ENHANCING DATA STORAGE SECURITY IN CLOUD COMPUTING USING PDDS TECHNIQUE

AparajitaSain,Parna Dutta ,NamrataDwivedi,PradnyaChikhale ,VrundaBhusari
Department of Computer Science, JSPM's BSIOTR,PuneUniversity,Maharashtra, India

Abstract: Cloud storage system provides user to remotely store and retrieve the data in cloud, as per their requirement. In cloud storage, user is not requiring to keep any burden of local hardware and software management. Cloud computing is the most challenging technology in today's world. In this work, the integrity of the data are enhanced by make use of the distributed storage servers and also by using the partitioning technique. Encryption and Decryption techniques are also used for securing the data which are stored in cloud. These techniques would provide the high data integrity, high efficiency, easy to identify the error localization and also help to identify the misbehaving server. Data integrity concept will also help to increase the performance of cloud storage. The data which are stored in cloud are dynamic in nature; hence our project also focuses on the reduced storage space with less time and on less computational cost.

Index Terms: Remote Data Integrity Checking, Partitioning, Error Localization.

I. INTRODUCTION

In the recent years, the Internet access become accessible in high speed network, Cloud Computing is an technology which is based on internet, Cloud Computing is used to deliver the services over the internet with the help of computing resources such as hardware and software. Nowadays Cloud computing can be widely used to enable the users or clients to use and create software from anywhere at any time without concerned about the execution of the data or instructions. In cloud computing the computing resources are utilized and these are delivered as services after computation over the network.

The Cloud Computing technique is assigned with services such as software as a service (saas), platform as a service (paas) and Infrastructure as a service (iaas) which are easily usable and payable by the end user. Fig[1] shows the cloud services architecture.Cloud storage is a model of data storage services where the developers can access and store digital data in cloud and the cloud resources are typically owned, managed and controlled by a serviceprovider. These cloud storage providers are responsible for keeping the data available and accessible, and the resources protected and running. The clients or Peoples and organizations buy or lease storage capacity from the providers to store end user, organization, or application data and access the data from the cloud storage via internet.

Like cloud many storage servers are handled in the large scale distributed system. Data dynamics is achieved with third party auditing and the remote integrity checking.Remote data integrity checking supports dynamic operations and verification information as in Fig [2] considering the untrusted server with security analysis. The advantages of the storage servers are flexible with reduced cost and they also manage the risk associated with data loss. The data is properly stored and prevented by the remote services. The remote data integrity checking procedure ensures high cloud storage reliability, improved error localization and also easily identifies misbehaving server in thecloud storage and detects the errors in the data. In the future work well-

Authors:

1. ***Ms. AparajitaSain****, Department of Computer Science, JSPM's BSIOTR, India*
2. ***Ms. Parna Dutta,*** *Department of Computer Science, JSPM's BSIOTR, India*
3. ***Ms. NamrataDwivedi, Ms. PradnyaChikhale, Ms. VrundaBhusari,*** *Department of Computer Science, JSPM's BSIOTR,PuneUniversity,Maharashtra, India*

ISSN: 2278 – 1323

organized flexible storage schemeis designed by partitioning algorithm to guarantee the accessibility of data and data correctness.

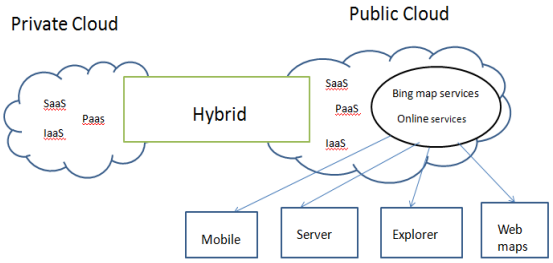

Fig1. Cloud services architecture

In this algorithm the data being used is controlled and Partitioning of data is done in alphabetical order with the help of index method. The actual Partitioning of data happens in vertical and horizontal directions. In order to prevent unrecoverable data loss the security method is also emphasized. Storage and retrieval methods are simplified by reducing the storage area by partitioning algorithm when it is require to store and retrieve the data by merging technique.

