*International Journal of LNCT, Vol 2(5)*
*ISSN (Online): 2456-9895*

# Survey of efficient remote data possession checking protocol in cloud storage

**Rashmi Dwivedi[1], Sunil Phulre[2], and Sadhana K Mishra[2]**
M.Tech Scholar, LNCT Bhopal India[2]
Associate Professor, LNCT Bhopal, India[2]

## Abstract
***Cloud storage offers the users with top quality and on-demand information storage services and frees them from the burden of maintenance. Cloud computing has been pictured because the on-demand self-service, present network access, location independent resource pooling, speedy resource elasticity, usage-based evaluation and transference of risk. Today, technical analyses works specialize in Remote information possession checking protocols allow examining that an overseas server will access an uncorrupted file with the assistance of third party verifiers. Remote information integrity checking is very important in cloud storage. It will build the purchasers verify whether their information is kept because it is while not downloading the complete information. In some application situations, the purchasers got to store their information on multi-cloud servers. At a similar time, the integrity checking protocol should be efficient so as to save the verifier's price.***

## Keywords
***Cloud storage, Data possession checking, Homomorphic hash function, Dynamic operations.***

## 1.Introduction
Cloud computing has been thought of as a replacement model of enterprise IT infrastructure, which might organize huge resource of computing, storage and applications, and modify users to enjoy present, convenient and on-demand network access to a shared pool of configurable computing resources with great efficiency and minimal economic overhead [1]. Attracted by these appealing options, each people and enterprises are driven to source their information to the cloud, rather than getting package and hardware to manage the information themselves.
Cloud storage provides a completely unique service model (Wu, 2011) during which information are maintained, managed and saved remotely and accessed by cloud users over the network at anytime and from anyplace. Nowadays, an increasing variety of organizations and people would like to source their information to cloud to relish appealing benefits of cloud storage. However, once an information owner uploads his/her data to cloud and delete the native copy of the files, the owner loses physical control over the outsourced information.

Cloud computing is the long dreamed visualization of computing as a usefulness, where users can remotely store their data into the cloud so as to like high quality applications and services from a common pool of configurable computing resources (fig.1). It works on a client-server basis, using web browser protocols.

A cloud user desires a consumer device like a laptop computer or microcomputer, pad laptop, good phone, or different computing resource with an online browser (or different approved access route) to access a cloud system via the World Wide Web. Usually the user can log into the cloud at a service supplier or private company, like their leader. The cloud provides server-based applications and everyone information services to the user, with output displayed on the consumer device.

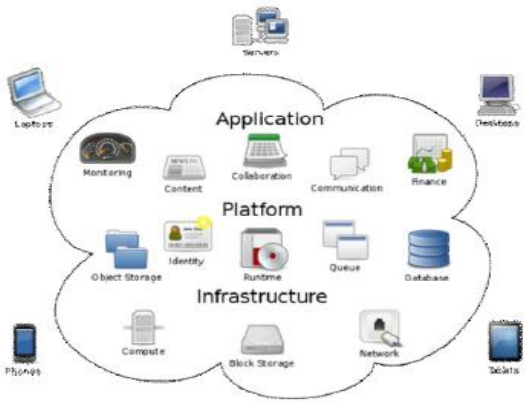


**Figure 1** Cloud computing

Memory allotted to the consumer system's application program is employed to create the applying information appear on the consumer system show, however all computations and changes are recorded by the server, and final results as well as files created or altered are for good keep on the cloud servers.

Performance of the cloud application relies upon the network access, speed and dependability also because the process speeds of the consumer device [2]. Whereas Cloud Computing makes these benefits additional appealing than ever, it additionally brings

new and difficult security threats towards users' outsourced information. Since cloud service suppliers (CSP) are separate body entities, information outsourcing is really relinquishing user's final control over the fate of their information.

## 2.Literature survey

Hao Yan et al.[1] "A Novel Efficient Remote Data Possession Checking Protocol in Cloud Storage", In this paper, we tend to study the problem for integrity checking of information files outsourced to remote server and propose an economical secure RDPC protocol with data dynamic. Our scheme employs a homomorphic hash operates to verify the integrity for the files keep on remote server, and reduces the storage prices and computation prices of the information owner. We tend to style a new light-weight hybrid organization to support dynamic operations on blocks that incurs minimum computation prices by decreasing the amount of node shifting. Using our new organization, the information owner will perform insert, modify or delete operation on file blocks with high efficiency. The given scheme is proved secure in existing security model. We tend to measure the performance in term of community price, computation price and storage price. The experiments results indicate that our scheme is practical in cloud storage.

