaik Hussain
PG Scholar,
Computer Science and Engineering,
Anna University Regional Centre,
Coimbatore, Tamilnadu, India

Mr. V. Yuvaraj
Teaching Assistant,
Computer Science and Engineering,
Anna University Regional Centre,
Coimbatore, Tamilnadu, India

Mr. K. Vishnu
PG Scholar,
Computer Science and Engineering,
Anna University Regional Centre,
Coimbatore, Tamilnadu, India

Abstract— Our aim is to take a study about the secure data sharing in public clouds. Due to the increasing popularity of cloud computing, there has been a growing trend to use the public cloud for secure data sharing and large-scale data storage. There are many issues and challenges are associated with the storage and retrieval of the data in the public cloud. By using public clouds, we have to improve productivity and reduce costs. In public cloud infrastructure, the user transfers its content to Public Cloud Server (PCS) and cannot able to control the remote data. This is an important problem. Other issues are privacy, security, result verification, confidentiality, integrity and availability. Thus we take these issues into account and collect different methods in which all gives a better solution to this.

Keywords— Public Cloud, Secure Data Sharing, PCS

I. INTRODUCTION

Cloud computing is typically defined as a type of computing that relies on sharing computing resources rather than having local servers or personal devices to handle applications. In cloud computing, the cloud is used as a metaphor for "the Internet," so the word cloud computing means "a type of grid computing," where alternate services such as data storage, servers and applications are delivered to an organization's computer and devices through the Internet. Cloud computing has started to obtain mass appeal in corporate data center as it enables the data center to operate like the Internet through the process of enabling computing resources to be accessed and shared as virtual resources in a secure and scalable manner. Different types of cloud are private cloud, public cloud and hybrid cloud. Private cloud is the phrase used to describe a cloud computing platform that is implemented within the firewall, under the maintenance of the IT department. A public cloud is one based on the standard cloud computing paradigm, in which a cloud service provider makes numerous resources like servers and storage, available globally over the Internet. Public cloud services may be free or based on a pay-per-use model. A hybrid cloud is an integrated cloud service utilizing both private and public clouds to perform distinct functions within the same organization.

The main issue in the public cloud is data sharing. So we are using many techniques to support the secure data sharing. Some of the techniques are certificate less encryption, functional proxy re-encryption, privacy preserving policy-based content sharing, proxy provable data procession and so on. Fig 1 indicates the public cloud architecture

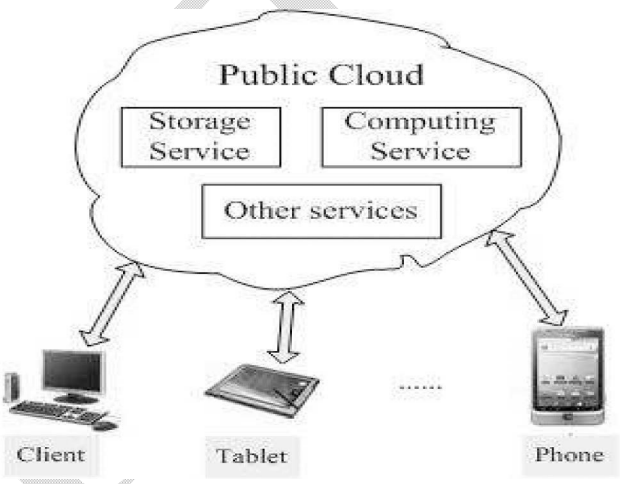

Fig 1. Public Cloud Architecture

II. STUDY OF EXISTING METHODS

2.1 DFA Based Functional Proxy Re-Encryption (PRE) Scheme

This method is based on the DFA. Here the encryption takes place normally. But the decryption takes place that depends on the decryptor in the sense the DFA associated with the user's secret key accepts the string. The string is associated with the ciphertext. It allows re-encryption in the way that the encryption can be transformed into another ciphertext using a new string. This takes place by a semi trusted proxy scheme. This method can raise the flexibility of users to provide their decryption rights to other users. The above method is an extension of Public Key Encryption (PKE) [1]. This method not only enhances the flexibility of data sharing, but also guarantees the confidentiality of data. Proxy Re-Encryption (PRE) is an honest- but –curious proxy in which re-encryption key that allows transferring ciphertext intended for one user to another user without revealing the plaintext and secret keys. Different types of PRE's are

- Conditional Proxy Re-Encryption (CPRE)
- Identity-Based Proxy Re-Encryption (IBPRE)
- Attribute Based Proxy Re-Encryption (ABPRE)

ISSN 2348 – 9928
Doi:01.0401/ijaict.2014.08.06 Published on 05 (7) 2017

Here we implement Attribute Based Proxy Re-Encryption (ABPRE) because it has more expressiveness in sharing of data.

