International Journal of
Emerging Research in Management &Technology
ISSN: 2278-9359 (Volume-3, Issue-3)

Research Article | **March 2014**

Partitioning Data and Domain Integrity Checking for Storage - Improving Cloud Storage Security Using Data Partitioning Technique

Santosh Jogade*, Ravi Sharma, Prof. Rajani Kadam
Department Of Computer Engineering
Dr.D.Y.Patil College of Engineering,
University Of Pune, India

Abstract—

Cloud computing is the delivery of computing services over the Internet. Cloud services allow individuals and businesses to use software and hardware that are managed by third parties at remote locations. In cloud computing data security, integrity and access control are challenging issues, these issues remain the primary inhibitor for adoption of cloud computing services. Existing solutions that use pure cryptographic techniques to mitigate security and access control problems. In this paper we proposed data partitioning technique with cryptography which ensure cloud storage security, integrity and error identification. Cloud storage integrity checking concept is used to enhance the integrity of cloud storage. System model comprises of three layers namely user machine, Third Party Auditor (TPA) and cloud storage servers. Partitioning method implemented at third party auditor.TPA performs operation like partition data, Extract digital signature of each partition, Secret key generation for each partition, Encrypt each partition using respective keys, storing partition sequence, signature key and file attribute on its own its own server, sending partition at appropriate server, retrieving as well merging of partitions, Decryption and integrity checking of data. These avoid the copy of data at user side. This work aims to provide robust security with optimum space and reduced time.

Keywords — Cloud Storage, Error Identification, Partitioning, Cloud Storage Integrity Checking, Digital Signature Extraction, Encryption, Decryption

I. INTRODUCTION

Cloud computing is the use of computing resources (hardware and software) that are delivered as a service over a Internet. Definition of cloud computing model, the most widely used one is made by NIST as "Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model promotes availability and is composed of five essential characteristics, three service models, and four deployment models." The cloud computing model NIST defined has three service models and four deployment models. The three service models, also called SPI model, are: Cloud Software as a Service (SaaS), Cloud Platform as a Service (PaaS) and Cloud Infrastructure as a Service (IaaS). The four deployment models are: Private cloud, Community cloud, Public cloud and Hybrid cloud.

1. Public Cloud - A public cloud can be accessed by any subscriber with an internet connection and access to the cloud space.
2. Private Cloud - A private cloud is established for a specific group or organization and limits access to just that group.
3. Community Cloud - A community cloud is shared among two or more organizations that have similar cloud requirements.
4. Hybrid Cloud - A hybrid cloud is essentially a combination of at least two clouds, where the clouds included are a mixture of public, private, or community.

Storage servers are managed in the distributed manner system like cloud. Third party auditing and the remote integrity checking, providing the data dynamics. Remote service is responsible of preventing the data loss. The cloud remote integrity checking mechanism detects the data corruption hence misbehaving server in the cloud storage. The advantage of the cloud storage is flexible with reduced cost and they also manage the data loss risk and so on. The architecture for cloud computing is as shown in Fig.1.

In the proposed work efficient flexible storage scheme designed to ensure the availability of data and data correctness in cloud, by partitioning algorithm. Data storage is done by using this algorithm. Partitioning happens in vertical and horizontal directions whereby the data being used is controlled. The security mechanism is also emphasized in order to prevent unrecoverable data loss. Storage and retrieval process are simplified by reducing the storage space when there is need to store and retrieved by merging technique correctness in cloud, by partitioning algorithm .cloud storage integrity checked by comparing Digital signature of data. Digital signature of data extracted before sending data to sever these digital signature stored at TPA, at time of data retrieval again digital signature of data extracted and compares with digital signature stored at TPA. If both are same then integrity of data not violated.

