ISSN:0975-9646

Data Partitioning Technique to Improve Cloud Data Storage Security.

Swapnil V.Khedkar , A.D.Gawande

Information Technology, Computer Science, SGBAU University
Amravati, Maharashtra, India

Abstract— Cloud storage enables users to remotely store and retrieve their data and enjoy the on-demand high quality cloud applications without the burden of local hardware and software management. Cloud storage system enables storing of data in the cloud server efficiently and makes the user to work with the data without any trouble of the resources. Cloud computing is highly promising technology because of its unlimited resource provisioning and data storage services which help us in managing the data as per requirements. In the existing system, the data are stored in the cloud using dynamic data operation with computation which makes the user need to make a copy for further updating and verification of the data loss. An efficient distributed storage auditing mechanism is planned which over comes the limitations in handling the data loss. In this work the partitioning method is proposed for the data storage which avoids the local copy at the user side by using partitioning method.

The cryptography technologies offer encryption and decryption of the data and user authentication information to protect it from the unauthorized user or attacker. This method ensures high cloud storage integrity, enhanced error localization and easy identification of misbehaving server. To achieve this, remote data integrity checking concept is used to enhance the performance of cloud storage. The data is stored in cloud datacenter hence this work aims to store the data in reduced space with less time and computational cost. Cloud storage is flexible with reduced cost and manages the data from loss risk. The Cloud server allows user to store their data on a cloud without worrying about correctness & integrity of data. Cloud data storage has many advantages over local data storage.

***Keywords*— AES Cryptographic Tools, RSA Algorithm, MD5, Data Partitioning Technique, Cloud Exchange, Datacenter**.

I. INTRODUCTION

The Internet access becomes available in the recent years, Cloud computing is an internet based technology, Cloud Computing is using hardware and software as computing resources to provide service through internet, Cloud computing being used widely nowadays to enable the end user to create and use software without worrying about the execution of the technical information from anywhere at any time. Over the network the resources are utilized and after computation these are delivered as services in cloud computing. The Cloud Computing technology is embedded with three services which are just one click away, easy to use and pay as you use the service. Cloud storage is a service for developers to store and access data in cloud. Cloud service provider will manage and control the cloud resources. Client uses the client devices to access a cloud system via World Wide Web. The benefits of the cloud storage are flexible with reduced cost and they also manage the data loss risk and so on. Recently many work focus towards third party auditing and the remote integrity checking, providing the data dynamics. Remote archive service is responsible for properly preserving the data. The remote data integrity checking protocol detects the data corruption and misbehaving server in the cloud storage. In the proposed work Data partitioning technique, remote data integrity checking is analyzed in internal and external ways. Partitioning happens in alphabetical order by using of index method 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.MD5 concept are used to check the integrity of data before storing of the data in dacenter.AES algorithm are used to store end user client data for security and RSA are used for communication of secure cloud data for storing and retrieving process.

II. LITERATURE REVIEW

In the Data Partitioning Technique literature review is done for data integrity checking and data storage mechanisms that are currently used in dynamic multi transactional applications. The dynamic data storage with token pre-computation and AES algorithm how it is stored in cloud is analyzed [1], [12] Integrity checking concepts is also used to detect and avoid misbehaving server considering data correction and error localization. Distributed scheme is used to achieve the data quality, availability, integrity of dependable storage services. The data storage using dynamic data operation method is used to perform various operations. Security analysis is done by RSA to encode the data. Distributed storage system is also used to support the forwarded data in cloud without retrieval, ensuring secured and robust data in cloud storage. Data integrity in cloud storage devices are analyzed in the research works [8],[12]. Dynamic data operation and public Auditability are used for supporting the data integrity. The objective of this work is to have independent perspective and quality in services evaluating with the third party auditor. Storage model is also devised here to support multiple auditing tasks to improve efficiency. In the works [3], [4], [5], author considers generating signature methods for ensuring the cloud storage security. Dynamic operations are supported by using the RSA method. This method discusses data integrity and data correctness stored in cloud.

