Consistency and Privacy based Replication System in Cloud Sharing Framework

S. Sindhuja*, K. Suriya Prakash
Assistant Professor,*
Dept. of IT,
A.V. C College of Engineering
Mannampanthal, Mayiladuthurai
IV year – IT, Dept. of IT,
A.V. C College of Engineering,
Mannampanthal, Mayiladuthurai.
Davidsurya054@gmail.com
Sindhusm77@gmail.com

Abstract— **The main objective of this paper is Division and Replication of Data in the Cloud for Optimal Performance and Security (DROPS) that collectively approaches the security and performance issues. Firstly, the data owners are registered into the cloud for using the cloud region and provide the secret key to trustee parties. The data files are uploaded into the cloud region for access the genuine users. Then the stored records are fragmented based on the data size, fragmented data are called data chunks. Fragments are placed in various providers using T-Coloring method. In T-coloring algorithm was implemented to measure the distance of each data, where the records are placed in cloud system. This is used for region assignment assigns region to the nodes, such that the channels are separated by a distance to avoid obstruction. The genuine users can access the data from cloud sector through cloud providers. The genuine users have secret key defined in the cipher text can retrieve the entire data content. It aims to allow the users with eligible key to decrypt the entire data stored in the cloud server and it cannot limit the data access control to the authorized users. Difficult to hack the files from cloud storage because fragmentation and replication placement approach. Heuristic auditing strategy (HAS) techniques used to the chunk the given data source. Data replication was performed to maintain the multiple copies of same data on same server or on different servers**.

Keywords: **Data chunks, Data replication, T-Coloring Algorithm, Heuristic Auditing Strategy (HAS*).***

I. INTRODUCTION

Cloud security follows traditional cryptography approach includes encryption and decryption. Cryptography includes symmetric and asymmetric approaches User based access control mechanism can be used at the time of data access by users. Cloud computing service providers require a system which can handle a large number of requests at a time.

For processing the huge cloud of requests for data access, services need to be highly available [1]. System keeps multiple copies of the blocks of data on different nodes by replication. A large number of replication strategies for management of replicas have been implemented in traditional system. As a result of replication, data replicas are stored on different data nodes for high reliability and availability [2]. Replication factor for each data block and replica placement sites need to be decided at first. In existing framework data can be lost so in this paper propose improved DROPS framework that includes heuristic auditing strategy to protect the data from loss [4].

It present efficient consistency as a service model, where a group of data owners that constitute service provider can verify whether the data cloud update the data or not and design user operation table to change status of fragmented files with different metrics [1][2][3]. Difficult to hack the files from cloud storage because fragmentation and replication placement approach. Improved scalability to store large data files. Proposed reduce response time for retrieving data from cloud [5].

II. LITERATURE SURVEY

In [1], Equal Cost Multi-Path (ECMP) was implemented in this paper. The main problem was analyzed in under various failure scenarios. Most of the metrics only consider the largest connected component for robustness evaluation.

In [2], Similarity hash table (SHT) was implemented in this paper. The main disadvantage of the paper was the replication data in store the cloud. Data replication approach for joint optimization of energy consumption and bandwidth capacity of data centers.

In [3], DCN topologies were implemented in this paper but the main negative aspect is the metrics only consider the largest connected component for robustness evaluation. Fat Tree is much higher than the Three Tier architecture, the number of failed nodes is around five times in the Fat Tree as compared to the Three Tier architecture.

In [4] Merkel Hash Tree (MHT) was used in this paper but the main inconvenience is the replication data in store the cloud. Data replication approach for joint optimization of energy consumption and bandwidth capacity of data centers.

In [5], Ceph production-grade was implemented, the major disadvantage is a public cloud provides a shared software repository that different groups of developers can fork into separate branches. Data replication approach for joint optimization of energy consumption and bandwidth capacity of data centers.

III. Proposed System

In this paper proposed to Division and Replication of Data in the Cloud for Optimal Performance and Security (DROPS) that collectively approaches the security and performance issues in following fig.1. Fig. 2 shows the use case system for proposed work.

