Secure Auditing of the User Data in Cloud Storage System

Geetha N, Jyothi T V, Prabhavathi
M.Tech/ME, Dept Of Computer Network Engineering
Visvesvaraya Technological University, Belgaum, Karnataka

***Abstract*-Cloud computing because of its wide range of applications and shared pool of resources, it has become a next generation IT technology, user stores their data in the cloud and enjoy the cloud resources involving on demand applications and services. Although Cloud has a full-fledged security resources there are so many security issues because of its distributed manner. The user does not having any control of their outsourced data. In this paper in order check the correctness of their outsourced data user takes the assistance of the Third Party Auditor who verifies of the data and sends the desired results to the requested user. In particularly maintaining privacy in the TPA verification so that he should not read the actual content of the user data which is outsourced in the cloud.**

***Keywords: Cloud computing, Secure Auditing, data integrity, cloud storage**.*

I. INTODUCTION

Cloud computing is an internet based computing which provides various applications and services like storage, servers, infrastructure, networking with low cost, on-demand self service, pay as you go model, location independent resource pooling, reasonable price , rapid elasticity etc. User can store their data on cloud and reveal from the local data storage and its maintenance. Cloud is in a distributive in nature includes shared pool of configuring resources both in hardware and software.

Cloud has many security issues because of its distributive nature and data integrity is the major security concern in cloud computing. User does know where their data is stored and not having idea whether their outsourced data is correct or not. The cloud service provider maintains the outsourced data of the user in the cloud, sometimes it behaves like a malicious server for example it can delete the rarely accessed data and in order to show their reputation it hides some corrupted user data blocks. User data while going through the network there may be many attacks like hackers, network problems so that their data may not be correctly uploaded to the CSP.

The usage and the behavior of cloud depend on some concerns are as follows:

- *Access:* client who stores their data in the cloud faced problems in securing their data by the unauthorized access.
- *Availability:* The client data that is available any time for them without having much affective problems for storage and become way to the data lose.
- *Network Load:* The over load capacity due to the huge clients uploading their data on the cloud may drop the servers out according to the high amount of the client data between the computers and the systems which stores the data.
- *Integrity:* The client doesn’t know where their data is stored in the cloud and the correctness of the data affect in many ways.
- *Data Location:* Cloud because of its distributive in nature user doesn’t know the location of the data which is stored and leads to confusion.

Data integrity checking in cloud computing is very essential so that the user can take the assistance of Third Party Auditor who has experience in doing auditing and providing correct results to the requested user. Here in our paper the TPA audits the requested user’s data without reading the actual content of the data of the requested user so that preserving more privacy and auditing in a effective way so that the client gets the required results so that he user can take his further steps in improving their data security.

II. RELATED WORK

Cloud Computing has many threats which are disturbing gigantic acceptance of cloud. Major threats that affect data integrity and privacy in cloud storage. In order to reduce this type of threats in cloud many researches are going on.

A. Existing system:

Many useful solutions were come in to picture by these research to reduce the threats in data integrity. Many approaches were come in to picture to assure the data integrity in cloud storage system. Ensuring data storage security in cloud computing by Wang C, Wang Q proposed a verification scheme for public verifiability and data dynamic operations and enhanced the POR model by changing the classic Merkle Hash Tree (MHT) construction for block tag authentication.

According to the ACM security issues which introduced one flexible and an efficient way of distributed method which attain the combined way of storage correctness assurance and supported efficient dynamic operations on data blocks along with and data error localization in the distributed verification of erasure-coded cloud data.

Dynamic Audit Services deals with the HAIL, integrity layer and a high-availability, a distributed cryptographic system which allows a group of servers to prove the client that the stored file is an intact along with retrievable.

Integrity check verification for SaaS introduced an useful approach based on the periodic verification for enhancing the performance of audit special services.

Multiple file remote integrity checking infers the notion of the proofs-of-ownership, which tells that the client accurately and efficiently prove that the client holds a file instead of than that of some sort of information about this. However, these approaches just consider the data integrity of storage of user data.