2.2 A Dynamic Secure Group Sharing Framework in Public Cloud Computing

In Public Cloud Computing, the two major problems associated with the group sharing data are privacy and security. Since the cloud service provider's semi-trust property, it is difficult to trust it as a third party. Therefore, they use a new framework that mixes proxy signature enhanced Tree based Group Diffie Hellman (TGDH) and proxy re-encryption together into a new protocol [2].

By using the proxy signature scheme, the group leader grants the permission of group management to anyone of the group members. The extended TGDH method allows the group to agree and update the group pairs with the assistance of cloud servers. By applying the Proxy Re-Encryption the intended operations can provide to the cloud servers without revealing any private information. Three kinds of proxy signature algorithms are there. They are

- Full delegation
- Partial delegation
- Partial delegation by warrant

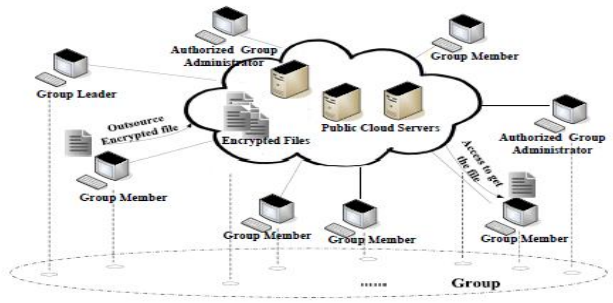

Fig 2. An example of Secure Group Sharing

The TGDH scheme uses an idea of binary key trees based on the decisional Diffie Hellman problem.

2.3 Privacy Preserving Policy-Based content sharing in Public Clouds

The main issue in public clouds is how to share the particular documents based on fine-grained attribute based Access control policies (ACPS). Here they proposed a new method called Broadcast Group Key Management (BGKM) and the secure construction of a BGKM scheme is called as ACV-BGKM [3]. The basic idea behind the scheme is to give the secret information to the users based on the identity attributes and allow them to develop an actual symmetric key based on their secret and some public information. The main advantage of BGKM technique is adding or removing users or updating ACPS can be done by updating only some public information. The control is based on the attributes of users named as identity attributes. The systems working towards this identity attributes are called as attribute based system. For supporting fine-grained access control, they need policies using identity attributes over encrypted data. The idea is to encrypt selected data using a set of policies with the same key and uploading the encrypted information to the cloud.

2.4 Privacy preserving Delegated Access Control in Public Clouds

In public cloud, the data owners suffer high communication and computation costs. The Adaptation of fine-grained access control to the cloud is the best method to avoid this issue. Here they propose a new scheme based on Two Layers of Encryption (TLE) to address these requirements. In this approach, 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 major issue is the decomposition of Access Control policies (ACP's). This Problem is referred to as NP-Completeness problem [4]. The TLE method has many benefits. When changes occur, only the external layer of the encryption needs to be modified. So no data transmission is required between the data owner and the cloud in this purpose. Both of the data owners and the cloud service uses a broadcast key management scheme. For resolving the problem of decomposing ACP's they proposed two optimal algorithms, namely Subset-cover algorithm and complete subtree algorithm.

2.5 Outsourcing large matrix Inversion Computation to a Public Cloud

Cloud Computing allows clients to outsource their large computation workloads to a cloud server with huge computational power. It is concerned with some issues such as input or output privacy and result verification. Here they take Matrix Inversion Computation (MIC) as an example [5]. MIC is a general scientific and engineering task.

