Data Partitioning Technique to Improve Cloud Data Storage Security.

[1] vikram kurandale, [2]Amit Gobare, [3]Pournima Dhumal, [4]Komal Gaikwad
Computer Department
P.D.E.A's college of engineering, Pune

***Abstract*—Use of cloud computing is increasing rapidly but the security is main issue inside the cloud computing. Lot of research have been done on the cloud. Data can be efficiently store, share and download on the cloud storage. This improves user's interaction with resources without any trouble. There are number of techniques to achieve the security in the cloud security inside the cloud computing. Many of them uses operations on dynamic data along with computation. This will force user to make copy of the user data on the cloud which will prevent the data loss and updation of the data. The efficient distributed storage auditing mechanism is prepare to overcome the data loss inside the cloud computing. But copies of duplicate data will lead to the memory overload of the cloud. So this paper presents the method for data partitioning. Data partitioning methods is also used to avoid the duplication of user data. Cloud data integrity get enhanced due to non-redundancy. It helps in enhancement of localization of the errors. It need to cooperate with server to detect the misbehaving user. This paper uses the DES algorithm for encryption of the data. To enhance the performance of the cloud storage remote data integrity checking concept is used. The cloud contains dynamic data and to reduce the time and computational cost data partitioning plays an important role.**

***Index Terms*—Cloud computing, security, domain, data security, partitioning.**

I. INTRODUCTION

Cloud computing is the use of computing resources (hardware and software) that are delivered as a service over an Internet. The cloud computing model definition is, the most widely used one is made by NIST as "Cloud computing is a model for on-demand network access, enabling convenient to a shared use of resources like networks, servers, storage, services and applications which can be rapidly provisioned and released with service provider interaction or minimal management effort. This cloud model promotes availability and is composed of five model in which three are service 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, and Public cloud and Hybrid cloud.

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

Cloud computing is simply defined as the sharing of the computing resources rather than having these resources personally or locally. In the cloud computing user can have access the services platform independent. Now a days different companies such as amazon server and other provides the data storage facilities to the customers.

Storage servers are managed in the distributed manner system like cloud. The data dynamics providing by third party auditing and the remote integrity checking. 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 data storage service is as shown in Fig.2.

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 criteria 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 partitioning algorithm to achieve correctness. Cloud storage integrity checked by comparing Digital signature of data. Before sending the data over the server need to extract digital signature stored at TPA, at time of data retrieval again DS of data extracted and compares with digital signature stored at TPA. If both are same then integrity of data is fine.

Cloud computing get spread wide in the network. It has wide scope now a days. As cloud computing is good resource for data storage but security of that data is the main issue with the cloud computing. To avoid the issue of data security we have proposed a novel method for the data security that is data partitioning. The following figure shows the data partitioning technique in the cloud computing. The cloud 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.

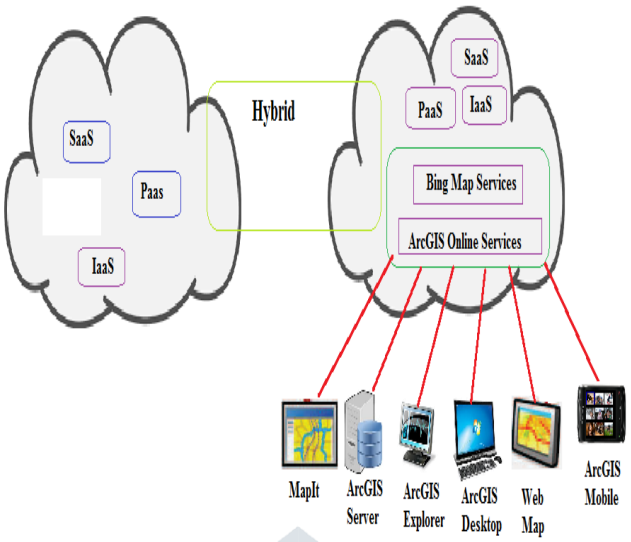

Fig.1. Cloud Computing Architecture

Chiraj p. vala [12] explains about how parametric analysis of the cloud partitioning is done. That is totally depends on the capacity of computation and other parameter. It manly checks that how it check the data partitioning by using the partitioning algorithm. No of data partitioning algorithms have been proposed by different authors. Computing provide infrastructure as a service platform for the data storage.

The remaining paper is organized in different sections such as proposed system literature survey, comparison of different methods and conclusion and acknowledgment and final section consist of references.