B. Proposed System

In this proposed system our security protocols for data storage in the cloud with the aforementioned research goals with aim to give security and started with some basic solutions to provide the integrity assurance of cloud data along with their demerits. Then started to present our protocol which supports the public auditability, alerts to the requested user by providing alerts and the data dynamics. Extending our results and support for the Batch auditing for TPA upon request from the multi-user in multi-cloud environment in a distributed manner.

Coming to issues in this cloud, enormous threats are raised as in Attacks on cloud. One of the major threats are data privacy and integrity. As mentioned in the existing system through many solutions and TPA can do with the auditing process by verifying blocks of the files to check the integrity of files stored by a remote server who provides the service without any knowledge of the actual data contents by comparing each in the batch auditing manner.
It has 3 phases: initialization, verification, and extraction for authentication we use the Encryption along with the block wise verifiability to maintain the local copy of data.

Advantages of Proposed Model:

For the secure data verifiability of the user data who stores their data in the cloud here in this paper using the secure Encryption methods along with the block wise verifiability to maintain the local copy of data.

The requested user will get an good idea of their data who stored it in the cloud and he can takes the further measures to secure their data.

TPA verification here is trusted and he is unable to read the actual data content so providing more security and verifying multiple files of multiple clients who requests for verification for integrity check.

The actual data size of storage file before and after verification files in cloud is maintained even though the user himself has done any modification, insertion, deletion, update and thus providing dynamics by this proposed scheme.

Here the user takes full control, accessing and processing the data stored in cloud instead of the Third party and giving strong assurance for protection to the data stored in multiple cloud server environments which is distributive. Server restore point and back up for any failure of the server by maintaining separate back up database.

III. SYSTEM DESIGN

In the system design the flow between the client i.e. the Data owner who has huge data files to be stored in the cloud storage system and depends on the cloud for data his data maintenance and can be an individual customer or an organization without the knowledge of his data location in the cloud.
Below fig shows the view of the cloud storage system
Showing the Users, auditor and the cloud service provider i.e. CSP.

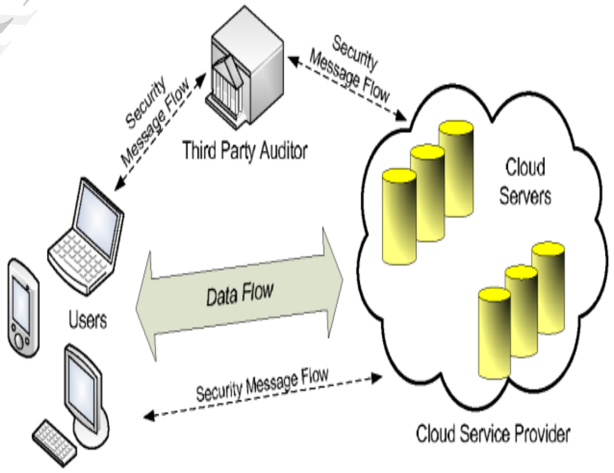

Fig. 1: The architecture of cloud data storage service

In Figure 1, the architecture introduced to the provide data integrity verification of the client data in the cloud storage system which has three main roles as below:

A- User: who stores their large data files in a cloud and who relay on the verification of their data through the TPA and in a secure way.

B- Cloud Server: Having huge amount of storage capacity and is managed by CSP i.e. cloud service provider, along with its storing space and flexible recourses to keep up the client data processing.

C- TPA: who has specialized skills, expertise in auditing of the user data that requests for the verification and provides the actual auditing results to the requested clients with the full details.

Whenever the client uploads a large amount data file like through many apps like Google drive to a remote cloud server, the users may not be able to process their data in their local storage; moreover, they are unable to verify their data in the remote servers as the data location in the cloud is independent and there are so many replicas to keep the back up of the clients data. In that case one must need to assign the data correctness verification assigns to TPA to do the verifying task in order to help the client who requests for correctness and that verification task is difficult procedure to him no any regular client can do it without having a background in the verification process . The TPA has an access to the cloud service provider environment and understands, accepts the service level agreements (SLA) that is between the customer and the provider.

IV. IMPLEMENTATION

To implement our design it is necessary to achieve some goals in our model by allowing the TPA to verify the correctness of the requested client outsourced data in the cloud. Additionally, it should follow that to ensure that the auditor does not manipulate or alter the user data in the cloud while verifying process is going on.