Reference [11] ensures remote data integrity with retrievability. Error correction and data integrity checking is used to detect the availability of data in cloud. Data availability and data error recovery mechanisms are not given much importance. In cloud storage services remote data integrity checking has many challenging issues [8], [9]. In the survey done much of the discussions are related to works, which ensures to have data copy in the local system. This limitation is overcome with the proposed approach of Data Partitioning Technique.

III. Analysis Of Problem

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. The Data Partitioning Technique overcomes such limitations with high performance, reduced cost and limited data storage space in cloud. It also ensures resilient against threads, attacks and misbehaving server.

To ensure security and data storage efficiency in cloud. Cloud Data partitioning and Integrity checking is designed effectively.

- Enhance the mechanisms work of the integrity checking against the service attacks and threads.
- Communication and computation cost in sharing and storage of the data in cloud.
- Error localization of data: Compute and consists fast access of the data and detect the error.
- Storage: End user can store the data in cloud at anytime and anywhere through internet.
- End user: Enable end user for storing the data without any difficulty in cloud.
- Web Server: Web Server contains various clouds Interface Storage Application
- Cloud Server (CS): Manage and provide storage space, computational resources and storage services by the cloud service provider (CSP).
- MD5 Technique for data integrity checking: Integrity checking to detect the data error and data localization in cloud data storage.

IV. Implimented Work

To improve cloud data storage security, we have to work on Data Partitioning Technique, Data Integrity Checking for data storage, and end users can stores their data in cloud with help of cryptographic tool for secure data storage.

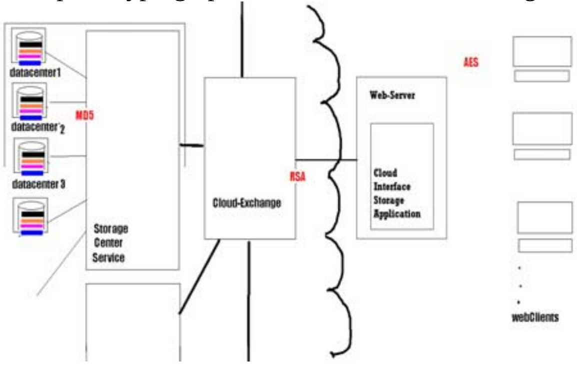

Fig. 1 Cloud Data Partitioning

A. *End user*

The numbers of end users are used web browser and access cloud interface storage application by using host name and local port number. By using that application allocated on web server we can store end user data on cloud server in secure way. The data security is provided to the data which is stored in storage cloud by using the encryption technique.

B. *Cloud Storage Server*

It detects the threats and misbehaving server and also prevents the data from attacks. Cloud Storage Server is a main storage server, it contents cloud exchange, cloud coordinator and four datacenter. Cloud exchange waits for client connection request. When it is accept client connection request at same time create a client request handler thread to handle another request and it is to be continuously. Client thread to handle client request methods- Constructor Method is Initialize client Thread to stores socket and storage Manager Reference in data members. Run Method will read a request first then process the request and send a response to the cloud client. In the process request first it will read command, domain name and password from client request packet. In datacenter to check a domain is registered or not if not registered then send a error massage in a response to the cloud client else do operation according to command. With the help of these commands we can perform four operations like store file, get file, delete file, or file list. At the time of storing file it retrieves file name, file size, and domain name from request packet and sends a request to storage manager to store a file. At the time of getting a file retrieve file name and port number from request packet and send a request to storage manager to get a file. To delete file retrieve file name and send a request to storage manager and it also show the file list according to client request send to storage manager.

Domain Manager to manage domains methods: In this method to check or verify domain is registered or not in domain folder is presented on data centre. If not present return false otherwise read password from password files if match return true else false.