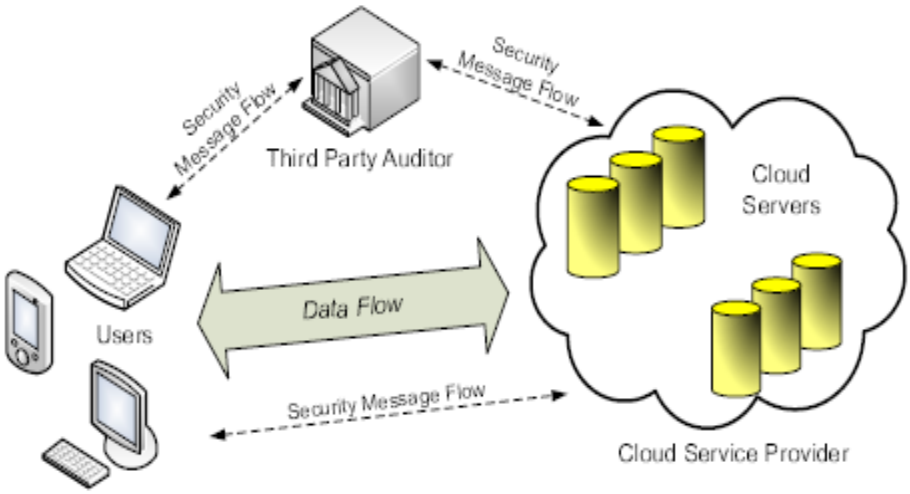

Fig.1: The architecture of cloud data storage service

II. CURRENT METHODOLOGY

Third Party Auditor is act as mediator and checker. There are two categories: private auditability and public auditability. Although private auditability can achieve higher scheme efficiency, public auditability allows anyone, not just the client, to challenge the cloud server for the correctness of data storage while keeping no private information. To let off the burden of management of data of the data owner, TPA will audit the data of client. It eliminates the involvement of the client by auditing that whether his data stored in the cloud are indeed intact, which can be important in achieving economies of scale for Cloud Computing. The released audit report would help owners to evaluate the risk of their subscribed cloud data services, and it will also be beneficial to the cloud service provider to improve their cloud based service platform. Hence TPA will help data owner to make sure that his data are safe in the cloud and management of data will be easy and less burdening to data owner [1]. Clouds have no borders and the data can be physically located anywhere in the world. So this phenomenon raises serious issues regarding user authentication and data confidentiality [5]. [3]The three major problems identified in references are legal issues, compliance and loss of control over data. These legal- and governance related concerns are followed by the first technical issue, isolation, with 7% of citations. The least cited problems are related to security configuration concerns, loss of service , firewalling and interfaces.

A privacy-preserving public auditing system for data storage security in Cloud Computing, where TPA can perform the storage auditing without demanding the local copy of data[2]. It utilize the homomorphism authenticator and random mask technique to guarantee that TPA would not learn any knowledge about the data content stored on the cloud server during the efficient auditing process, which not only eliminates the burden of cloud user from the tedious and possibly expensive auditing task, but also alleviates the users' fear of their outsourced data leakage. Considering TPA may concurrently handle multiple audit sessions from different users for their outsourced data files, we further extend our privacy-preserving public auditing protocol into a multi-user setting, where TPA can perform the multiple auditing tasks in a batch manner, i.e., simultaneously. Extensive security and performance analysis shows that the proposed schemes are provably secure and highly efficient. [3]The public key, hash, and private key ciphers that are proposed between cloud service provider, data owner, and user ensure an isolated and secure execution environment at the cloud. We believe all these advantages of the proposed schemes will shed light on economies of scale for Cloud Computing.

[4] A cloud-based storage scheme that allows the data owner to benefit from the facilities offered by the CSP and enables indirect mutual trust between them. The proposed scheme has four important features: (i) it allows the owner to outsource sensitive data to a CSP, and perform full block-level dynamic operations on the outsourced data, i.e., block modification, insertion, deletion, and append, (ii) it ensures that authorized users receive the latest version of the outsourced data, (iii) it enables indirect mutual trust between the owner and the CSP, and (iv) it allows the owner to grant or revoke access to the outsourced data. We discuss the security issues of the proposed scheme. Besides, we justify its performance through theoretical analysis and experimental evaluation of storage, communication, and computation overheads.

In the survey conducted the discussions are related existing system, which ensures to have data copy in the local system. This limitation is overcome with the proposed approach. This mechanism provides data storage security. The limitation with existing mechanism is, it takes more time and cost to perform the dynamic processing of data encryption and decryption techniques to store data in cloud with security. Proposed method overcomes such limitations with high performance, reduced cost and limited data storage space in cloud.

III. PROPOSED METHODOLOGY

In cloud data storage system, the clients stores data in cloud and also they maintain data locally. Here Partition of data provides security is in providing the security and avoid local copy of data.Fig.2 show the proposed system architecture.