Fig.1. Cloud computing security and storage

II. LITERATURE SURVEY

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] concepts of Integrity checking 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 operation such as dynamic data method is used to perform various operations [2]. 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. Is also multiple auditing tasks can be supported by Storage model 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] explains remote data integrity with irretrievability. Error correction and data integrity checking is used to detect the availability of data in cloud. In existing system stated by the S.V Khedka and A D Gavande Data accessed from cloud service enables the services in secured manner. It uses MD5 which 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. Kisung Lee, Ling Liu, gives Customize data partitioning for distributed big RDF data processing. This uses scalable data partitioning (SPA) algorithm along with

big RDF. This is having two sides. First, a suite of vertex centric data partitioning building blocks to allow efficient and second, yet customizable partitioning of large heterogeneous RDF graph data. It consist of two different types of processing: intra-VM processing and inter-VM processing. By intra-VM processing, we mean that a query Q can be fully executed in parallel on each VM by locally searching the sub graphs matching the triple patterns of Q, without any coordination from one VM to another. The coordinator simply sends Q to all worker nodes (VMs), without using Hadoop, and then merges the partial results received from all VMs to generate the final results of Q.
Data availability and data error recovery mechanisms are not given much importance. In cloud storage services remote data integrity checking has been studied in different papers by different authors.

III. PROBLEM STATEMENT

1. *Data Partition And Domain Integrity Design Goals:*
   To increase the data security over the cloud need to store the data on different server by dividing the data into parts. Then the stored data is encrypted by using the DES algorithm.
2. *Design of PDDS Model:*
   PDDS model architecture consist of the Data storage cloud, File sender and the encryption and decryption of the data on the cloud.

IV. PROPOSED SYSTEM

Proposed system consist of the three main concepts one of which is the data partitioning and second is the data security of the data which is to be stored on the cloud server. For the data security we have used the data partitioning and domain integrity check algorithm and for the data security we have used DES data security algorithm. Following figure consist of the entire architecture of the proposed system.

A. Data partitioning and Domain integrity checking:

Data partitioning plays main role in the data plays important role in the data dividing in the number of parts and make easy to retrieve the data from the cloud storage. The data partitioning and domain checking algorithm consist of the use, third party auditor and cloud storage elements in its architecture. The figure 4 shows the working of the data partitioning and domain integrity checking.

Data Access: If user wants to upload the new file on the cloud then he needs to send this file to third party auditor will decide the how many block have to be done of the uploaded file according to the value of S file is split into blocks. This blocks are then encrypted by using DES algorithm and store on the cloud server.

Data Security: Data security is achieved by using the data encryption algorithm DES. DES is the one of the best algorithm to provide the security to the data. The detailed working of the data encryption standard algorithm is explained in the next section.

Cloud Storage: Cloud storage is the third party where user have to store his data. As explained in the section one cloud computing uses the pay as per use method for provide the infrastructure to the user data. The user have to select the cloud and need to pay the charges as per he use the size of the cloud. When file is needed to the user he/she can downloads the file from the cloud storage and after making the changes in the file again split the file into number of blocks and again upload on the cloud server. If user want to upload the new file on the cloud server he need to split the file and then encrypt the file and upload the encrypted file on the cloud server.

B. DES security algorithm:

Data Encryption standard algorithm is used to provide the data security over the cloud. The figure 4 shows the working of the DES algorithm.

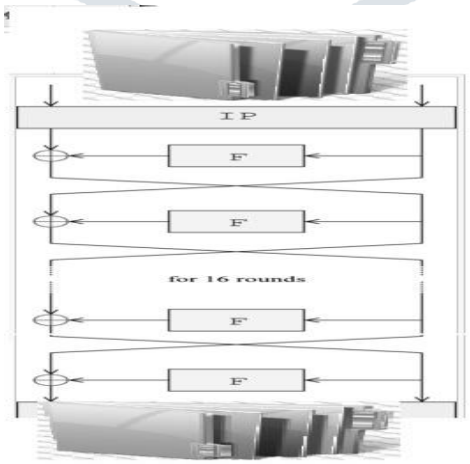

Fig.1. DES Algorithm Working

Algorithm Steps:

For the encryption purpose load the file and its size to decide the number of block. For the partition if size is greater than s then divide the file into n number of blocks. Encrypt the all files and store the file on the cloud. And finally decrypt the file for the use it.

The calculated key is used for the data encryption and data decryption. We have used data encryption technique data encryption standard in the proposed paper.

The following figure shows the architecture of the proposed system which comprises of cloud server and user and third party authority to check the data and decide the in how many numbers of block need to create depends on the size of that data to be uploaded. If the file is already present on the cloud storage user need to download that file for the use and after updating again need to upload the same file on the cloud server. The file access system is very easy user need the security key to access the data and need to decrypt the data before use.

