Data Partitioning and Recovery using Cloud

Prof. Priyanka Kedar[1] Kavita Bhor[2] Sonali Kamble[3] Renuka Khatal[4] Varsha Gore[5]
[1,2,3,4,5]Department of Computer Engineering
[1,2,3,4,5]DPCOE, Wagholi, Pune 412 217

Abstract— Cloud storage able to remotely store and recover their data and use data when we want in efficient manner and client can work with the data without any difficulties of resources. In existing system, using dynamic data operation the data can be stored in cloud which makes user to make copy for verification and updation of data loss. In proposed system, partitioning method is used for avoid loss of data during the storing data in cloud. For the data recovery we use seed-block algorithm in proposed system due to this we can avoid the loss of data during the storage. Goal of this work is storing data in cloud with confidentiality, integrity, availability, privacy issues and avoiding attacks also. Hence during the storage of data the space, cost is reduced and also it takes less time.

Key words: Cloud Storage, Integrity, Confidentiality, Partitioning, Availability

I. INTRODUCTION

Cloud computing is totally depends on internet which is widely used for enhancing performance. User can retrieve the information which is stored in the cloud from anywhere at any time. Resources are delivered to the user over the internet to provide the service. Cloud storage technique provides easy access and storage of data in effective manner. To store data in a cloud we use different network services. Managing and controlling of cloud resources is done by cloud service provider. Cloud storage comprises three service models are, software as a service (Saas), cloud platform as a service (Pass), and cloud infrastructure as a service (Iaas). Depends on priority of data can be stored in public cloud, private cloud, hybrid cloud [9].

Public cloud: information stored in a public cloud can be used by any user over the internet.

Private cloud: private cloud is promoted by particular group or organization. Data stored in private cloud is accessed by that group or organization only.

Hybrid cloud: it is a combination of two or more clouds; including clouds are public, private etc.

In cloud data storage we use concept are third party auditing and remote integrity checking .third party auditor is mediator between the user and cloud server.

Data decomposition and misbehaving server in cloud storage is detected by remote data integrity checking [5]. When user wants to accessed data from cloud server third party auditor will provide authentication to the user .data storage is done by partitioning algorithm. Data can be stored using partitioning method and retrieved using merging technique.

II. SYSTEM ARCHITECTURE

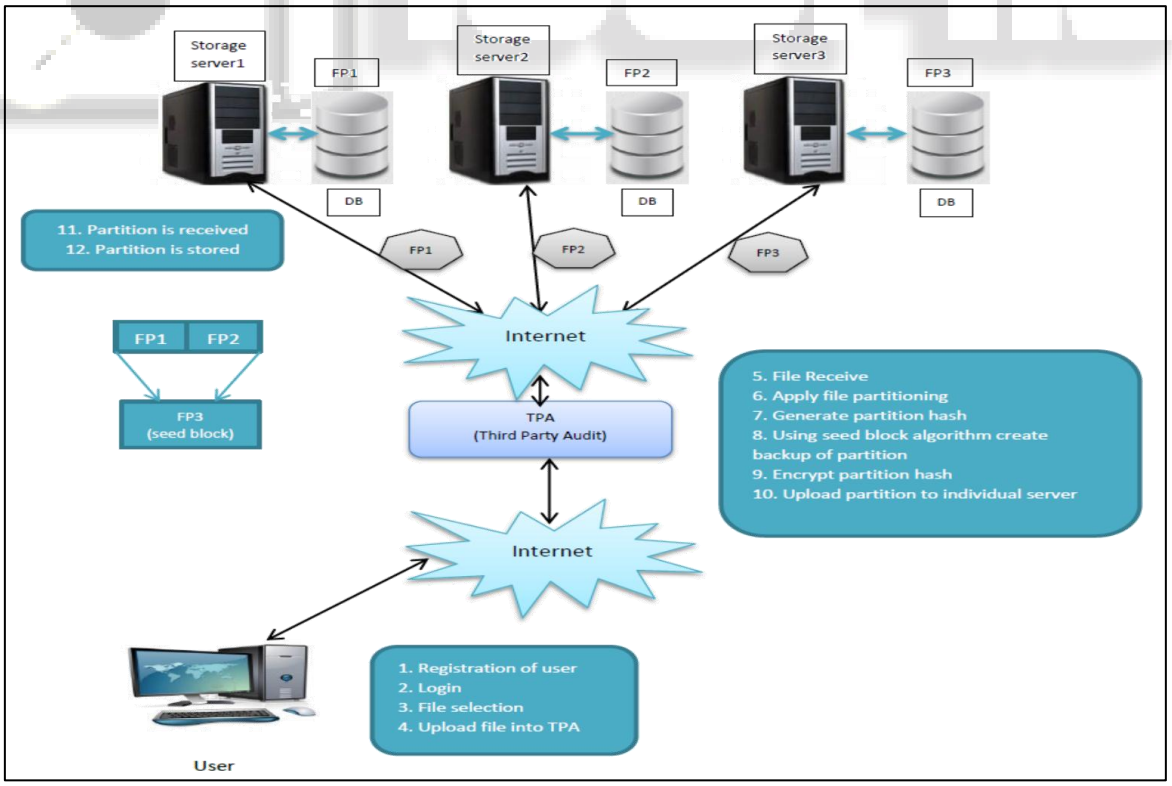

Fig. 1: System Architecture

File partition done at third party auditor. User will send file to the TPA over the network then authentication is provided to the user. TPA receive file then TPA performs partition on that file after that extract digital signature of

each file partition then generate secrete key of each partition.

TPA encrypt each partition using respective secrete key and stores partition sequence, signature, keys and file attributes on its own server.