Our proposed system divided in 3 different layers as follow:

1. Client machine: client machine are used by users who have to be data stored on cloud.
Client machine either PC or browser enabled mobile device that rely on the cloud for data computation, consist of individual consumers and organizations.
2.cloud storage server: Manage and provide storage space, computational resources and storage services by the cloud service provider (CSP).
3. Third Party Auditor (TPA): TPA, who has expertise and capabilities that users may not have, is trusted to assess and expose risk of cloud storage services on behalf of the users upon request.TPA perform security related operations .

Partitioning data

Partitioning of data performed at Third Party Auditor. Partitioning module accept user input file. Partitioning function has an important role in this work. It Splits (break up) larger files into smaller parts. It helps to store the data effectively in quick manner enhancing easy access to data also when there is need. The original data is complex and there is Difficulty in storing it in cloud, so partitioning function is used to make the storage easy in cloud. The partitioned files are encrypted, that is encoded with the public key and stored in cloud. Partitioning takes place automatically when the data is fed for storing in cloud. Original file is also reconstructed when there is need to access the same.

Algorithm: Partitioning and merging files

1. Load the Input file.
2. Calculate size of file.
3. Partitioning file: If size<=minimum size or size>=maximum size Show error message.
   Else
   Split file respect to number of servers with extension and index value.
4. Extract Digital Signature of each partition.
5. Generate secret key for each partition.
6. Encrypt respective partition using respective secret keys.
7. Store partition sequence, digital signature, keys and file attribute at TPA.
8. Send each partition at respective server.
9. Merging file: TPA request for file partitions from servers.
10. Extract new digital signature of each partition and compare it with stored digital signature at TPA.
    If new digital signature equals to stored digital signature at TPA
    Merge file otherwise data is corrupted.
11. Decrypt the merged file with key.

Encryption

Encryption technique is used to encrypt the partitions of files for security. By encrypting the file, the file will be in cipher. A common approach is used to encrypt with shared key algorithm and public key is randomly generated. Here we create public and private RSA key for encrypting the files, and stored in cloud. The generated private key length is 2048 bits. Secret key is symmetric encryption

Decryption

Decryption technique is used to decrypt the partitions of files and the private key is generated to access files from cloud. For each end user separate private key is generated to access from any location with security. Non shared private key is used to decrypt files. The private key is an asymmetric technique. When decrypting files private key is generated for accessing ensuring file access control

Cloud storage integrity checking

Cloud storage integrity checking is used to preventing the data loss. It also manages the effective storage and retrieval processes. The public auditability method manages the error identification by comparing digital signature, verification, misbehaving server and error recovery. This ensures data security from unauthorized access. It also increases the performance. Flexible access control is also provided for authentication in this work and to detect the attacks. Dynamic data operation, like insertion, deletion, and updating is also done before partitioning the data.