Huiling Qian et al.[2] "Privacy-preserving personal health record using multi-authority attribute-based encryption with revocation", In this paper,we propose a privacy-preserving multi-authority CP-ABE scheme that may be utilized in PUDs of PHR system [4] in cloud computing. Once encrypting PHRs, patient will associate an expressive access tree structure with the ciphertext, therefore achieving fine-grained access management. We tend to additionally accomplish privacy-preserving by using anonymous key supply protocol. Corrupted authorities will get nothing regarding user's GID whereas execution anonymous key supply protocol, and so, they can't collect user's attributes by tracing GID. Moreover, our theme supports efficient and on-demand lazy user revocation that reduces the overhead lots. We tend to prove the protection of our scheme below a regular complexness assumption (respectively, DBDH).

Jiguo Li et al.[3] "Flexible and Fine Grained Attribute-Based Data Storage in cloud Computing", In this article, we tend to provided a proper definition and security model for CP-ABE with user revocation. We tend to additionally construct a concrete CP-ABE scheme that is CPA secure supported DCDH assumption. To resist collusion attack, we tend to insert a certificate into the user's private key. So malicious users and also the revoked users don't have the power to come up with a sound personal key through combining their personal keys. In addition, we tend to source operations with high computation price to E-CSP and D-CSP to reduce the user's computation burdens. Through applying the technique of source, computation price for native devices is way lower and comparatively mounted. The results of our experiment show that our scheme is efficient for resource constrained devices.

Jiguo Li et al.[4] "KSF-OABE: Outsourced Attribute-Based Encryption with Keyword Search Function for Cloud Storage", In this article, we tend to propose a CP-ABE scheme that has outsourcing key-issuing, coding and keyword search perform. Our scheme is efficient since we tend to only got to transfer the partial decryption ciphertext such as a selected keyword. In our scheme, the long pairing operations are often outsourced to the cloud service supplier, whereas the slight operations are often done by users. Thus, the computation value at each users and sure authority sides is decreased. Moreover, the projected scheme supports the perform of keywords search which may greatly improve communication efficiency and additional defend the protection and privacy of users. Actually, we tend to are simple to increase our KSF-OABE scheme to support access structure diagrammatic by tree in [9].

Zhangjie Fu et al.[5] "Enabling Personalized Search over Encrypted Outsourced Data with Efficiency Improvement", In this paper, we tend to address the matter of personalized multi-keyword graded search over encrypted cloud knowledge. Considering the user search history, we tend to build a user interest model for individual user with the assistance of semantic ontology WordNet. Through the model, we've got realised automatic analysis of the keyword priority and solved the limitation of the artificial technique of measure. Moreover, we tend to propose 2 PRSE schemes to resolve 2 limitations (the model of "one size work all" and keyword actual search) in most existing searchable encoding schemes. Additionally, thorough privacy analysis and performance analysis demonstrates that our scheme is practicable.

## 3.Methods

**Online memory checker and sublinear authenticator**

Remote integrity verification incorporates a close relationship with memory integrity verification. The notion of authenticator projected by Naor and Rothblum is developed for memory integrity checker. there's a vital difference between memory checker and proofs of storage drawback studied during this paper: within the memory checker drawback, an honest prover can follow the required protocol to verify its storage, wherever the storage is untrusted and will be altered by outside attackers or random hardware failure; within the proofs of storage drawback, each the prover and its storage are untrusted, specified the prover may do anything5 throughout a verification and also the storage may well be altered carefully by the dishonest prover. Consequently, any resolution to a symbol of storage drawback is additionally a solution to the memory checker drawback. Thus, the lower bound on complexness of memory checker discovered by Naor and Rothblum additionally applies to proofs of storage. In addition, the concept of introducing redundancy to trade-off resources is useful in proofs of storage.

**Proofs of retrievability and provable data possession**

Recently, there's a growing interest within the cryptographical aspects of cloud storage drawback. maybe Filho and Barreto 1st studied the situation wherever the verifier doesn't have the first. They represented 2 potential applications: uncheatable information transfer and demonstrating information possession, and projected the RSA-based scheme. Juels and Kaliski projected a formulation referred to as Proofs of Retrievability POR for the proofs of storage drawback. Basically, during a POR scheme, if the cloud storage server will pass verification with an apparent likelihood, then the verifier will retrieve the first information from messages collected throughout polynomially several verification interactions between the verifier and therefore the cloud storage server. Thus POR formulation permits a user to confirm whether his/her file is so within the cloud storage in an intact form while not truly downloading the file. However, the POR construction in Juels and Kaliski will support only a predefined constant range of verifications.

Ateniese et al. gave an alternate formulation referred to as demonstrable information Possession for proofs of storage drawback, and projected an efficient construction. Their technique may be viewed as an extension of the RSA-based scheme. The scheme EPOS projected during this paper exploits similar plan, that is way additional efficient than Ateniese et al.

Shacham and Waters projected 2 efficient constructions of POR, wherever one scheme supports private key verification and therefore the different supports public key verification.