TPA send partition to the storage server and server will receive the partition and store the partition, when user wants data from the data storage hash code of data is matched with TPA hash code if hash code matches then server will send the data to the user.

III. ALGORITHMS

A. *Encryption:*

Encryption is the conversation of data into a form called a cipher text that can't be easily understood by unauthorized people. In technical term process of encoding plain text into cipher text message is called as "Encryption."

B. *Decryption:*

Decryption is the process of converting encrypted data back into its original form. So it can be understood.

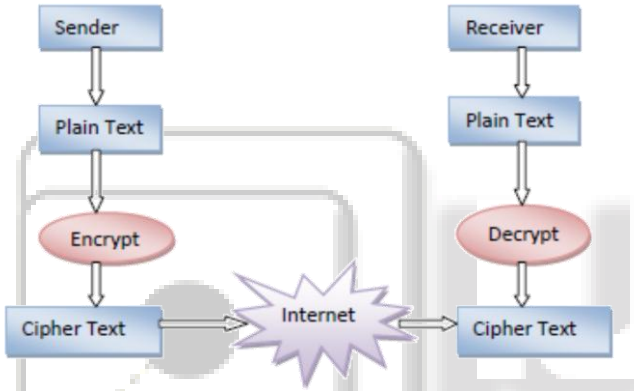

Fig. 2: Encryption and Decryption

C. *Partitioning and Merging Files:*

(1) Upload the file
(2) Calculate file size
(3) partitioning file check file size is minimum show error message or if maximum then show error message else, split file into n partitions
(4) Generate hash code of each partition
(5) Extract secrete key for each partition
(6) Encrypt file partition and generate respective secrete key
(7) Store partition sequence, Hash code, Secrete key at TPA
(8) Send each partition to the server
(9) Merging File:TPA sends request to the server for getting file partition
(10) Generate new Digital Signature and compare it with Digital Signature stored at TPA

Then check new Digital Signature are matched with Digital Signature which stored at TPA

(11) Merge file
(12) Decrypt the merge file with key.

IV. EXISTING SYSTEM

In the existing system, data is stored dynamically, which prepares the user to make copy for additional updation and verification of the data-loss through the encryption technique security can be provided to encode the data misbehaving server is detected by remote data integrity checking.

Data partitioning can be done vertically and horizontally. In partitioning method they split data into small parts. In the existing system data availability and data recovery technique have not more importance. There are many challenging issues in remote data integrity checking in the existing system.

From the survey of existing system we have the copy of data in the system and risk of losing data. This limitation is overcome with proposed system and also provides more security.

Existing system having disadvantages like it take more time, space and cost. To perform operation on data such as encryption and decryption while storing the data in cloud. The previous system do not create backup of data due to this data will be loss. When system falls due to some reasons data can be loss because in previous system we don't have backup so user can't access his data.

V. PROPOSED SYSTEM

Partitioning method is proposed to avoid copy of data at the client side by using partitioning method by this performance can be increases.

In the proposed work it has capability of flexible storage to make sure the availability of data and correctness of data in server by partitioning method. We can make the partitions vertically and horizontally. To prevent data loss from unauthorized person we use difference security technique like secure hash function, encryption, decryption, etc.

Digital signature of data can be matched while storing in the server. Before sending data to the server we can extract hash code of that data and stored at TPA when we want to recover data again hash code of data extracted and match with hash code stored at TPA. If both hash codes are same then integrity of data not opposed.

VI. CONCLUSION

In this work by using partitioning algorithm we can store data in easy and effective manner. it reduces space and time during storage. Encryption and Decryption process provide security to the data when storing into cloud. The future work is planned to feed higher level of security.

REFERENCES

[1] Ms. Kruti Sharma, Prof K. R. Singh, 2012, "Online data Backup And Disaster Recovery techniques in cloud computing: A review", IJEIT, Vol.2, Issue 5.
[2] EleniPalkopoulouy, Dominic A. Schupke, Thomas Bauscherty, 2011, "Recovery Time Analysis for the Shared Backup Router Resources (SBRR) Architecture", IEEE ICC.
[3] C. Wang, Q. Wang, K. Ren, and W. Lou, "Privacy-Preserving Public Auditing for Storage Security in Cloud Computing," Proc. IEEE INFOCOM, Mar. 2010.
[4] Yoichiro Ueno, NoriharuMiyaho, Shuichi Suzuki, MuzaiGakuendai, Inzai-shi, Chiba, Kazuo

Ichihara, 2010, "Performance Evaluation of a Disaster Recovery System and Practical Network System Applications," Fifth International Conference on Systems and Networks Communications, pp 256-259.

[5] BhavnaMakhija, VinitKumargupta, Indrajit Rajput ,"Enhanced Data Security in Cloud Computing with Third Party Auditor", HasmukhGoswami College of Engineering, Vahelal, Gujarat, International Journal of Advanced Research in Computer Science and Software Engineering

[6] Vijaykumar Javaraiah Brocade Advanced Networks and Telecommunication Systems (ANTS), 2011, "Backup for Cloud and Disaster Recovery for Consumers and SMBs," IEEE 5th International Conference, 2011.

[7] 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.

[8] Lili Sun, Jianwei An, Yang Yang, Ming Zeng, 2011, "Recovery Strategies for Service Composition in Dynamic Network," International Conference on Cloud and Service Computing.

[9] 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.

[10] Y.Ueno, N.Miyaho, and S.Suzuki, , 2009, "Disaster Recovery Mechanism using Widely Distributed Networking and Secure Metadata Handling Technology", Proceedings of the 4th edition of the UPGRADE-CN workshop, pp. 45-48.

[11] 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.

