A SECURED DATA TRANSFORMATION AND VALIDATION PROBING IN MULTI CLOUD ENVIRONMENT

Jaya prakash Koyyalmudi [1], J Armsrong Paulson [2]

[1]Pursuing M.tech (CS) , [2]Assistant professor,
Nalanda Institute of Engineering & Technology, Siddharta Nagar,
Kantepudi (v), Sattenapalli, Guntur, Andhra Pradesh, India – 522483

ABSTRACT

In recent years, cloud storage service has become a faster profit growth point by providing a comparably low price, scalable, location independent platform for clients' data. Because cloud computing environment is constructed based on open architectures and interfaces it has the ability to incorporate multiple internal and/or external cloud services together to provide high interoperability. In multiple cloud servers there is a necessity **f***or maintain availability, scalability, and durability to the customer's data which leads to be replicated on multiple cloud servers. When cloud service provider stored more data copies then the more fees the customers are charged. To increase the security in cloud server and to maintain the data in secure form we are providing here a secured privacy based data sharing process in cloud servers. When user store his data will store directly in cloud servers for that user may face some of the problems in some times he may lost the data in server to avoid that all the things here we proposed the multi sharing copy concept over the cloud servers when user stores his files information in cloud server. And here in this when the third party user stores the data in cloud servers it will divided into multiple copies and that will store after the storing it will be decrypted by the cloud user and he can change the modification in server that will effect in the stored data then user can know that whenever he modify after at finally user can download the file. In this paper, we propose a provable multi copy data possession (PMDP) scheme, which provides evidence to the customers that all outsourced copies are actually stored and remain intact. Moreover, it allows authorized users (i.e., those who have the right to access the owner's file) to seamlessly access the file copies of data stored by the CSP and it supports public verifiability and also the proposed scheme is proved to be secure against colluding servers. In the proposed scheme the verification time is practically independent of the number of file copies.*

Keywords: ***Data Storage, Multiple Data Copies, Integrity, Provable Data Possession, Cloud Server Provider.***

I INTRODUCTION

Cloud storage service has turn into a faster earnings growth point by providing a comparably low price, scalable, location independent platform for clients' data or information. As cloud computing environment is constructed based on unfasten architectures and interface, it has the potential to include multiple domestic and/or peripheral

cloud services mutually to provide high interoperability. It was called as a distributed cloud environment as a multi Cloud or hybrid cloud. A multi cloud allows clients to easily access his/her resources remotely through interfaces such as Web services. We have some existing tools and technologies for multi cloud like Platform VM Orchestrator, VMware v Sphere, and Ovirt to help cloud providers construct a distributed cloud storage platform (DCSP) for managing clients' data. Still, if such an important platform is weak to security attacks and it would bring irretrievable losses to the clients.

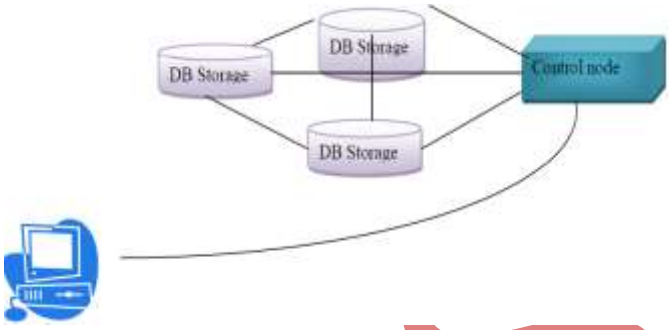

Fig 1 Architecture of a cloud storage system including control severs and control storage servers

In this paper we are propose a way of outsourcing information in cloud servers and that to stored by the admin who providing the space to the data owner. In general whenever user wants to store his data in cloud servers he has to check the availability of data and store his information on cloud server and in some of the times data may pass or may not pass to the data in some of the data miss caring transactions. When the data has stored in cloud server or an out sourcing data base that data will become automatically an untrusted data. So we may not say it's in secure zone or not so the data owner can lose his control on his sensitive data. This lack of knowledge gets the some distractions and formidable things in the time of data processing and to make that in secure manner. This all should work on cloud based on the priority mode only in the server and that data will still passing the information of storing the data in to the cloud servers. We can focus many researches here on the server side consequential of data transferring information and in its storing process of data transaction. And through that we are proposed some of new auditing concepts for the data transaction of implantation process in cloud out sourcing data engines.