C. *Access Data from Cloud Storage Service*

Cloud Data are retrieved from the storage service as per the end user request. Data Storage architecture the end user can also decide what data need to be accessed and shared by the other users in cloud. Data accessed from cloud service enables the services in secured manner. MD5 improves performance ensuring data security during storage and retrieval of data in cloud. The data is partitioned into smaller blocks with file name before encryption for security by generating the public key to encode the data before storage. During the retrieval, the data are decrypted by generating the private key. Remote data integrity checking is used to maintain the data from threats. It also manages the effective storage and retrieval processes. This ensures data security from unauthorized access. Storage Manager will maintain cloud client storage space. And separate folder will maintain for each sub domain to store files .Port counter will be maintain to store a new thread to store and receive file. To store cloud client file on cloud then port counter will be increment and create a new thread of type

UDP File Store with new port to receive a file. To send a file from cloud to cloud client first it will check the file is present or not in datacenter and send a response at the same time create a new thread UDP File Send to send a file to cloud client. To delete a file from cloud check if file is present or not if not present then return false else will delete the file. To get file list will return file list of a sub domain to cloud client check if sub domain is present or not if not present then return blank else return file list separated by comas. UDP File Store it will receive a file from cloud client and will store at a specified location on datacenter. UDP File Send it will send a file to cloud client at a specified IP address and Port number from specified location on datacenter.

D. Cloud Exchange

Cloud Exchange Server wait for client application connection request when it is accept the client application connection request at the same time creates client request handler object to handle another client request. At the same time Client Thread to handle client request then read, process and send a response to the client by using RSA algorithm. In cloud exchange cloud Info class to maintain cloud service Information. To maintain Cloud Service Registry it reads the information from "Cloud" which maintains cloud service registry and then creates Cloud Info type of object for each Service then register the cloud service.

Cloud Computing is not secure computing model because there are many data security issues. The data security is provided to the data which is stored in datacenter by using the encryption technique. But still there is a loophole through which the data integrity can be compromised i.e. when data is moving from the storage cloud to computational cloud for processing. So, in this paper we are going to secure data in this stage to make the cloud computing more reliable technology for customers .In the below diagram, first of all end user asks for the task execution from the broker. After this, broker again asks end user for the task specification and end user submits its task specification.

Thereafter broker sends task specification to the cloud exchange to get the available clouds. Cloud exchange sends request to all connected cloud coordinator to provide their current status with available resources needed to complete the execution of the task. Cloud coordinator updates the available datacenter of the cloud to cloud exchange. Cloud exchange gives information of available of all clouds and datacenter to broker. Broker asks end user to send encrypted data using AES cryptography tool. Finally broker receives encrypted data with key from end user and forwards this data to the cloud exchange to storage cloud service to store the data in datacenter by using partitioning algorithm, and whenever data will retrieve from the storage cloud service to cloud client. Then again it will be decrypted at cloud storage interface application with help of cryptographic tool end user or end user can decrypt that data by using key which are known to end user which are presented in given path of key folder in own computer system.

Fig .2 Cryptographic Tools by Using AES

E. RSA Algorithm

RSA algorithm is designed by Designed by Ron Rivest, Adi Shamir, and Leonard Adleman Published in 1977.Most commonly used for encryption and authentication algorithm. It involves a public key and private key. The public key can be known to everyone and is used for encrypting messages. The basic steps of RSA algorithm are Key Generation Encryption and Decryption

1) Encryption:

Encryption technique is used to encrypt the 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 and public key is asymmetric encryption.

Algorithm 1: Encryption

1. Create a Cipher object and Key Generator object.
2. Create a Secret (private) key using cipher object.
3. Initialize it with private key.
4. Encrypt the files.
5. Get recipient's public key and Create Cipher and Initialize it for encryption with recipient's public key.
6. Create Sealed Object to seal session key using Asymmetric Cipher and Serialize Sealed Object.
7. Return the encrypted files and serialized Sealed Object to recipient.

