International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347 - 6435 (Online)), Volume 2, Special Issue 3, February 2014)
International Conference on Trends in Mechanical,Aeronautical,Computer,Civil,Electrical and Electronics Engineering (ICMACE14)

Effective Verification on Data Integrity in Cloud Storage

S.Deeparani[1] and A.Jebasheela[2]

[1]PG Student

[2]Assistant Professor

[1]sdeeparanisenthil@gmail.com

[2]jebasheela.soft@gmail.com

***Abstract*— Effective Data Integrity verification scheme ensures integrity of the data in cloud based storage. This scheme is based on homomorphic encryption and hash index hierarchy to provide high security. It introduces third party verifier to eliminate the involvement of the client and verify the integrity of the data stored in the cloud. It performs periodic verification to enhance audit performance. If cloud service provider illegally accessed the clients data TPV send alert to data owner. This Effective Integrity verification scheme resists various security attacks. It stores and maintain clients data effectively and achieves privacy protection.**

***Index Terms*—Effective Integrity Verification, Third Party Verifier, Periodic Verification**

I.INTRODUCTION

Cloud storage means the storage of data in the cloud where in a company's data is stored in and accessible from multiple distributed and connected resources that comprise a cloud. In cloud based storage, the data is stored in virtualized pools of storage system. Cloud storage provides ease of access and lower overall storage costs, reliability, strong protection for archival and data backup and disaster data recovery , manage expensive hardware.

Various technologies and tools for cloud computing such as VMware vSphere and Platform VM Orchestrator, Ovirt. These technologies help cloud service providers to construct a cloud storage platform. However, confidential data may be lost or tampered in cloud storage. Outsourcing data should be protected in cloud environment.

Provable Data Possession and Proofs of retrievability are technique for a cloud storage provider to prove the integrity of owner's data without downloading the data. It is most important for large files and folders. To check the client's data have been lost or tampered without downloading.

Many PDP scheme have been proposed such as light weight PDP and Scalable PDP. This scheme does support dynamic operations and it has some limitations for data challenges. Cloud storage system adopt many new distributed file systems. for example Cloud Store, Apache ad hoop Distribution file System, Amazon S3 File System, Google file system.

II. MOTIVATION

Cloud Storage offers many benefits like low cost, location independent platform and scalable for client's. However it is difficult to perform an efficient verification on the integrity of stored data in cloud storage. Additionally it provides reliability and automatic redeploying processing logic for event failure.

Related Works. Many PDP schemes developed to ensure the integrity of the data stored in cloud based storage. Initially PDP scheme were developed for ensuring integrity of files at untrusted cloud storages and provided RSA scheme for static operations.

Next they proposed a public verification which allows anyone do the challenge to the server for data integrity. These schemes are not secure against security threat in dynamic scenarios .To support dynamic data operation, they developed a DPDP scheme proposed based on cryptographic hash function and symmetric key encryption.

Cloud owner can illegally access the client's data because of insuffient randomness in the challenges. This scheme has limited number of challenges and fixed number of updates. So client cannot perform insertion operation.

International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347 - 6435 (Online)), Volume 2, Special Issue 3, February 2014)
International Conference on Trends in Mechanical,Aeronautical,Computer,Civil,Electrical and Electronics Engineering (ICMACE14)

III. Structure And Techniques

Effective integrity verification scheme for cloud based storages is based on homomorphic encryption and hash index hierarchy. These techniques are mainly used to provide a high performance, transparent verification and high security. Homomorphic encryption would allow the chaining together of different services without establish the data to each of those services.

Homomorphic property can be used to create collision resistant hash function. Widespread use of cloud computing by ensuring the confidentiality of processed data. Hashing can be used not only for file organization but also for index structure creation. Hash index organizes the search keys with their associated record pointer into a hash file structure. Hashing is generally better at retrieving records having a specified key value and ranges queries are common ordered indices are to be preferred. Hash index hierarchy is used to record the changes of file blocks and generate the block hash value for the verification process. Hash index hierarchy has hierarchy structure which represents file storage. it has three layers to represent the relation among stored resources.