II ARCHITECTURE DESCRIPTION

We are using the PDP (provable of data possessions) technique for the validation of data in remote servers and through this we can get the some data from the server like Meta data. All the researches has proposed the things of remote area network of data transaction and it has to pass the different types of cryptographic dimensional assumptions. In general when we check only the data owner will check the data is it available or any modification but here in this process we are giving an auditing permission to the third party person to store the data in cloud servers that with the multiple copies of data modification and t split in different servers at a time. For the pubic users or third party users verification there must be a key required to verify the data and to modify it and place in to server after it has been placed in server we have to check that is it available or not and the data was valid in remote server or not. Mainly our contribution is summarize data transaction and to store it in

secure manner. Here in this we are proposed a pair based data transaction of implementation this will provides and exact and unique of identity to the data and its accurate availability in process and it will gives the guarantee to the user for the protection of the process in cloud server pointer that is CSP. That all the copies of data has to be store in the cloud server and it will provide the whole thing to the user and the performance check of data in cloud servers and these copies of data are intact. So only the authorised person or data valid owner can only check or access the data in the cloud servers and the PDP technique will support the public verification.

Fig 2 Architecture Description of PDP

Here in this paper we justify that the efficiency of PDP technique and through this we are analysing the concept of implementation and the process of transaction implementation to modify the user data to get an expected results from the server for the modification of the data and here we are discussed about the corrupted data and the valid data in the server through this we can know that our data is it in secure place or not and it will give the re-conformation about the things and the reliability of the server transaction and its manipulation things will work for the data transforming of files.

In this paper we are considered the CSP is the most economically it's may not be a use full storage for the process of data transformation and its implementation of things. But it's used to store in less amount of data storage than the required amount of data needed and by the contacts of the server and its usage of storage we can delete the files and its related data. In cloud computing model we are find three types of modules here for the transaction of the data usage and its maintenance in the server. We can see that all three types of process here in the above diagram and that who can maintain the data we can take an example of an health data application it's a government organization application. It will be considered as a data owner part of the accessing of each and every patients details and all his medical bills we are storing the cloud server. Here in this we have to focus on the sensitive data transaction of the data warehousing of each and every data and its essentially to apply the storage purpose data and maintain in the library data storage information of all the medical and scientific, all the legal values of data has to be tore in the server and for the information of interface checkups and its transaction process workings. The integrity of all the customers data in cloud servers and all the risky data due to it has to be instruct and it has to store by the reasons whenever the user or data owner in the cloud server pointer who wants to make the profit and the to pass the things. And it has to maintain the data it has t be store in the server side as well as it has to hide the information of the data owner and all his personal information which his data has to be a sensitive data in all this content of cloud stored data.

III RELATED WORK

Security in cloud is indispensible. For checking the accessibility and integrity of outsourced data in cloud storages, researchers have suggested two basic approaches called Provable Data Possession (PDP) and Proofs of Retrievability (POR).

Ateniese et al. first proposed the PDP model for ensuring control over the files on untrusted storages without retrieving it. Client maintains constant amount of metadata to verify proof. This PDP approach has also provided an RSA based scheme for a static case that achieves the 0 communication cost. They also suggested a publicly verifiable version, which allows client (data owner) as well as anyone other than owner, to challenge the server for data possession. This property has made immense impact on application areas of PDP protocol due to the separation of data owners and the users. However, these strategies are insecure against replay attacks in dynamic scenarios. Moreover, they do not fit for multi-cloud storage due to the loss of homomorphism property in the verification process. And also he developed a dynamic PDP solution called Scalable PDP. This highly efficient and provably secure PDP technique is based entirely on symmetric key cryptography without requiring any bulk encryption. This PDP technique allows outsourcing of dynamic data. This supports operations, such as deletion, block modification and append, However, since it is based upon symmetric key cryptography, it is unsuitable for public (third-party) verification. Also, servers can deceive the owners by using previous metadata or responses due to the lack of randomness in the challenges. The numbers of challenges and updates are limited and fixed in advance and users cannot perform block insertions anywhere.

Erway et al. proposed two Dynamic PDP schemes with a hash function tree to realize (log *n*) communication and computational costs for a *n*-block file. The basic scheme, called DPDP-I, keeps the drawback of Scalable PDP, and in the 'block less' scheme, called DPDPII, the data blocks can be leaked by the response of a challenge, .However, these schemes are also not effective for a multi cloud environment because the verification path of the challenge block cannot be stored completely in a cloud.

Juels and Kaliski presented a POR scheme, which depends largely on preprocessing steps that the client conducts before sending a file to a CSP. Unfortunately, these actions prevent any efficient extension for updating data.

Shacham and Waters introduced an improved version of this protocol called Compact POR. This protocol uses homomorphic property to aggregate a proof into (1) authenticator value and (*t*) computation cost for *t* challenge blocks, but their solution could not prevent the leakage of data blocks in the verification process because of its static nature.

