Paper ID:CSEIT15

PROVABLE MULTI-COPY DYNAMIC DATA POSSESSION WITH MULTI-OWNER IN CLOUD COMPUTING SYSTEM

Ms.Priya V. Sontakke
Computer science and technology department, Department of technology Kolhapur, India
Ms.Amrita A. Manjrekar
Computer science and technology department, Department of technology Kolhapur, India

Abstract—Most of organization store almost unlimited amount of their data in cloud with facility of retrieving. Users pay fees for storing data. Many of the users are in collaborative relationship; at that time data sharing and dynamic operation are useful to improve productive benefits. So, propose system introduced the multi owner with data sharing concept. Most of the time customers store their important data on multiple servers for accessing on different geographical location. When data store on multiple server then data owner need evidence of all outsourced file copies are intact. But some time few copies may be corrupt. So, proposed system identifies corrupted copies and corrects it before dynamic operation performs. In addition, proposed system allows multi-owner facility for sharing data.

Keywords- Cloud Computing, Dynamic Data, Cloud service provider (CSP),Data Integrity, Multi-copy, Multi-Owner .

I. INTRODUCTION

An increasing number of clients organization use cloud to store data which has become trend [1]. Cloud service provider (CSP) allows storing much more data than private computer. Once data stored in remote server, authorizer can access all data from any geographical location. Most of the time organization store important data in cloud, without leaving a copy in local computer. Once data is stored in cloud they may not be trustworthy due to losing control on data. So, it is important to ensure data is not lost or corrupted by checking data integrity.

In data integrity checking, client challenge remote server and server response by proving that. Many researchers have focused on this problem and find out different technics.

PDP is one of the techniques for validating data integrity. In this model, do not need to store all file to local computer to check data integrity. It creates metadata information of each file and that store it in local computer without storing whole file. At the time of verification of data integrity it sends the metadata to the verifier side. PDP model used both static data and dynamic data.

In static PDP schema used data which cannot change, it only store and access by authorize users [2][3].

In dynamic PDP schema stored data can be modify by performing operation like modify, insert, delete etc. and also it can be scaled by inserting more data [4] [5] [6].

For efficient validation of outsourced data integrity, a number of PDP schema proposed, which is based on single copy [7] where no need to proof that CSP store all copies but in multiple copy CSP need to proof. In multiple data copies, the overall system integrity fails if there are one or more corrupted copies. Also, we need to check integrity each time when we performing dynamic operation. MB-PDP schema used dynamic data to store multiple copies on different server across different data centers [8]. In this proposed system, address all of this issue and recognize list of corrupted copies and reconstruct them. In addition to improve scalability, this system provides Multi-owner and sharing facility.

II. RELATED WORK

Ateniese et al. [2] are the first to consider public auditability in their de fined "provable data possession"(PDP) model for ensuring possession of data files on untrusted storages. Their scheme utilizes the RSA-based homomorphic linear authenticators for auditing outsourced data and suggests randomly sampling a few blocks of the file. However, the public auditability in their scheme demands the linear combination of sampled blocks exposed to external auditor. When used directly, their protocol is not provably privacy preserving, and thus may leak user data information to the auditor.

Roberto Di Pietro [9] propose a partially dynamic operation like block modification , deletion and append of the prior PDP scheme, using only symmetric key cryptography but with a bounded number of audits. Also, it is unsuitable for public verifiability.

Curtmola et al. [10] propose a multiple replica PDP (MR-PDP) which ensures that multiple replicas of the client's data are stored at the cloud storage server, so that the data availability is improved. It can generate further replicas on demand, at little expense, when some of the existing replicas fail. It is not efficient as we would like for integrity issue.

Ayad F. Barsoum and M. Anwar HAsan [14] provide a multi-copy dynamic data possession. It provides evidence to customer that CSP store all copies. Also, it support full block level dynamic operation by data owner using map version table and allow authorized user seamlessly access data and finally, discussed about to identified list of the corrupted copies.

III. SYSTEM PRILIMINARIES

Basic equation which are used in this proposed system:

a) Pseudo-Random Permutation (PRP):

$$\pi_{key} : key \times \{0, 1\}^{log2(m)} \rightarrow \{0, 1\}^{log2(m).1}$$

b) Pseudo-Random Function (PRF):

$$\psi_{key} : key \times \{0, 1\}^{*} \rightarrow Z_p \text{ (p is a large prime).}$$

c) Bilinear map/Pairing:

Let G_1 , G_2 and G_T be cyclic group of prime order p. Let g_1 and g_2 be generators of G_1 and G_2, respectively . The bilinear pairing is a map e is defined as follows: e: $G_1 \times G_2 \rightarrow G_T$ with the properties.

- Computability: There exists an efficient algorithm for computing map e.
- Bi-linearity

$\forall u, v \in G_1$ and $\forall a, b \in Z_p$,$e(u^a,v^b)=e(u, v)^{ab}$

- Non-degeneracy

$$e(g, g)\neq 1$$

d) Hash Function (Map to Point):

$H(.): \{0, 1\}* \rightarrow G1$.

e) Encryption Algorithm:

EK is an encryption algorithm with strong diffusion property, e.g., AES, Attribute based encryption with constant cipher text.

IV. PROPOSED SYSTEM

Proposed system consists of the main entities:

- Data Owner-

  That can be an organization or an individual originally possessing sensitive data to be store in the cloud.
- CSP-

  Who manages Cloud Servers (CSs) and provide paid storage space on its infrastructure to stores files.
- Authorized Users

  Users who have right to access remote data.
- Verifier

  It may be Data Owner or Third Party Auditor or Authorized User.