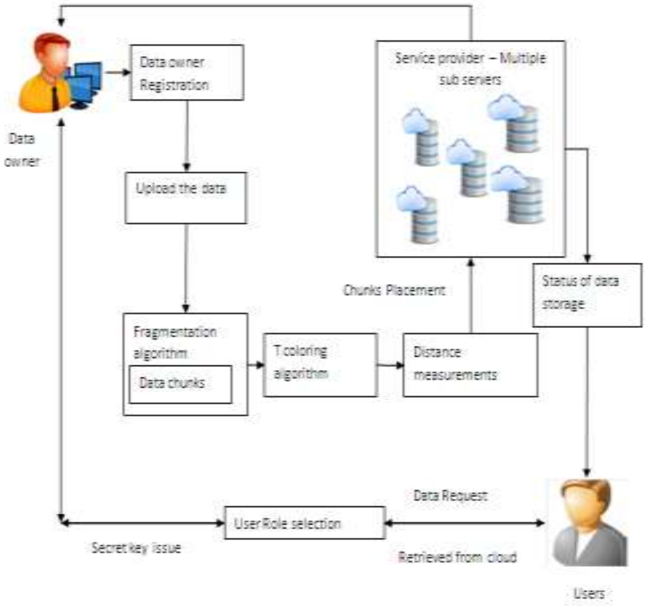

Fig.1 show overall proposed system architecture.

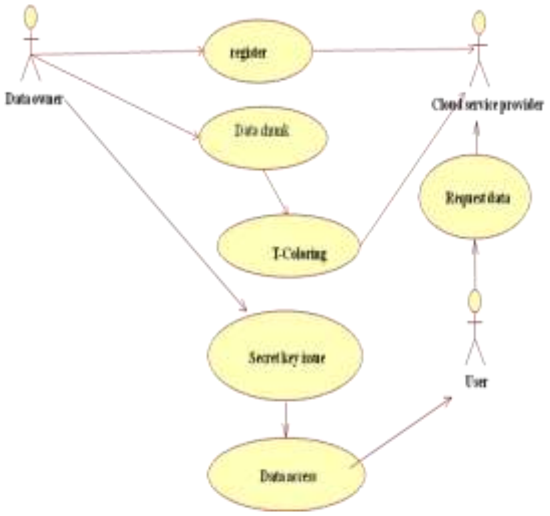

Fig. 2Use Case for proposed system

A. Cloud Framework

In this module, cloud data storage service. Cloud computing is demand on shared computing resources Three different entities such as the cloud user, who has large amount of data files to be stored in the cloud Define abbreviations and acronyms the first time they are used in the text, even after they have been defined in the abstract. Abbreviations such as IEEE, SI, MKS, CGS, sc, dc, and rms do not have to be defined. Do not use abbreviations in the title or heads unless they are unavoidable.

The cloud server, which is managed by the cloud service provider to provide data storage service and has significant storage space and computation resources. The third-party auditor, who has expertise and capabilities that cloud users do not have and is trusted to assess the cloud storage service reliability on behalf of the user upon request.

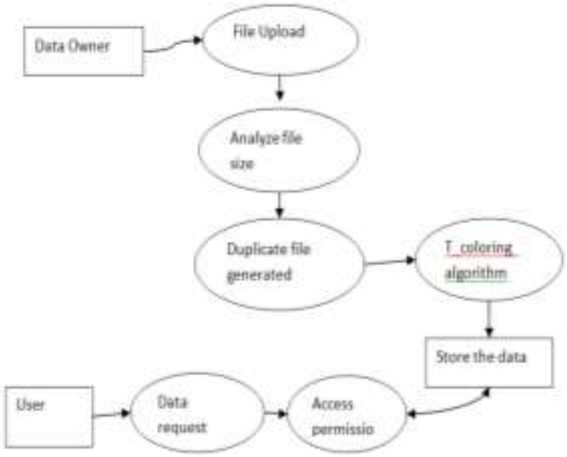

Fig. 3 Flow of cloud frame work

Fig. 4 Registration to cloud server

Fig. 5 cloud provider page

Fig. 6 Data owner details page

B. Data chunking

In this module all data records are split into data chunks. Data owner upload the files to cloud system. Chunk contains a header which indicates some parameters e.g. the type of chunk, comments, size etc. Chunks may also be fragments of information which are downloaded or managed by distributed programs. These files are fragmented based on size. Fragmented data is placed in following module.