In our model, first the client stores his data in the cloud system and it is maintained by the cloud service provider as illustrated in the below fig.

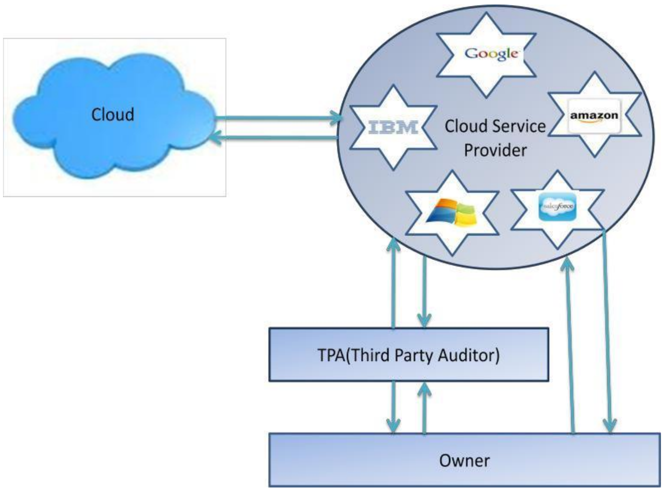

Fig.2: Flow of data between client, TPA and CSP

In the fig.2 the flow between the client i.e. the Data owner who has huge data files to be stored in the cloud storage system and depends on the cloud for data his data maintenance and can be an individual customer or an organization without the knowledge of his data location in the cloud.

Cloud Storage Service Provider(CSP) who provides data storage service to many customers on the basis of pay as you go method, in a cost effective manner and has enough storage servers to maintain multiple clients data.

Next the Third Party Auditor(TPA) a trusted person who verify or monitor outsourced data under the request from the owner.

Consider the above fig showing many cloud service providers like Amazon, IBM, Google etc, having huge storage capacity, the owner having data files prefer to store their data in the cloud environment, one should wants there data to be safe and secure.

While uploading the data he used to do encryption methods for transferring the data and the key is transferred to the CSP, who misbehaves in sometimes to show their reputation, it may be a CSP employee or sometime while uploading, downloading or in transferring the client data to cloud ,there may be a chances of losing the data.

The data in the cloud may not be correct as discussed above so it is necessary for the client or data owner to verify their data, but it is time consuming if he is the verifier instead of this he will choose TPA whose duty is auditing data's of requested user.

Upon request from the client the TPA here should follow the rules that he should not read the actual data, many researches were introduced but still there exists a leakage data to TPA, here in our system it will not happen because here I am going to use encrypted block wise verification thus preserving more security and giving results to the requested user in the form of alerts so that the user can take further steps in order secure his data.

In our model it also supports for data dynamics infers client can update his data in the cloud thus preserving data dynamics, and giving alerts to multiple requested clients with alerts simultaneously.

The following will explanation for the each entity function in the proposed model as follows:

1- User: He first chose a random parameter to construct Encryption key then he will sign the data using that key that should be uploaded to the cloud, then sending the signed data to the cloud server along with the key and deletes its local copy and became free from burden.

2- CS: provides data storage service to many customers on the basis of pay as you go method, in a cost effective manner and has enough storage servers to maintain multiple client data, takes the encrypted data verified for the authenticated user and stores it in its storage environment.

3- TPA: After cloud server completes its role, TPA checks for the clients requests for verification if it so, the TPA will starts to verify over the cloud server by taking the encrypted data from the cloud server. Then he will do that to divide it in to blocks, he takes another client data block randomly picking and goes on comparing the encrypted blocks but here he could not read the actual content of that data. After finishing the verification, the TPA will inform the user if the service provider was trusted or not to the client leaving a message like this block is modified by this server.

