A Novel Approach for Ensuring Data Integrity and Verification in the Cloud

Lenkala Ganeshreddy¹, Bhaludra Raveendranadh Singh², Moligi Sangeetha³

¹ Lenkala Ganeshreddy, Pursuing M.Tech (CSE) from Visvesvaraya College of Engineering and Technology (VCET), M.P Patelguda, Ibrahimpatnam (M), Ranga Reddy (D)-501510, India
² Bhaludra Raveendranadh Singh is working as Principal from Visvesvaraya College of Engineering and Technology (VCET), M.P Patelguda, Ibrahimpatnam (M), Ranga Reddy (D)-501510, India
³ Moligi Sangeetha is working as Associate professor & HOD (CSE) from Visvesvaraya College of Engineering and Technology (VCET), M.P Patelguda, Ibrahimpatnam (M), Ranga Reddy (D)-501510, India

Abstract: - 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.

Keywords: —data integrity, cryptographic protocols, Outsourcing data storage.

I. INTRODUCTION

In this paper we are proposing a way of outsourcing data 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 un-trusted 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. Here 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 public 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.

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
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 to 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.

II. 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 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.

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 simplifed 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 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.

To increase the security in cloud server and that 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 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.

III. RESULTS

Here 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.

IV. 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.

V. FUTURE ENHANCEMENT

Here in the above content we are discussed about our process and way of maintenance and the data protection and there are many scopes in this project to implement and maintain for the future enhancement on this project we that as we are seen in the integrity comparison process of algorithm how efficiently we store data and how we can protect the data in cloud servers and we are provided all the information which was required for the protection of the data usage and its maintenance. Those as we can improve the effective write and read protocols for data calculation in the cloud server like for
the count of day wise and all the count base of its data capacity and the space allocated in the cloud servers that we have some more in security. And after that we are mentioned above that the security issues. So we are planning to implement and maintain a lock system to the user data or the file by the help of cloud server pointer so we can constantly secure the data from the attacks and lose of data in storage server with the expected levels of integrity factors and to maintain the well performance in cloud servers.

REFERENCES

[1] Towards Secure and Dependable Storage Services in Cloud Computing Cong Wang, Student Member, IEEE, Qian Wang, Student Member, IEEE, Kui Ren, Member, IEEE, Ning Cao, Student Member, IEEE, and Wenjing Lou, Senior Member, IEEE-2011.

[2] A privacy preserving remote data integrity checking protocol with data dynamics and public verifiability” Qian Wang, Student Member, IEEE, Cong Wang, Student Member, IEEE, Kui Ren, Member, IEEE, Wenjing Lou, Senior Member, IEEE, and Jin Li ” MAY-2011.


AUTHOR PROFILE

Mr. Lenkala Ganeshreddy currently pursuing M.Tech in the Department of Computer Science & Engineering, Visvesvaraya College of Engineering and Technology, M.P Patelguda, Ibrahimpatnam (M), Ranga Reddy(D), India. Her research interests include Cloud Computing.

Sri Dr. Bhaludra Raveendranadh Singh working as Associate Professor & Principal in Visvesvaraya College of Engineering and Technology. He obtained M.Tech, Ph.D(CSE), is a young, decent, dynamic Renowned Educationist and Eminent Academician, has overall 20 years of teaching experience in different capacities. He is a life member of CSI, ISTE and also a member of IEEE (USA).

Ms’s. Sangeetha M working as Assoc. Professor & HOD (CSE). She has completed bachelor of technology from Swamy Ramananda Theertha Institute of Science & Technology and Post-graduation from Jawaharlal Nehru Technological University, Kakinada campus and is having 12 years of teaching experience.