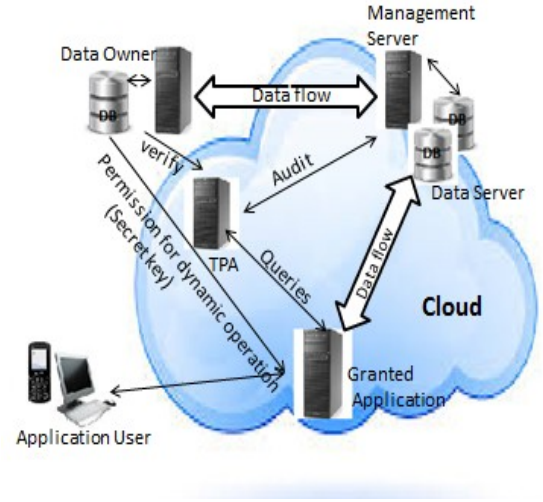

Fig2. Data storage in cloud

The integrity of cloud storage is determined by comparing Digital signature of data. The digital signatures of the client data are first extracted and stored at TPA before sending the client data to server, again the digital signature of client data are extracted at the time of retrieval process and compares with the digital signature at TPA.If both are equal then reliability of data is not despoiled.RSA algorithms are used for encryption and decryption processes and communication of secure cloud data for storing and retrieving process and AES algorithms are used to store client data for security.

II. PROBLEM STATEMENT

A. PDDS - Design goal

To ensure the security and dependability for data storage efficiency in cloud .we aim to plan efficient techniques for dynamic data operation and integrity checking and accomplish the following goals:

- *Dependability:* enhancing the integrity checking mechanisms against the malicious data modification, threads and service attacks, i.e. reducing the effects caused by server failures.
- *Lightweight:* to allow users to check the correctness of data with minimum overhead.
- *Error localization of data:* to successfully locate the faulty server when errors in the data has been detected.
- *Storage:* to confirm users that their data are stored correctly and kept together all the time in the cloud.End user can store their data and applications in cloudservers from anywhere at any time via internet.

B. PDDS - System model

Cloud storage service architecture with different network entities is represented as below.

- *User:* A unit, who has different types of data or applications to be stored in the cloud and depends on the cloud for data storage and computation, can be either enterprise or individual customers.
- *Cloud Server (CS):* A unit, which is accomplished by cloud service provider (CSP) to offer data storage facility and has significant storage area and computational resources.
- Remote data integrity checking: Integrity checking to find and correct the errors in cloud data storage.
- *Third Party Auditor (TPA):* an elective TPA, who has skill and abilities that end users may not have, is reliable to measure and expose threats of

ISSN: 2278 – 1323

cloud storage services on behalf of the users upon demand.

C. Notation and Preliminaries

- F – The data file to be stored in cloud. We assume that F can be represented as a matrix of m equal-sized data, each comprising of n blocks.
- E –Encryption technique is used for Encoding the files each consists of n blocks and ensures security to the data.
- IN- Each independent block comprises an index to signify the block when it is accessed.
- FS-Data files are partitioned into fragments and stored.
- Fek - Creating the public key for encoding the files.
- Fdk - Creating the private key to decode the files for access.
- D –Decryption technique is used for Decoding the files each consists of n blocks and ensures security to the data.

III.RELATED LITERATURE

In literature survey, study is done for checking data integrity and data storage technique that have been recently technologically advanced in the domain of cloud computing.

The secure dynamic operation performed in outsourced data by means of token pre-computation and the design of how it is put in storage in cloud is evaluated [1,2] which offer effective technique for storage of data. Storage integrity checking mechanism is used to identify and avoid unauthorized server considering fast data error localization and its correction. Partitioning technique is used to provide the quality of data, accessibility and security to dependable storage services.

With another new concept of proxy encryption mechanism is discussed in [3] to encode the information. Integrity auditing is done to check the misbehaving server. Data storage distributed mechanism is also support the forwarded data in cloud without repossessing the data back. These features permit more flexible adjustment between the number of storage servers, ensure security provide robustness.