For outsourcing this task to a cloud, they need an efficient protocol to enable security, robustness and efficient outsourcing. The main approach is to preserve the privacy by transforming original matrix into an encrypted matrix that is sent to the cloud and then re-transforming the result to get the original matrix. For result verification they use a Monte Carlo verification algorithm. The following are the design goals

- Correctness
- Security
- Robust cheating resistance
- Efficiency

ISSN 2348 – 9928
Doi:01.0401/ijaict.2014.08.06 Published on 05 (7) 2017

2.6 Proxy Provable Data Procession in Public Clouds

In Public cloud computing, the client transforms its data to cloud server and cannot able to control the remote data. Therefore, information security is an issue in public cloud storage. The issues are confidentiality, integrity and availability. Here they proposed a framework called proxy Provable data Procession (PPDP) [6]. Cloud Service Providers (CSPs) control the public cloud server (PCS) and offers three categories of services, namely Infrastructure as a Service (IaaS), Platform as a Service (Paas) and Software as a Service (SaaS). In Public cloud, a cloud service provider creates resources such as application and storage, which is globally accessible to the public. Here CSP and the client have some 'Visibility Gap' where they cannot able to see other's content and their mechanisms. The client cannot accomplish the remote data integrity checking protocol. Instead, they outsource this task to Third-Party Auditing (TPA). The TPA performs third party auditing at frequent intervals. PPDP system comprises of three important network entities, namely Client, PCS and Proxy.

2.7 Achieving Secure Role-Based access Control on Encrypted Data in Cloud Storage

One of the major issues in the public cloud storage is the unauthorized access to the data. For this they proposed Role-Based Access Control (RBAC) model, which assures flexibility and management through two mappings such as users to roles and roles to privileges on data objects [7]. Here the Role-based Encryption (RBE) technique that integrates the RBAC with cryptographic techniques. Using the proposed RBE scheme, a secure cloud data storage architecture using a hybrid cloud mechanism which is a combination of both the public and private cloud. The private cloud is used for storing only the organizations sensitive structure information's and the public cloud is used to store the original data which is in the encrypted format. In this infrastructure, the users who want to share the data only interact with the public cloud whereas no access for public users to access the private cloud. It reduces the attack on the private cloud. The RBE consists of the following algorithm,

- Setup
- Extract
- ManageRole
- AddUser
- RevokeUser
- Encrypt

2.8 Cloud Computing: The Limits of Public Clouds for Business Applications

Cloud Computing is an evolving technology that will continue to identify new invocations and thus provides numerous advantages to businesses. It reduces architecture and major expense. In some situation enterprises face limitations in using the cloud for mission-critical and high performance applications like ERP [8]. The major issue is that lack of well-define Service Level Agreements (SLA's) by the cloud providers. Here they cannot able to identify the guaranteed uptime. The following are the main challenges in the cloud computing era, namely interoperability, portability and migration. The cloud is treated as a solution for organizations with large variations in computing demands. Applications that use large volumes of data transfer increases the bottleneck problem. Cloud computing is not a matter of adding an infinite number of servers. It requires architecture of processing, memory and storage. Fig 3 indicates the secure data sharing in public cloud.

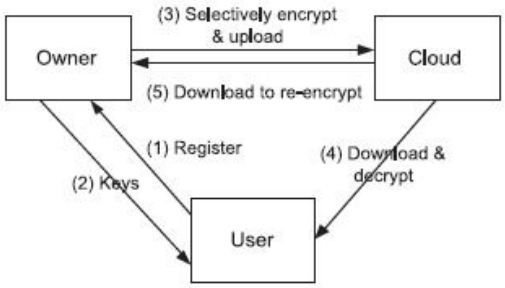

Fig 3. Secure data sharing in public cloud

III. CONCLUSION

Public clouds are popular nowadays, where they are generally used in the storage and retrieval of the user's information. It is given as a secure way of data sharing. It has very impact in the user's way of data storage. The study of secure data sharing is an increasingly research problem. The invention of various schemes for secure data sharing is crucial in business applications. Thus, in this paper, we present a survey of different techniques used in the storage and retrieval of data in the public cloud.

References

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

[2] 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

[3] Content Sharing in Public Clouds" IEEE Transactions on Knowledge and Data Engineering, VOL. 25, NO. 11, November 2013.

ISSN 2348 – 9928
Doi:01.0401/ijaict.2014.08.06 Published on 05 (7) 2017

[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] Xinyu Lei , Xiaofeng Liao, " Outsourcing Large Matrix Inversion

[6] Computation to a Public Cloud" IEEE Transactions On Cloud Computing, Vol. 1, No. 1, January-June 2013

[7] Huaqun Wang, "Proxy Provable Data Possession in Public Clouds" IEEE Transactions On Services Computing, Vol. 6, No. 4, October-December 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] Paul Hofmann Dan Woods, " Cloud Computing: The Limits of Public Clouds for Business Applications " IEEE Internet Computing (2011)