Homomorphic encryption is the key technique of effective integrity verification because it reduces communication bandwidth as well as finds data leakage in storage outsourcing. Effective integrity verification is constructed on collision resistant hash, bilinear map group and homomorphic responses

IV.Proposed System

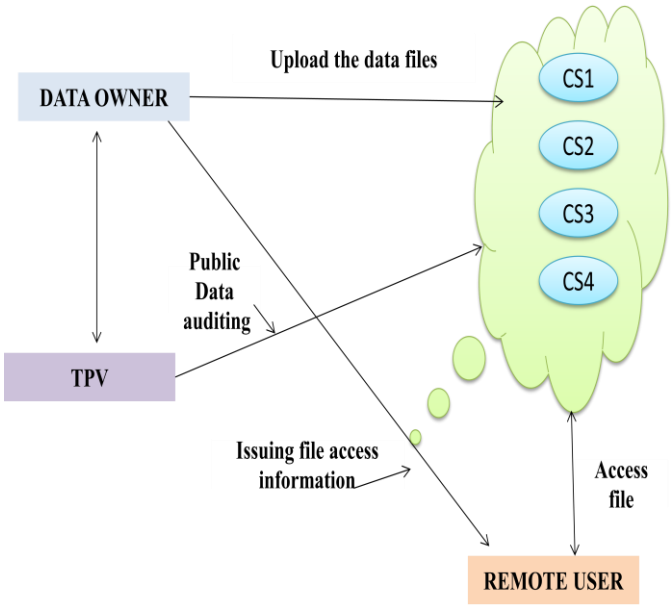
Security is a one of the major issue during data storage in cloud computing environment. For secure data storage and correctness of user's data, to construct a verification framework based on homomorphic encryption and hash index hierarchy. It introduces TPV to eliminate the involvement of client and TPV verify the integrity of the data stored in the cloud. It performs periodic verification to ensure correctness of the data. It resists various data leakage and security threats. If cloud service provider illegally accessed the data, TPV sends alert to data owner.Client sends only Meta data to the third party verifier for verification process. So third party verifier does not get full details of stored data.

However TPV performs auditing by using the meta data about storage outsourcing. so TPV has no choice of getting the clients detail.

System architecture:

The design module of the effective integrity verification has three major entities. they are data owner, cloud user and cloud service provider. This scheme is used to verify the client's data correctness by using integrity technique. Data owner can store their data in the cloud based storage. Initially client gets their space. To get the space for their storage client send their request to the cloud service provider and gets their space for the data storage. Cloud service provider allocates the space for their client with time period. After cloud service provider allocates space, client sends their data and store in the cloud. In this way data owner uploads their data. Cloud service provider provides services for the data owner's data stored in cloud. Whenever cloud user uses the data, cloud user can download their files. User can also perform dynamic operations.

System Architecture Diagram for integrity verification



International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347 - 6435 (Online)), Volume 2, Special Issue 3, February 2014)
International Conference on Trends in Mechanical,Aeronautical,Computer,Civil,Electrical and Electronics Engineering (ICMACE14)

To check the integrity of the data in the cloud based storage, this scheme introduces third party verifier. Data owner gives verification parameter to TPV.TPV is trusted to cloud user. This verification parameter generated by homomorphic encryption. TPV stores all verification parameters. Whenever client wants to verify the correctness of the data stored in the cloud, Client can issue a request

for the audit and this request send to TPV. TPV performs the auditing and check all the details.

After auditing, TPV sends the report to the data owner. If any unauthorized attack in the client's data immediately an alert send to the data owner.

V. Integrity Verification In Cloud

Effective integrity verification system defines four modules to ensure the data integrity in the cloud based storage.

1. Cloud storage
2. Integrity verification
3. Third party verifier
4. Cloud user

CLOUD STORAGE

Cloud-based storage relieves the client's burden for storage management and maintenance. Cloud allocates the space for the individual cloud user after cloud service provider receives the request from the data owner. cloud service provider send user name and password to cloud user. User can enter the cloud space by using the password only. cloud user can use their space and user can upload their data into the cloud space. cloud storage services has three entities. These entities can enter into the cloud space and access the stored data. The entities are cloud user, cloud service provider and third party verifier

INTEGRITY VERIFICATION

Data Integrity is one of the important in database operation in particular. Because Data Integrity ensured that data is of high quality, correct, consistent and accessible. Client can issue a challenge for their data. Data owner sends verification parameters to third party verifier.