In the research paper [1, 4], the study of data storage integrity in cloud computing is done. Dynamic data operation and public audit ability are used for assisting the data integrity. To have quality in service, extensive security, better performance and independent perspective evaluating with the third party auditor is the aim of this work. Storage model is also developed here to support multiple auditing works to improve security and efficiency.

Partitioning of data in vertical and horizontal direction is another innovative concept discussed in [5]. In this concept, the data is divided into buckets and slicing mechanism is used for storage of data i.e. a new methodology for privacy conserving data publishing. Detail review in [6],[7],[8] shows that the author considers producing signature techniques for providing security and privacy in data storage. Dynamic operations are carried using the RSA based storage security (RSASS) method. This method uses public auditing of the remote data by enhancing existing RSA based signature production. This public key cryptography mechanism is widely used for givingsecurity and data correctness in cloud storage. Reference [9] guarantees remote data integrity with irretrievability.

Reference [11],[13] and [14] defined the “provable data possession” (PDP) model for guaranteeing possession of file on un trusted storages. These systems uses public key based homomorphism tokens for checking the data file. However, the pre-computation of the tokens causes large computation overhead that can be costly for the whole file. In their subsequent research work [13] described a PDP

ISSN: 2278 – 1323

model that utilizes only symmetric key based cryptography. This scheme has lower-overhead than their earlier scheme. Detail review shows that PDP concentrates on single server scenario and does not offer data availability assurance against server failures, leaving both the distributed scenario and data error recovery problem unmapped. Integrity on remote data checking has many challenging issues [4], [12] in cloud storage services.

Among all the technique reviewed the discussions are related to works, which confirms to have data copy in the local system. This restriction is overcome with the proposed methodology PDDS. Token pre-computation method guarantees dynamic data operation and the integrity testing. This technique provides security to the data storage.

Detail survey displays that none of these techniques are able to provide best performances under all uncontrolled circumstances. The limitation with existing techniques is, it time consuming and expensive to perform the dynamic processing of data encryption and decryption to ensure security to data storage in cloud. The PDDS technique kills such limitations with best performance, reduced cost and limited data storage space in cloud. It also guarantees robustness against attacks and unauthorized server.

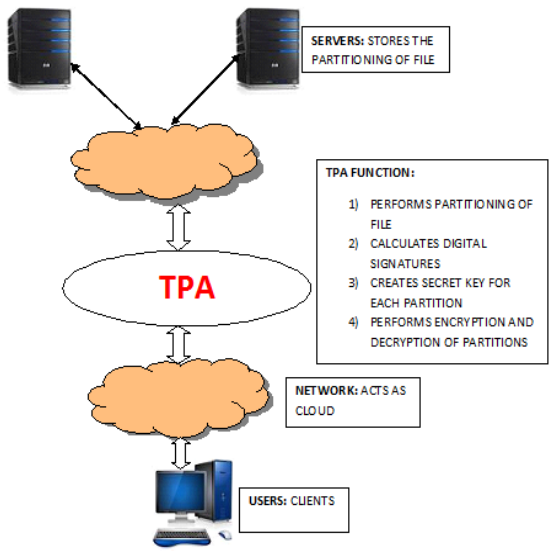

Fig 3. Architecture of data partitioning in cloud

IV.PARTITIONING AND DOMAIN INTEGRITY CHECKING FOR DATA STORAGE

The end user stores the data in the System of cloud data storage. It is also used for maintaining the data in the nearest public house. The PDDS means partitioning and the Domain Integrity Checking for Data Storage. It highly aims on giving an assurance for data security.

To reload the original record from the cloud server the decryption technique processes the private key. The encoded record is decoded to vision the original record with no coupling the re-encryption scheme. The actual Partitioning of data happens in vertical and horizontal directions. In order to prevent unrecoverable data loss the security method is also emphasized.

A. Storage in Cloud

The fig. 3 shows how the cloud helps the users with dynamic data operation and storage security. The hackers cannot access the information .It discovers the black-looking and misbehaving server and also thwart the information from attacks. The architecture of data storage guarantees pre-evaluation to verify the exactness of the records. This occurs prior of storing the data. The dynamic data operation is done after the evaluation. This process enhances the safety since the data are stored after the pre-evaluation process.