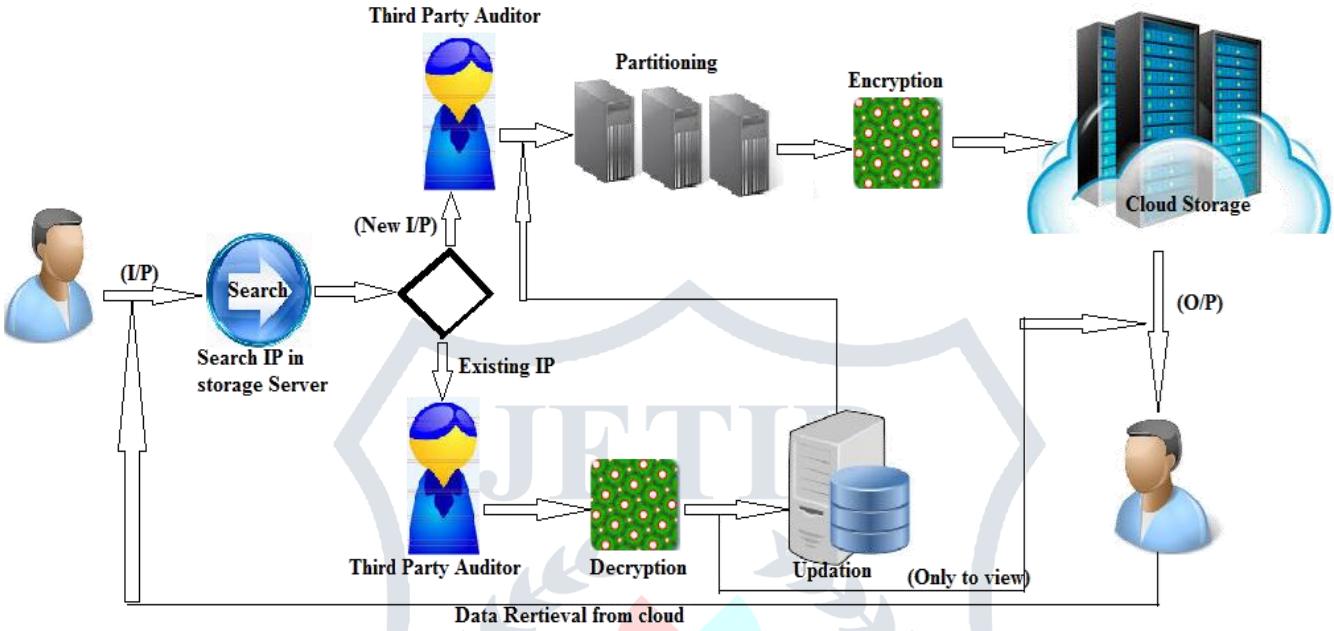

Fig.3. Framework of the proposed system

V. COMPARISON OF DIFFERENT METHODS

In this section we will compare the different data partition methods and our proposed method. As seen in the literature survey lot of research have been studied on the data partitioning on the cloud storage. There are different methods for the data partitioning but in this paper we have used Data partition and Domain integrity checking algorithm for making the partition of the user data. For the security purpose there are number of algorithms are there such as AES, RSA, MD5, data encryption standard etc. But in this paper we have used DES algorithm for the data security to provide the security to the data present on the cloud storage. The efficiency of the DES security algorithm is more as compare to the other security algorithm. The result and analysis shows the reduced time required to store the data and provide the security to the user data.

VI. CONCLUSION

In this paper we propose a model which provide an security to an efficient data storage in cloud service.Data can be stored in easy and efficient manner due to the partitioning of data. And also stored data can be secure due to the use of DES security algorithm.Due to that it gives flexibile access and data will be stored in less cost.So that the space and time are also effectively reduced during storage.Encoding and decoding secures data by dynamic operation, when storage into cloud. Also the remote data integrity checking detects the threats and misbehaving server while storing the data in cloud ensuring data security. In future we have planned searching mechanisms for outsourced computations in cloud services.

VII. ACKNOWLEDGMENT

We are highly indebted to (Name of your Organization Guide) for their guidance and constant supervision as well as for providing necessary information regarding the project & also for their support in completing the project. We would like to express my gratitude towards my parents & member of (Organization Name) for their kind co-operation and encouragement which help me in completion of this project. We would like to express our special gratitude and thanks to industry persons for giving me such attention and time. Our thanks and appreciations also go to our colleague in developing the project and people who have willingly helped us out with their abilities.

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] 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..

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

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

[8] 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.

[9] 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.

[10] B. Hendrickson and R. Leland, "A multilevel algorithm for partitioning graphs," in Supercomputing, 1995.

[11] 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..