Third party verifier store these verification parameters and offer query services for these parameters.

THIRD PARTY VERIFIER

Third party verifier is trusted to data owner.TPV is a independent and reliable one through the verification process. Third party verifier performs periodic verification based on cloud user request. TPV periodic verification enhances the performance. Whenever user wants to check the correctness of the data, User sends a request and generates the verification parameter. User encrypts all the details. By using public key TPV decrypt the client details and performs auditing. if any data leakage, an alert send to the data owner. After this verification process, TPV generate the report and send to data owner

CLOUD USER

The Cloud User who has a large amount of data to be stored in cloud space and have the permissions to access and manipulate data. The client's Data is converted into data blocks. The data are uploaded to the cloud. In cloud based storage anything we can store it in cloud space. For example music files, video files, images, data files. The TPA view only meta data. The user can update the data in cloud space. If the cloud user wants to download the files, the data's in cloud can be downloaded. user can rename the file and user can delete the data files. All type of dynamic operations can be performed.

VI. Conclusion And Future Enhancement

Provable data possession is a data integrity technique which is used to ensure the correctness and consistency of the data. In this paper, the construction of an effective integrity scheme for cloud based storage ensures the integrity of data without downloading. This scheme is based on homomorphic encryption and supports dynamic operation in cloud based storage. It resists various security attacks in cloud environment. Behalf of the cloud client, effective integrity verification scheme use third party verifier to perform auditing. It reduces involvement of the client and it enhances the performance through the periodic verification. It introduces small amount of computation and less communication overheads.

Furthermore, it optimized the probabilistic query services and periodic verification to enhance the audit performance. Therefore, solution can be treated as a new candidate for data integrity verification in cloud based storage systems. As part of future work, extend the work to explore more effective integrity verification constructions. It is a challenging problem for the generation of tag with the length irrelevant to the size of data. This scheme explores such an issue to provide the support of variable-length block auditing.

As part of future work, extend this to explore more effective integrity verification Constructions. First, from this project we found that the performance of EPDP scheme, due to its high complexity of the large file, it is affected by the bilinear mapping operations. To solve this problem, RSA based constructions will be a better choice, but still this is a challenging task because the existing RSA schemes have too many restrictions on the performance and security. Next, from a practical point of view, still we need to solve some issues about integrating effective integrity verification scheme smoothly with existing systems, for example, how to match hash index hierarchy with HDFS two-layer name space, how to match index with cluster network model, and how to dynamically update the parameters according to HDFS specific requirements. Still it is a challenging problem for the generation of tag with the length irrelevant to the size of data . Finally, I would explore such an issue to provide the support of variable-length block verification.

VII. REFERENCES

[1] G. Ateniese, R. C. Burns, R. Curtmola, J. Herring, L. Kissner, Z. N. J.Peterson, and D. X. Song, "Provable data possession at untrusted stores,"in ACM Conference on Computer and Communications Security, 2011.

[2] G. Ateniese, R. D. Pietro, L. V. Mancini, and G. Tsudik, "Scalable and efficient provable data possession," in Proceedings of the 4thinternational conference on Security and privacy in communication netowrks, SecureComm, 2010.

[3] C. C. Erway, A. K¨upc¸ ¨u, C. Papamanthou, and R. Tamassia, "Dynamic provable data possession," in ACM Conference on Computer and CommunicationsSecurity, 2011.

[4] Q. Wang, C. Wang, J. Li, K. Ren, and W. Lou, "Enabling public verifiability and data dynamics for storage security in cloud computing,"in ESORICS, 2009.

[5] Y. Zhu, H. Wang, Z. Hu, G.-J. Ahn, and H. Hu, "Zero-knowledge proofs of retrievability," Science China: Information Sciences, 2011.

[6] H. Shacham and B. Waters, "Compact proofs of retrievability," inASIACRYPT, 2008.

[7] A. Juels and B. S. K. Jr., "Pors: proofs of retrievability for large files,"in ACM Conference on Computer and Communications Security, 2007.