1) Decryption:

Decryption technique is used to decrypt the 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.

Algorithm 2: Decryption

1. Get encrypted message and serialized Sealed Object.
2. Re-serialize Sealed Object.

3. Create Cipher object, and initialize it for decryption
   And generate private key.
4. Unseal the key using the asymmetric Cipher.
5. Create Cipher object and Initialize it with the Recovered private key for decryption.
6. Decrypt the files for access.

F. MD5 Message Digest Algorithm

MD5 algorithm was developed by Professor Ronald L. Rivest in 1991. According to RFC 1321, “MD5 message-digest algorithm takes as input a message of arbitrary length and produces as output a 128-bit "fingerprint" or "message digest" of the input. The MD5 algorithm is intended for digital signature applications, where a large file must be "compressed" in a secure manner before being encrypted with a private key under a public-key cryptosystem such as RSA. MD5 is an algorithm that is used to verify data integrity through the creation of a 128 bit message digest from data input. MD5 digests have been widely used in the software world to provide some assurance that a transferred file has arrived intact.

G. Partitioning Data

Partitioning function plays an important role in this work. It splits (break up) larger files into smaller parts 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. Partitioning happens alphabetical order by using index method. It retrieves first two letters and checks it in folder with present having same letter. If it is not present then creates a folder and store the file in that folder .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. The partitioning concept is provided in the following algorithm.

Algorithm 1: Partitioning

```
1. Load the Input file with name.
2. Retrieve first two letters.
3. Check it in folder.
4. With present having same letter.
5. If not present then create a folder.
6. Encrypt all partition file with the help of public key
   and store the file in cloud datacenter
7. Decrypt the original file with the help of private key
   when there is need to access the end user.
```

V. PERFORMANCE ANLYSIS

In Fig. 3 contents the performance of the reduced space during storage of the partitioned data with data security is shown. It is analysed that the data partitioning technique outperformance the existing method by reducing the complexity of data storage and access time. Explicitly shows the time reduction during the data storage. By this way the data can be stored in a quick manner and the retrieval can happen effectively.

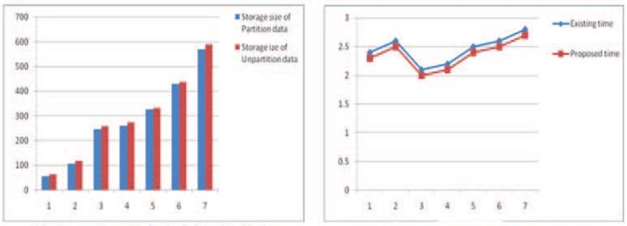

Fig.Storage Space Reduction in Data Partitioning

Fig.Storage Time Reduction in Data Partitioning

Fig.3 Performance Analysis

VI. CONCLUSION AND FUTURE WORK

In this review paper, We propose an efficient data storage security in cloud service. The partitioning of data enables storing of the data in easy and effective manner. It also gives way for flexible access and there is less cost in data storage. The space and time is also effectively reduced during storage. Dynamic operation is another key concept where, encoding and decoding process secures data, when storing into cloud. Also the remote data integrity checking detects the threats and misbehaving server while storing the data in cloud ensuring data security. Future work is planned to provide higher level of security and searching mechanisms for outsourced computations in cloud services.

REFERENCES

[1] Wang Cong, Wang Qian, Ren Kui, 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.

[2] 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.

[3] 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.

[4] 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.

[5] 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.

[6] Tian cheng 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.

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

[8] Qian Wang; Cong Wang; Kui Ren; 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.

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

[10] 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.

[11] 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.

[12] 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.

[13] C. Selvakumar, G. Jeeva Rathanam, M. R. Sumalatha,” PDDS - Improving Cloud Data Storage SecurityUsing DataPartitioning Technique” 3rdIEEE International Advance Computing Conference (IACC),2013.