Fig.3 showing the detailed view of the secure auditing process in cloud storage system

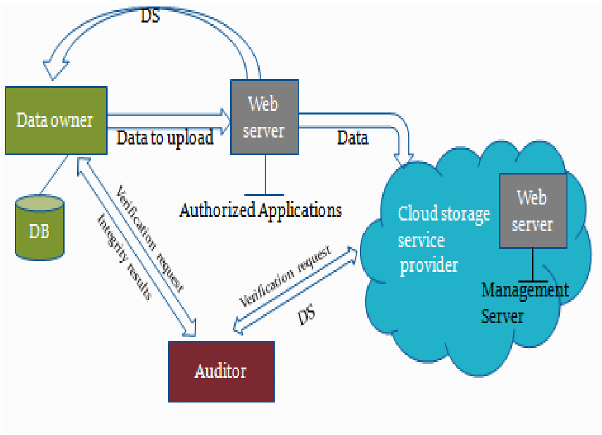

Fig.3. Detailed architecture of auditing process.

IF the user needs to verify his data means the verification request should be send to TPA whose work is auditing, the TPA checks for the clients requests for verification if it so, the TPA will starts to verify over the cloud server by taking the encrypted data from the cloud server. Then he will do that to divide it in to blocks, he takes another client data block randomly picking and goes on comparing the encrypted blocks but here he could not read the actual content of that data. After finishing the verification, the TPA will inform to the user if the CSP was trusted or not to the client leaving a message like this block is modified by this server.

Here in the TPA there the data should be readable but not editable and verifying correctness of data. The main aim of this scheme is to ensure that the data

Integrity in the cloud storage system and is efficient. Data integrity in the sense, the data stored by the data owner or client should be same without any lose or any modification of his data in the receiver side.

Consider a client has stored his data at an untrusted server to verify that server possess the original data without retrieving or modifying it.

In the TPA verifying process if the compared data is not same in the sense the TPA will send an alert message to the data owner who requests for verification.

In the case of implementation it consists of three important modules namely admin i.e. CSP, user i.e. client and auditor modules.

The admin module has to responsible for maintaining the whole security system. It maintains the user's detailed list which consists of the username, Password, gender, phone number and email id. The admin is capable to edit, update, add or delete the list.

Same like that the list of auditors is also maintained by the admin with details and for authenticated auditors. Next in the transaction details which will contain the logged in time and date, if profile of user or auditor is modified that details and the uploaded file names, time and date are maintained regularly. In the case of the user module the user details can be viewed. For that the user can click into add then choose a file by clicking browse from the system and then submit and sometimes to which the cloud server, the file will be uploaded successfully and having this much of size. Before uploading one can give the key to encrypt data which is going to upload application will generate the message digest and encrypt it and then send it to the cloud storage in the encrypted form itself then he requests TPA for verification by clicking on the request button.

Next coming to the auditor module, who checks for integrity of the data upon request from the client. In this TPA verifying process if the compared data is not same in the sense the TPA will send an alert message to the data owner who requests for verification.

Along with this it also support for the data dynamics and the auditing time for the multiple clients become fast simultaneously sending alerts to the requested clients, after the message reaching the specified clients one can update their original data in the client or he/she can change the storage server.

V. CONCLUSION

There are various existing auditing schemes available to ensure integrity of the client data as mention above. But in most of those schemes there is a leakage of information from the verifier or the auditor side because the verification is done with the use of local copy of the requested data, or it may lead to extra burden to the data owner i.e. client in the case of private auditing of their data. In our proposed scheme the zero knowledge property i.e. the TPA verifies the requested client data without knowing the actual data content of the client such that the TPA who is responsible to verify the user's data will not be having any knowledge about the client data thus providing more secure. So, our proposed scheme can be more secured than any other if we compared it to the existing conventional schemes. Next, for the verification, only the encryption of the data with the block wise auditing and such that communication cost can also be reduced in our scheme. By all these advantages of the proposed scheme it is the most economical secured way of auditing in the storage system of Cloud Computing.

REFERENCES

[1] Akhil Behl, Emerging Security Challenges in Cloud Computing . Congress on Information and Communication Technologies (WICT), 2011 World.