The encryption technique is used for generating the security key to ensure safety from illegal access in pre-evaluation process. The encryption and decryption technique generates public and private key to ensure safety. Data integrity function is the significant function in cloud storage. The user keeps on checking whether the stored data in the cloud is proper or not. With the help of integrity checking process, the records are stored with security. Records are handled by remote data integrity checking, they do pre-evaluation process to keep away from intimidation

ISSN: 2278 – 1323

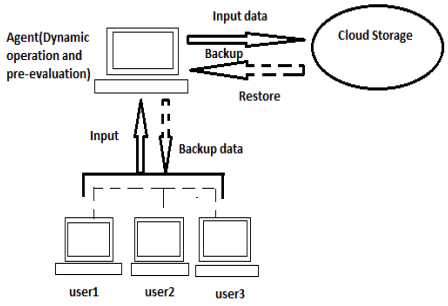

Fig 4.Architechture of Cloud Storage

B. Accessing record from cloud storage

Records are accessed from the storage service on the demand of the end user. As shown in the figure 2 the records are accessed and restored from the storage server by ensuring the record accuracy. To reload the original record from the cloud server the decryption technique processes the private key. The encoded record is decoded to vision the original record with no coupling the re-encryption scheme.

The users can decide the number of records that needs to be accessed and shared by the other members of the cloud. Records accessed from cloud service allow the services in secured way. The records are partitioned into smaller ones before encryption for ensuring security by producing the public key prior the storage. During storage and retrieval of records in cloud PDDS advances the performance by ensuring data security. At the time of retrieval the records are decrypted by producing a private key and combining the record with the original one.

Remote integrity checking helps in preserving the record from risks. It also deals with efficient retrieval and storing processes. The public audit ability method deals with the fault localization, confirmation, unruly server and error recovery. The hackers or unauthorized users are avoided because of this and it also increases the performance, flexibility in access control and to notice the threats. Before partitioning of data the data operations like insert, delete and update are performed. In PDDS the partitioned records are stored on the cloud. During the retrieval these partitioned records are combines to form the original record. Therefore if an unauthorized person tries to access the record then he will not be able to detect that in which server the partitioned records are stored. This enhances the cloud storage services and the data storage costs are also reduced by this mechanism.

C. Data Partitioning

Partitioning means the division of a record. It plays a vital role in the cloud storage. It breaks up the larger file into smaller parts to store the record efficiently in a quick way by enhancing trouble-free access to records. The original record length is large and complex so it is difficult to store it in cloud. To reduce the complexity we use the partitioning function to make storage easy.

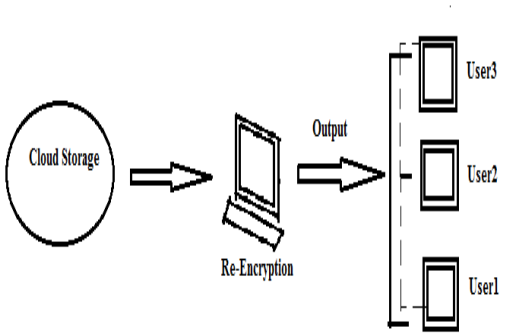

Fig5.Accessing Record from cloud

The partitioning takes place as soon as the records are provided for storing in cloud. The portioned files are first encrypted and assigned by the public key. During the retrieval these files are decrypted with the private key. The original file is also reconstructed if there is a need to access the same. The partitioning and merging can be well understood by the following algorithm.

Algorithm 1: Partitioning and merging files

- s =Maximum storage size.
- Load the participating file and its size.
- Partitioning files: Count size <= s then split file in to n blocks with extension and index value.
- Return files, otherwise announce as unacceptable size
- Encrypt all partitioned files and store in cloud.

ISSN: 2278 – 1323

- Merge files: check if (! file) then file is absent. Otherwise count the index value and merge files.Return file.
- Merge the decrypted file for access.