Wang et al. presented a dynamic scheme with (log *n*) cost by integrating the Compact POR scheme and Merkle Hash Tree (MHT) into the DPDP. Several POR schemes and models have been recently proposed including.

Bowers *et al.* introduced a distributed cryptographic system that allows a set of servers to solve the PDP problem. This structure is based on an integrity-protected error correcting code (IP-ECC), which upgrades the security and efficiency of existing tools. However, a file must be transformed into distinct segments with the same length, which are distributed across servers. Therefore, this system is more suitable for RAID rather than cloud storage.

IV PROPOSED WORK

In this paper we propose a way of security and an auditing permission to the third party user and the cloud serve provider but in the existing system we know that whenever the user wants to store his data in cloud server he has to keep directly without the interaction of the third party user and anyone help. So here in this paper to overcome that and to maintain the data in safe manner we are proposed a new way of auditing the data. In existing system if user had stored directly to the server or else in some of the times server may fails when user storing his data or incase of any error detection and its server low or high of burden it may interrupt when user uploading his data in cloud servers. So to avoid that and to concentrate on the third party user we are implemented this paper. And this person has t receive the files or the data from the user and here in this paper his task is the main task on the work of this project and he has audit share the data to the cloud servers in to a different copy of tracks of information in cloud server and here this a best option to the user and to this application also through TPA auditing storing the data is good and if the data was not stored directly it may not be good for the user and un secure (Fig 3).

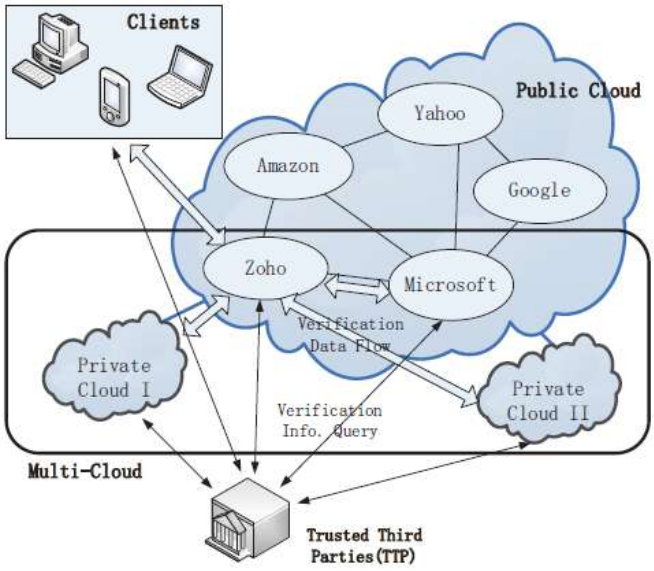

Fig 3 System Architecture for verification

We are assumed that make our data in secure to store in our space in cloud servers and the out sourced data has been to integrate the users calculation and with its weighted information. Here in existing system we are keeping all the data in one place and we are storing in any some other areas but here in this we are keeping all our data in to number of locations of cloud server points and when ever user wants to receive or he want to get that data he has to access from the servers and he will get if incase of any server fails from the remaining he will get the information without any breaking in cloud servers.

Here are implementing the way of protecting data in cloud server even if it was lost by the cloud collapsing we are making that data in perfect and we are using a simplified comparison algorithm for the protection of data in cloud server through this we can get the data backup even in some of the times if we lost data. In general whenever the data in cloud server has lost or the cloud server has collapsed then that we cont get back the data

from the cloud server points so that is the main drawback of the existing system but here in this application we are implemented to protect all the data and providing an integrity verification rules in cloud servers and that we are implemented a way of protection of server.

V PERFORMANCE COOPERATIVE PROVABLE DATA POSSESSION

To increase the security in cloud server and to maintain the data in secure form we are providing here a secured privacy based data sharing process in cloud servers. When user store his data will store directly in cloud servers for that user may face some of the problems in some times he may lost the data in server to avoid that all the things here we proposed the multi sharing copy concept over the cloud servers when user stores his files information in cloud server. And here in this when the third party user stores the data in cloud servers it will divided into multiple copies and that will store after the storing it will be decrypted by the cloud user and he can change the modification in server that will effect in the stored data then user can know that whenever he modify after at finally user can download the file and here we are following few steps to maintain the data and when we are storing data in cloud server we are not calculating the data how much it should required and how much capacity it will occupied the data cloud servers so maintain all this information and the remaining space what was left after the data stored in server for all this things we are maintain an integrity approach for the application and for the storage of data content in cloud servers. But here in this paper we are maintained everything very clearly for the security purpose and to maintain in safe manner.