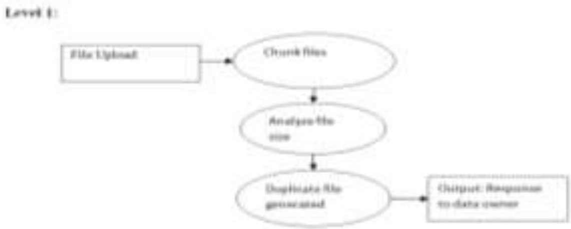

Fig. 6 flow of data chunks

Fig. 8 User entry page

Fig. 9 Upload data file

Fig.10 Store the data files

C. T-Coloring method

The fragments are placed in various providers using T-Coloring method. This is used for channel assignment assigns channels to the nodes, such that the channels are separated by a distance to avoid interference. This is used for channel assignment assigns channels to the nodes, such that the channels are separated by a distance to avoid interference In such a case, only for the remaining fragments, the nodes that are not holding any fragment are selected for storage randomly. These modules using the distance calculate.

D. Data access

In this module, user accesses the data from cloud through providers. The users those who are having matching secret key defined in the cipher text can retrieve the entire data content.
It aims to allow the users with eligible key to decrypt the entire data stored in the cloud server. These cannot limit the users from accessing the data's which are not accessible to them. That is it cannot limit the data access control to the authorized users

Level 2:

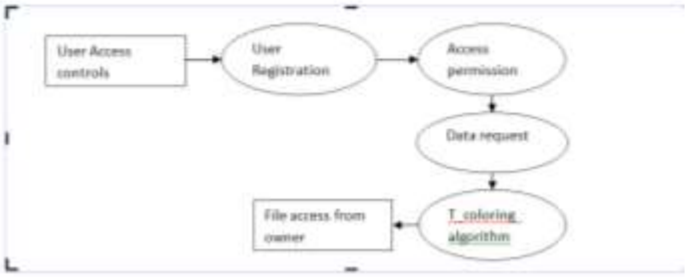

Fig. 11 Flow of Data access

E. Security performance

The performance of the system using the performance metrics such as storage overhead, communication cost and computation efficiency. The storage overhead is one of the most significant issues of the access control scheme in cloud storage systems. In our scheme, besides the storage of attributes, each sub server also needs to store a public key and a secret key for each user in the system.

Thus, the storage overhead on each server in our scheme is also linear to the number of in the system. The communication cost of the normal access control is almost the same. The communication cost of attribute revocation is linear to the number of cipher texts which contain the fragments. The computation efficiency of both encryption and decryption in two criteria: the number of sub server and the number of fragments per server.

IV. RESULTS AND DISUSSIONS

In this paper, we have implemented the main objective of this paper is division and replication of data in the Cloud for Optimal Performance and Security (DROPS) that collectively approaches the security and performance issues. In before methodologies key values will be applicable to access the data values. But in those technologies there is a drawback is that third party actor may be un trustable person some time so that we were not applied that concept in this work. Instead of those methods we fragmented the given input data and provide the duplication with same name and stored to different server in cloud region. By this concept data will be secured.

V. CONCLUSIONS

The system monitors consistency service model as well as level of data upload which helps the user to get the data in updated version. User can understand various sub servers in cloud service provider. It is a strategic to provided automatic update mechanism to identify fragments easily and provide the data to users after updating only.

REFERENCE

[1] D. Zissis D.Lekkars, “Addressing Cloud Computing Security Considerations,” 2013.

[2] Dejene Boru,”Energy-efficient data replication in cloud computing datacenters”., Received: 18 March 2014 / Revised: 4 July 2014 / Accepted: 24 September 2014© Springer Science+Business Media New York 2015
Y Tang, PPC Lee, “FADE: Secure Overlay Cloud Storage with File Assured Deletion,” in Magnetism, vol. III, G.T. Rado and H. Suhl, Eds. New York: Academic, 2010, pp. 271-350.

[3] K. Bilal, M. Manzano, S. U. Khan, E. Calle, K. Li, and A.Zomaya, “On the characterization of the structural robustnessof data center networks,” IEEE Transactions on Cloud Computing,Vol. 1, No. 1, 2013, pp. 64-77.

[4] D. Sun, G. Chang, L. Sun, and X. Wang, “Surveying and analyzing security, privacy and trust issues in cloud computing environments,” Procedia Engineering, Vol. 15, 2011, pp. 2852 2856.