V. IMPLEMENTATION ISSUES

The methods and techniques which are used for data partitioning and to maintain its integrity, are being explained under in this section. These techniques such as hash calculation, partitioning of data, Encryption and Decryption are used. The factors like computational cost, storage space, time, performance and efficiency are also considered. The modules which are used for enhancing data integrity by data partitioning operation are defined as follows.

A. Public Audit ability

This module is used to identify the error localization and misbehaving server at the time of storing of data with security. The third party auditor plays an important role in dividing and in merging of files at the time of retrieval and of storing of data in cloud.

B. File Access

The data which are stored in cloud are easily accessible by the user as per their requirement. At the time of storing of data in cloud, Partitioning and Encryption techniques are used and also at the time of retrieval, Decryption technique is used.

C. User Revocation

This module will keep the records of key which are used during the time of Encryption and Decryption of data in cloud. At the time of re-encrypting of the original data, one private key is generated for the user and the information are managed properly.

D. Hashing

This technique is used to calculate the hash function and the digital signature of the partitioned data. SHA algorithm is used to calculate the hash of the partitioned data and it will help also help to find the digital signature of these data.

E. Encryption

Encryption is defined as the technique which is used to encrypt the data for security purpose The file will be in coded form(cipher), by the time of encrypting the data. RSA algorithm will be used, where public and private RSA key are used at the time of encrypting the data and then it get stored in cloud. The public key is known to everyone. In symmetric encryption, private key is used and in asymmetric encryption, public key is used.

***Algorithm 2:*Encryption**

1. Generate a Code object and Key Generator object.
2. Generate a session (secret) key using code object.
3. Secret key will be used to initialize
4. The files will be encrypted.
5. Obtain recipient's public key and generate Code and initialize it for encryption with recipient's public key.
6. Generate preserved Object to lock secret key using asymmetric Code and Serialize preserved Object.
7. Return the encrypted files and serialized preserved Object to recipient.

F. Decryption

Decryption is defined as the technique which is used to decrypt the data at the time of retrieval from cloud. Here private key is used to access the files from cloud. Separate Private key is generated for each end user. So that users can access the files from any location with security. The private key which is used by end users to decrypt the files are non shareable

***Algorithm 3*: Decryption**

1. Obtain encrypted message and serialized preserved Object.
2. Re-serialize preserved Object.
3. Generate code object, and initialize it for decryption and create secret key.
4. Open the key using the asymmetric Code.
5. Generate Code object and Initialize it with the recovered secret key for decryption.
6. The files for access will be decrypted.

ISSN: 2278 – 1323

VI . PERFORMANCE ANALYSIS

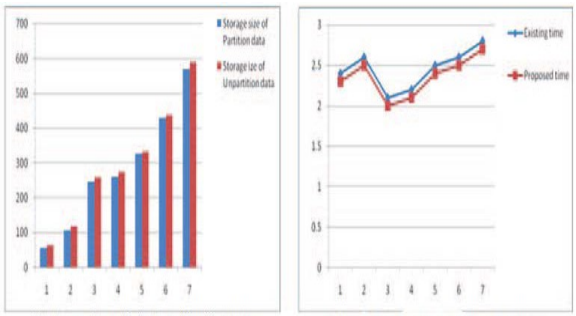

Fig.Storage Space Reduction in Data Partitioning

Fig.Storage Time Reduction in Data Partitioning

Fig.6 Performance Analysis

In Fig.6, the performance of the reduced spaceduring storage of the partitioned data with data security isshown. It is analyzed that the data partitioning techniqueoutperformance the existing method by reducing thecomplexity of data storage and access time. It alsoshows the time reduction during the data storage. By thisway the data can be stored in a quick manner and theretrieval can happen effectively.

VII .CONCUSION AND FUTURE SCOPE

In this paper, we put forward an efficient record storage security in cloud service. The partitioning of record permits storing of the record in straightforward and efficient way. Dynamic operations are a further important concept where, encoding and decoding process secures records. It also provides method for flexible access and retrieval. Cost is reduced in data storage. The time and space is also reduced through storage. Also the remote data integrity checking identifies the threats and unruly server while storing the records in cloud guaranteeing data security. Future effort is designed to offer advanced level of protection and probing mechanisms for outsourced evaluations in cloud services.