After all things and securing operations we are moved forward in this project and we are implemented a three way communication in this page and we are provided security to the user uploaded data with the help of the third party authenticator here in this paper we are provided security of integrity based data sharing mechanisms for the data sharing in the cloud servers because here we are not storing the data in single cloud server but we are storing the data in different servers which doesn't have relation with each other and through this servers only we are providing security to the data owners data and when he is uploaded his data in server that data has been sent successfully to the TPA then he use to share the data based on the content and the availability of its related servers and its configuration based. He is the person mainly auditing the data in the server but yet the permissions had not passed him to change the data or re-modify the user uploaded data. Data owner may not get the accessing permission until it has stored in the cloud server through the data owner and after TPA has shred and after the cloud server owner has checked and done validation of the data only user can get the accessing permission to download or change or to check the data. Whenever he done modifications in his data it will automatically update in the server by the help of the TPA user, Then the user can access the data at any time whenever he access the data it will collect all the information from all the different cloud servers and that will appear to the cloud server then he can access it any time so when he done changes in single copy of data it will reflect in all the servers. That and when the data has checked or updated in the cloud servers that all the related information and where in which server the data has been changed that all the information will update in each and every time to the data owner then in that cases he can check and valid his data, so like this way we are protected the user data in cloud server by using an integrity verification of TPA and transaction of sharing algorithm.

VI PERFORMANCE ANALYSIS

In this paper we are proposed a three way of communication path between the data owner, cloud server that is the third party authenticator. Here in this the TPA is the main user he has to upload all the data in cloud server point. Here in this application data owner will register his details and he will upload his data or the important information that all the data files and his information will be send to the TPA he will audit the files and he have the permission to store in the cloud servers and he only can do.

When after that he will share that data in to number of cloud servers that will be an encryption format that data will store in the clouds that time the TPA will generate an encryption key for the file decryption and that data will send to the data owner through the TPA and the updated information of the file will be send to the data owner as well as. After that we can check that all the data or files data in the cloud servers the cloud server authenticate have the permission to change and to check about the data and the information what was updated by the data owner. Whenever the data has modified in the cloud server that times the user can know that his information in the clouds has been checked or modified in the cloud server then he can simply identify the data whenever someone has checked and any modification was happen in the cloud server data then it should be a protected in the cloud server then data owner can be a free of all the troubles and after the data was updated in cloud server then only the data will appear in the data owner side then he can download the files when he wanted and when he need the data then that time he can check his all information without any distraction and without data lost from the cloud server we get this results in our application.

VII CONCLUSION

The integrity modification theme of this application is storing the data in un-trusted cloud server in a secure manner here in this application TPA is the main user he has to upload all the data in cloud server point. Here in this application data owner will register his details and he will upload his data or the important information that all the data files and his information will be send to the TPA he will audit the files and he have the permission to store in the cloud servers and he only can do. When after that he will share that data in to number of cloud servers that will be an encryption format that data will store in the clouds that time the TPA will generate an encryption key for the file decryption and that data will send to the data owner through the TPA and the updated information of the file will be send to the data owner as well as. Finally we got the exact results from the cloud server with an exact data without modification our data with security.

REFERENCES

[1] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, “Provable data possession at Untrusted stores,” in CCS ’07.

[2] Ayad F. Barsoum, M. Anwar Hasan “Integrity Verification of Multiple Data Copies over Untrusted Cloud Servers”.

[3] Enabling Public Verifiability and Data Dynamics for Storage Security in Cloud Computing Qian Wang1, Cong Wang1, Jin Li1, Kui Ren1, and Wenjing Lou2-Springer-Verlag Berlin Heidelberg- 2009.

[4] Priyanka V.Mogre, Prof.Girish Agarwal, Prof.Pragati Patil " Data Storage and Data Integrity in Multi-Cloud Storage" on International Journal of Advanced Research in Computer Science and Software Engineering.

[5] Cloud security defence to protect cloud computing against HTTP-DoS and XML-DoS attacks, Ashley,YangXiangn, WanleiZhou, AlessioBonti, Elsevier- 2010.

[6] A Multiple-Replica Remote Data Possession Checking Protocol with Public Verifiability- Second International Symposium on Data, Privacy, and E-Commerce- 2010.

AUTHOR PROFILE

Jaya prakash Koyyalmudi is currently pursuing M.Tech in the Department of Computer Science, from Nalanda Institute of Engineering & Technology (NIET), siddharth Nagar, Kantepudi(V), Sattenapalli (M), Guntur (D), Andhra Pradesh , Affiliated to JNTU-KAKINADA.

J Armsrong Paulson working as Associate Professor at Nalanda Institute of Engineering & Technology (NIET), siddharth Nagar, Kantepudi(V), Sattenapalli (M), Guntur (D), Andhra Pradesh , Affiliated to JNTU-KAKINADA.