**Proofs of storage with more features**

Very recently, many works have dedicated to extend proofs of storage to support additional options. In, friend checks whether or not the cloud storage server so keeps multiple intact copies of a user's file. Dynamic-PDP permits insertion and deletion of information blocks on the fly when setup. Proofs of storage schemes supporting public verifiability are projected in Shacham and Waters and Wang and also the privacy issue publically verification is studied in Wang very recently, dynamic POR is studied.

**More general delegated computation and proofs of storage**

Kate and Zaverucha and Goldberg projected an economical commitment scheme for polynomial and Benabbas and Gennaro and Vahlis projected a secure delegation scheme for polynomial analysis. each schemes will be extended to support POR simply however with limitations: the POR scheme implied in Kate and Zaverucha and Goldberg has giant storage price on shopper aspect and also the POR scheme implied in Benabbas and Gennaro and Vahlis has giant storage and computation price on the server aspect. The 2 solutions to verifiable delegation of generic computation task supported totally homomorphic encryption conjointly imply secure proofs of storage scheme. However, the efficiency overheads in communication, storage and computation on the server aspect are large, rendering the resulting proofs of storage schemes impractical.

## 4.Conclusion

Currently, cloud storage has become a vital storage pattern and users will source their files there. This storage pattern provides many edges for users, as well as measurability and accessibility, and considerable price saving. It additionally brings some security risks to users. During this paper, a privacy-preserving protocol for remote information storage within the cloud is said work work the remote information possession checking. During this paper, we tend to study the techniques of confirming the

information integrity over the cloud servers, the safety issue and planning strategies of remote information possession checking protocol.

## References


[1] Yan H, Li J, Han J, Zhang Y. A novel efficient remote data possession checking protocol in cloud storage. IEEE Transactions on Information Forensics and Security. 2017; 12(1):78-88.

[2] Qian H, Li J, Zhang Y, Han J. Privacy-preserving personal health record using multi-authority attribute-based encryption with revocation. International Journal of Information Security. 2015; 14(6):487-97.

[3] Li J, Yao W, Zhang Y, Qian H, Han J. Flexible and fine-grained attribute-based data storage in cloud computing. IEEE Transactions on Services Computing. 2017; 10(5):785-96.

[4] Li J, Lin X, Zhang Y, Han J. KSF-OABE: outsourced attribute-based encryption with keyword search function for cloud storage. IEEE Transactions on Services Computing. 2017; 10(5):715-25.

[5] Fu Z, Ren K, Shu J, Sun X, Huang F. Enabling personalized search over encrypted outsourced data with efficiency improvement. IEEE Transactions on Parallel and Distributed Systems. 2016; 27(9):2546-59.

[6] Xia Z, Wang X, Sun X, Wang Q. A secure and dynamic multi-keyword ranked search scheme over encrypted cloud data. IEEE Transactions on Parallel and Distributed Systems. 2016; 27(2):340-52.

[7] Yu Y, Ni J, Au MH, Liu H, Wang H, Xu C. Improved security of a dynamic remote data possession checking protocol for cloud storage. Expert systems with applications. 2014 Dec 1;41(17):7789-96.

[8] Haifeng M, Zhenguo G, Nianmin Y. Hierarchical Enhanced Remote Data Possession Checking in Cloud Storage. Boletín Técnico. 2017;55(3):145-54.

[9] Serrano JF, Rina S. Communication complexity in high-speed distributed computer network in an agent based architecture for grids service. International Journal of Advanced Computer Research. 2018; 8(35):72-89.

[10] Ren YJ, Shen J, Wang J, Han J, Lee SY. Mutual verifiable provable data auditing in public cloud storage. 網際網路技術學刊. 2015; 16(2):317-23.

[11] Deswarte Y, Quisquater JJ, Saïdane A. Remote integrity checking. In integrity and internal control in information systems VI 2004 (pp. 1-11). Springer, Boston, MA.

[12] Hao Z, Zhong S, Yu N. A privacy-preserving remote data integrity checking protocol with data dynamics and public verifiability. IEEE transactions on Knowledge and Data Engineering. 2011; 23(9):1432-7.

[13] Ateniese G, Burns R, Curtmola R, Herring J, Kissner L, Peterson Z, et al. Provable data possession at untrusted stores. In Proceedings of the 14th ACM conference on Computer and communications security 2007 (pp. 598-609). ACM.

[14] Ateniese G, Di Pietro R, Mancini LV, Tsudik G. Scalable and efficient provable data possession. In Proceedings of the 4th international conference on Security and privacy in communication netowrks 2008 (p. 9). ACM.

[15] Nalini DT, Manivannan DK, Moorthy V. Efficient remote data possession checking in critical information infrastructures ensuring data storage security in cloud computing. International Journal of Innovative Research in Computer and Communication Engineering. 2013; 1(1).