ACKNOWLEDGEMENT

This work was guided by Prof.Mrs.VrundaBhusari. Authors would also like to thank Prof. Mrs.G.M. Bhandari head of computer department, JSPM's BSIOTR & Prof. Mrs. J. Chaudhari, project coordinator for providing all facility and every help for smooth progress of Project work

REFERENCES

[1] C. Wang, Q. Wang, K. Ren, and W. Lou, "Ensuring Data Storage Security in Cloud Computing," Proc. 17th Int'l Workshop Quality of Service (IWQoS '09), pp. 1-9, July 2009.

[2] Wang Cong, Wang Qian, RenKui, Cao Ning and Lou Wenjing , "Toward Secure and Dependable Storage Services in Cloud Computing," Services Computing, IEEE Transactions on , vol.5, no.2, pp.220-232, April-June 2012.

[3] Hsiao-Ying Lin; Tzeng, W.-G.; , "A Secure Erasure Code-Based Cloud Storage System with Secure Data Forwarding," Parallel and Distributed Systems, IEEE Transactions on , vol.23, no.6, pp.995-1003, June 2012.

[4] Qian Wang; Cong Wang; KuiRen; Wenjing Lou; Jin Li; , "Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing," Parallel and Distributed Systems, IEEE Transactions on , vol.22, no.5, pp.847-859, May 2011.

[5] Tiancheng Li; Ninghui Li; Jian Zhang; Molloy, I.; "Slicing: A New Approach for Privacy Preserving Data Publishing," Knowledge and Data Engineering, IEEE Transactions on , vol.24, no.3, pp.561-574, March 2012.

[6] Zhiguo Wan; Jun'e Liu; Deng, R.H.; , "HASBE: A Hierarchical Attribute-Based Solution for Flexible and Scalable Access Control in Cloud Computing," Information Forensics and Security, IEEE Transactions on , vol.7, no.2, pp.743-754, April 2012.

[7] Paredes, L.N.G.; Zorzo, S.D.;, "Privacy Mechanism for Applications in Cloud Computing," Latin America Transactions, IEEE (Revista IEEE America Latina) , vol.10, no.1, pp.1402-1407, Jan. 2012.

[8] C. Wang, S.S.M. Chow, Q. Wang, K. Ren, and W. Lou, "Privacy- Preserving Public Auditing for Secure Cloud Storage," IEEE Trans. Computers, preprint, 2012.

[9] Takabi. H, Joshi.J.B.D and Ahn.G, "Security and Privacy Challenges in Cloud Computing Environments," Security & Privacy, IEEE, vol.8, no.6, pp.24-31, Nov.-Dec. 2010.

[10] K. Ren, C. Wang, and Q. Wang, "Security Challenges for the Public Cloud," IEEE Internet Computing, vol. 16, no. 1, pp. 69-73,2012.

[11] C. Wang, K. Ren, W. Lou, and J. Li, "Towards Publicly Auditable Secure Cloud Data Storage Services," IEEE Network Magazine, vol. 24, no. 4, pp. 19-24, July/Aug. 2010.

[12] C. Wang, Q. Wang, K. Ren, and W. Lou, "Privacy-Preserving Public Auditing for Storage Security in Cloud Computing," Proc. IEEE INFOCOM, Mar. 2010.

[13] G. Ateniese, R. D. Pietro, L. V. Mancini, and G. Tsudik, "Scalable and efficient provable data possession," in Proc. of SecureComm'08, 2008, pp. 1–10.

[14] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, "Provable Data Possession at Untrusted Stores," Proc. of CCS '07, pp. 598–609, 2007.

ISSN: 2278 – 1323

Authors

***Ms. AparajitaSain**, Department of Computer Science, JSPM's BSIOTR, India*

***Ms. Parna Dutta,** Department of Computer Science, JSPM's BSIOTR, India*

***Ms. NamrataDwivedi, Ms. PradnyaChikhale, Ms. VrundaBhusari,** Department of Computer Science, JSPM's BSIOTR,PuneUniversity,Maharashtra, India*

ISSN: 2278 – 1323