Proposed system achieves the following main objectives:

1. Implement the system which allows multi owner facility for dynamic data with notification.
2. Allow to reconstruct the corrupted copies using existing duplicate file copies.
3. Allow shared access authority by anonymous access request matching mechanism with security and privacy consideration.

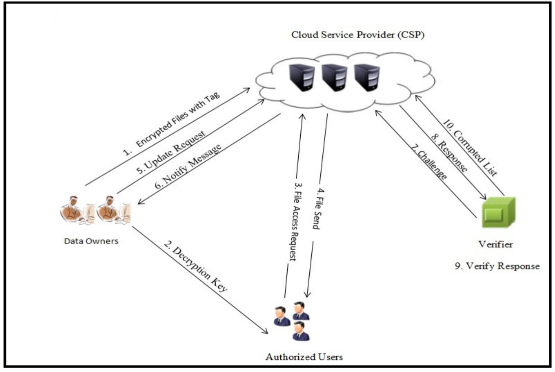

Fig. Cloud Computing Data Storage System Model

System will be consisting of following module, which is formed on the basis of the functionalities that are found in the system.

- Registration

  The user can store the file into the cloud storage only if he/she is a registered owner of this web application. The registration can be made as either free or a paid registration depending on the organization's requirement.
- Copies Generation

  File copies are created by Data Owner side. Propose system allows a user to stores all copies of a file in a storage system. Each copy of file can be produced at the time and it will store into storage system with tag of each file copies.
- File Division

  User's file is divided into data blocks of different sizes for improving the efficiency of storage and as well as to improve security of file.
- File Upload

  File is uploaded on the cloud storage with the help of CSP. Files store on cloud storage infrastructure which is location independent. While we upload file ultimately CSP store all copies of file which is agreed on service.
- View Files

  File content can be viewed in original format by Data Owner and Authorizer User but file content is viewed in encrypted format by CSP and Verifier.
- File Modify

  File can be modified only by the File Owner. Modification will be done by inserting, appending, editing or changing the data.
- File Deletion

  The Uploaded file can be deleted by the File Owner or CSP.
- File Download

  Only the verified Files can be downloaded by the File Owner and Authorized User. But they don't know which copy of file is downloaded.
- File Verification

Public key shared by data owner for the verification process. File cannot be downloaded by the verifier side at the time of verification process.

- File Storage
  File is stored in the cloud is an Encrypted format using the private key which is generated by data owner. File copies can be stored in multiple servers with unique copy.
- Verifier
  Verifier is one of the users in this application. Verifier is used to verify the copies of file that are stored into cloud storage. Verifier randomly checks the integrity of all file copies by sending challenge to the CSP.
- Integrity Verification
  Verifier randomly send a challenge to the CSP to check integrity and consistency of file copies then CSP send proof of that challenge and finally verifier check is it correct or not without downloading of files copies.

V. CONCLUSION

The proposed system can be helpful to create multiple copies of sensitive data in different server. Also, it verifies integrity where CSP prove all copies are intact. In addition it identifies corrupted copies and reconstruct before dynamic operation performs. It also discussed to share access authority by providing security and privacy.

REFERENCES

[1]. R. Buyya, C.S. Yeo, S.Venugopal, J. Broberg , and I. Brandic, “Cloud computing and emerging IT platforms”, Future generation computer system, vol. 25, no. 6, pp. 599-616, 2009.

[2]. Giuseppe Ateniese, Randal Burns,RezaCurtmola, Joseph Herring,
LeaKissner, Zachary Peterson, and Dawn Song, “Provable data possession at untrusted stores”, in Proceedings of the 14th ACM
Conference on Computer and communications security, Oct 2007.

[3]. F. Sebé, J. Domingo- Ferrer, A. Martinez-Balleste, Y. Deswarte and J.-J. Quisquater,“Efficient remote data possession checking
in critical information infrastructures,” IEEE Trans. Knowl. Data Eng. vol. 20, no. 8, pp. 1034–1038, Aug. 2008

[4]. Giuseppe Ateniese, Roberto Di Pietro, Luigi V.Mancini and Gene
Tsudik, “Scalable and Efficient Provable Data Possession”, in
Proceedings of the 4th international conference on Security
and privacy in communication, 2008.

[5]. C. Wang, Q. Wang, K. Ren, and W. Lou.(2009).”Ensuring data security in cloud computing”, http://eprint.jacr.org/

[6]. C. Erway, C. Papamanthou, and R. Tamassia, “ Dynamic provable data possession”, USA, 2009, pp. 213-222.

[7]. Decio Luiz Gazzoni Filho and Paulo Sergio Licciardi Messeder Barreto, “Demonstrating data possession and uncheated data transfer”, 2006

[8]. Ayad F. Barsoum and M. Anwar HAsan “Provable Multi-Copy Dynamic Data Possession in Cloud Computing Systems” IEEE trans. On information foraensics and security VOL10, NO. 3, March 2015.

[9]. Giuseppe Ateniese, Roberto Di Pietro, Luigi V.Mancini and Gene Tsudik, “Scalable and Efficient Provable Data Possession”, in Proceedings of the 4th international conference on Security and privacy in communication, 2008.

[10]. RezaCurtmola, Osama Khan, Randal Burns and Giuseppe Ateniese, “MR-PDP: Multiple-Replica Provable Data Possession”, in 28thInternational Conference on Distributed Computing Systems, 2008.

[11]. Ayad F. Barsoum and M. Anwar HAsan “Provable Multi-Copy Dynamic Data Possession in Cloud Computing Systems” IEEE trans. On information foraensics and security VOL10, NO. 3, March 2015.