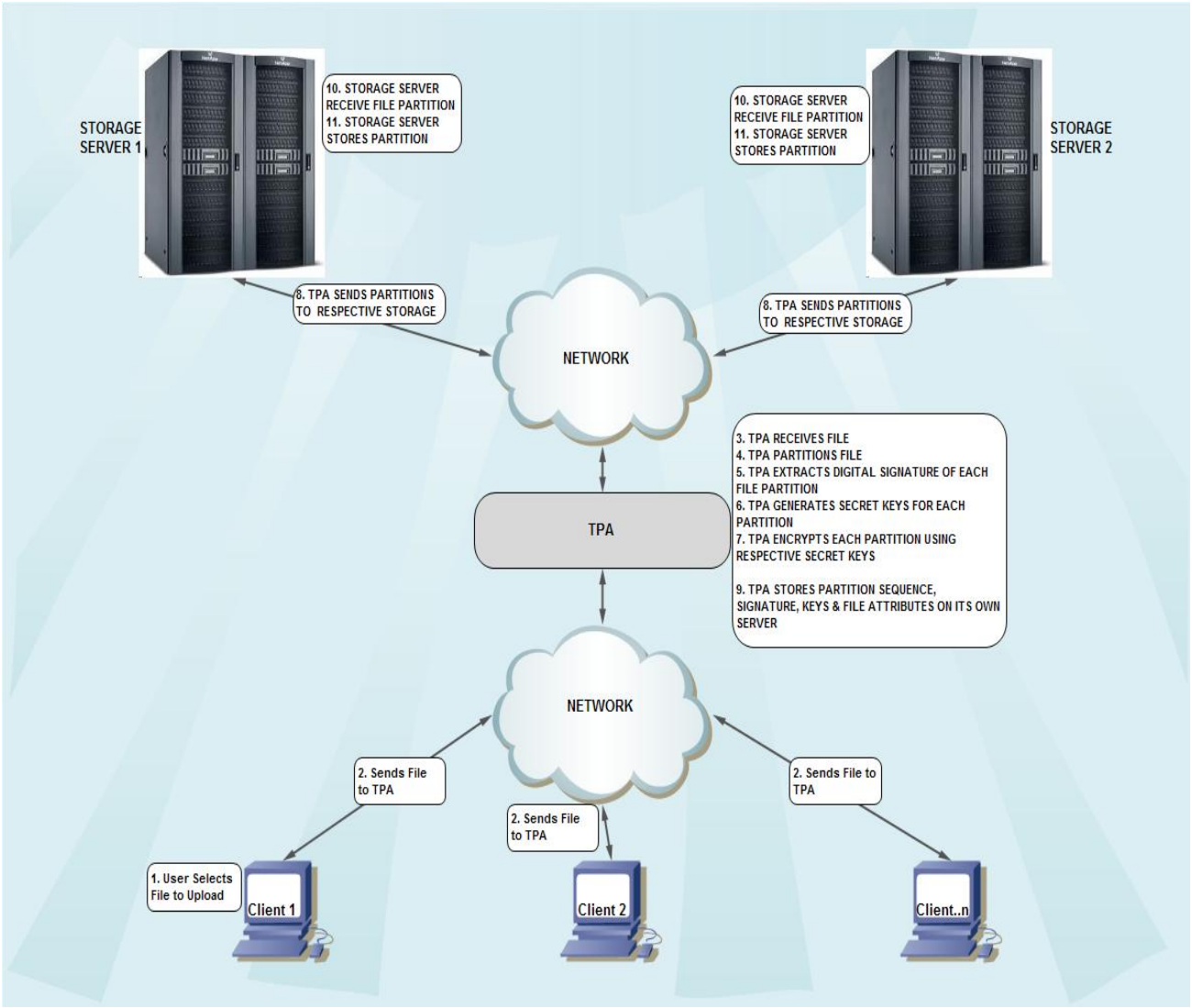

Fig.2 Proposed system architecture

IV. CONCLUSIONS

In this paper we proposed data partitioning technique for data storage security in cloud service. The partitioning of data enables storing of the data in easy and effective manner. Partitions are again divided into chunks for send at servers this helps to quick retrieval and store. It also gives way for flexible access and there is less cost in data storage. Cloud storage integrity concept used to ensure integrity of stored data The space and time is also effectively reduced during storage. Dynamic operation, encoding and decoding process secures data, when storing into cloud. Also Future work is planned to provide higher level of security and searching mechanisms for outsourced computations in cloud services

References

[1] Bhavna Makhija,VinitKumar gupta,Indrajit Rajput ,"Enhanced Data Security in Cloud Computing with Third Party Auditor",Hasmukh Goswami College of Engineering,Vahelal,Gujarat, International Journal of Advanced Research in Computer Science and Software Engineering

[2] Cong Wang, Qian Wang, Kui Ren, and Wenjing Lou,"Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing", IEEE INFOCOM 2010, San Diego, CA, March 2010

[3] Sunil Sanka, Chittaranjan Hota, Muttukrishnan Rajarajan," Secure Data Access in Cloud Computing", Computer Science and Information Systems Group, Birla Institute of Technology and Science-Pilani.

[4] Ayad F. Barsoum and M. Anwar Hasan," Enabling Data Dynamic and Indirect Mutual Trust for Cloud Computing Storage Systems", University of Waterloo, Ontario, Canada. IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSYEMS VOL: PP NO: 99 YEAR 2013

[5] Nelson Gonzalez, Charles Miers, Fernando Red, Marcos," A quantitative analysis of current security concerns and solutions for cloud computing", at Journal of Cloud Computing: Advances, Systems and Applications 2012, 1:11

[6] M. Sudha, Dr.Bandaru Rama Krishna Rao, M. Monica," **A** Comprehensive Approach to Ensure Secure Data Communication in Cloud Environment" International Journal of Computer Applications (0975 – 8887) Volume 12– No.8, December 2010