[2] Wang, Q., Wang, C., Li, J., Ren, K., Lou, W.: Enabling Public Verifiability and Data Dynamics for Storage Security in Cloud Computing. In: Backes, M., Ning, P. (eds.) ESORICS 2009. LNCS, vol. 5789, pp. 355–370. Springer, Heidelberg (2009)

[3] Amazon.com,"Amazon s3 availability event: July20,2008,"http://status.aws.amazon.com/s3-20080720.html, 2008

[4] Wang, C., Wang, Q., Ren, K., Lou, W.: Ensuring data storage security in cloud computing. In: 17th IEEE International Workshop on Quality of Service (IWQoS 2009), pp. 1–9. IEEE Press, New York (2009)

[5] Jianfeng Yang, Zhibin Chen, Cloud Computing Research and Security Issues. 2010 International Conference on Computational Intelligence and Software Engineering (CiSE)

[6] Bowers, K., Juels, A., Oprea, A.: HAIL: a high-availability and integrity layer for cloud storage. In: Proceedings of the 2009 ACM Conference on Computer and Communications Security (CCS 2009), pp. 187–198. ACM, New York (2009)

[7] G. Ateniese, R. Burns, R. Curtola, J. Herring, L.Kisser and D. Song, "Provable data possession at untrusted stores", in Proc. Of CCS'07, pp.598-609.

[8] Chandran S. and Angepat M., "Cloud Computing: Analyzing the risks involved in cloud computing environments," *in Proceedings of Natural Sciences and Engineering*, Sweden, pp. 2-4, 2010.

[9] Zhu, Y., Wang, H., Hu, Z., Ahn, G., Hu, H., Yau, S.: Dynamic Audit Services for Integrity Verification of Outsourced Storages in Clouds. In: The 26th Symposium On Applied Computing, pp. 1550–1556. ACMSAC, Taiwan (2011)

[10] B. Priyadharshini, P. Parvathi "Data Integrity in Cloud Storage", IEEE International Conference On Advances In Engineering, Science And Management, 2012.

[11] Shi, Y., Zhang, K., Li, Q.: A New Data Integrity Verification Mechanism for SaaS. In: Wang, F.L., Gong, Z., Luo, X., Lei, J. (eds.) WISM 2010. LNCS, vol. 6318, pp. 236–243. Springer, Heidelberg (2010)

[12] Shuai Han, Jianchuan Xing "Ensuring data
storage security through a novel third party auditor scheme in cloud computing", in the International Conference on Cloud Computing & Intelligence Systems, 2011.

[13] Shi, Y., Zhang, K., Li, Q.: Meta-data Driven Data Chunk Based Secure Data Storage for SaaS. International Journal of Digital Content Technology and its Applications 5, 173–185 (2011)

[14] Sravan Kumar R, Ashutosh Saxena "Data Integrity Proofs in Cloud Storage", IEEE International Conference on Communication Systems & Networks, 2011.

[15] Pinkas, B., Shulman-Peleg, A., Halevi, S., Harnik, D.: Proofs of ownership in remote storage systems. Cryptology ePrint Archive, Report 2011/207 (2011)

[16] Xiao, D., Yang, Y., Yao, W., Wu, C., Liu, J., Yang, Y.: Multiple-File Remote Data Checking for cloud storage. Computers and Security 31(2), 192–205 (2012)

[17] Juels, A., Kaliski Jr., B.: PORs: proofs of retrievability for large files. In: Proceedings of the 2007 ACM Conference on Computer and Communications Security (CCS 2007), pp. 584–597. ACM, New York (2007)

[18] Balakrishnan S, Saranya G, et al. (2011). Introducing Effective Third Party Auditing (TPA) for Data Storage Security in Cloud, International Journal of Computer Science and Technology, vol 2(2), 397–400.

[19] Ateniese, G., Burns, R., Curtmola, R., Herring, J., Kissner, L., Peterson, Z., Song, D.: Provable data possession at untrusted stores. In: Proceedings of the 2007 ACM Conference on Computer and Communications Security (CSS 2007), pp. 598–609. ACM, New York (2007)

[20] Reza, C., Osama, K., Randal, B., Giuseppe, A.: MR-PDP: Multiple-Replica Provable Data Possession. In: The 28th International Conference on Distributed Computing Systems, pp. 411–420. IEEE Press, Beijing (2008)

[21] Xian, H., Feng, D.: An Integrity Checking Scheme in Outsourced Database Model. Journal of Computer Research and Development 47(6), 1107–1115 (2010)

[22] Merkle, R.C.: Protocols for public key cryptosystems. In: Proc. of IEEE Symposium on Security and Privacy, pp. 122–134. IEEE Computer Society, Washington (1980)