A Review of Research on Ensuring Outsourcing of Multiple Copies of Data over Cloud

[1]Snehal.G.Shirole, [2]Prof. N.B.kadu
[1]PG Student, [2]Associate Professor
[1]Department of Computer Engineering
[1]Pravara Rural Engineering College, Loni, India

***Abstract* - The advantage of cloud computing has expand quickly in several organization. Cloud computing gives many profit in relating to low cost and availability. Providing the security of cloud computing is the main element in cloud computing environment. If we are storing some data on cloud we pay rent for them. The Cloud service provider issues paid loading area on its framework to save clients data. Therefore it is important for customer to have powerful assurance that really getting receiving service as they paid for them. In this paper we are introducing ensuring outsourcing of multiple copies of data over cloud. It provides a confirmation to the client that the cloud service provider is not defrauder by saving limited copies. It support dynamic operations like as block modification, insertion, deletion, and append. It also provides the security to our system.**

***Index Terms – Cloud service provider, outsourcing,* data integrity**

I.INTRODUCION

Cloud computing is described as a kind of computing that depend on *dividing the computing resources* instead of having localized servers or individual equipment to manage the approach. These cloud service provider assit the user to deliver their data to cloud. Cloud computing is defined as reserving and approaching data across the internet. Today, numerous individuals and institution transfer their data to cloud service providers. Such transferring of data storage allow client to save extra data on the cloud service provider than on personal computer. Systematic provable approach is of meaningful value for cloud client to recognize data integrity over the cloud service provider. Provable data possession (PDP) is a procedure for protecting the integrity of data in storage outsourcing. In provable data possession model the data owner produce some intelligence for a data file to be used ensuring for support basis across a protocol with the cloud server. This means that the remotely stored data can be not only retrieve by the authorized users, also modify and spread by the data owner. The owner gives the file to reserve on a remote server which might be distrustful and remove the local copy of file. While provable data possession strategies have been introduce for multiple copies of static data. To principle of our understanding, this task is initially provable data possession to handle with multiple copies of dynamic data. Furthermore several authorized user can approach the remotely saved data from different geographical position creating it more appropriate for them.

II.BACKGROUND OF PROBLEM

Cloud storage has different benefit across the conventional data allocation. Suppose if you save your data on a cloud storage system you will be capable to obtain to that data taken away any position that has Internet connection. These cloud service providers are important for maintaining the data obtainable and convenience. It is critical need of client to have a powerful assurance that the cloud server exhibit their data and it is not vary or partly deleted over time. When checking multiple data copies the total system integrity observe fail if at that place there is extra spoil copies. To reference this problem and identify which copies have been spoiled we analyze a slight change to be useful to proposed system. Our contribution can be as follows. In this we are introducing multiple copies of dynamic data over the cloud. In this it ensure that cloud service provider reserve all the copies that are recognize on that commitment. It also support block level operation. We show the correctness of our system. We show problematic evaluation to explain the work of proposed system.

III.PROPOSED SYSTEM

The system consists of three main components. Data owners that can be a framework basically exhibit sensible data to be stored in the cloud. An organization that offers services to customers from a remote facility connected via the Internet. Cloud service provider that provide client storage and services facility along with public or private cloud. That is the storage and software is usable for approach by the internet. A cloud service provider which control the cloud servers (CSs) and distribute paying storing area on its framework to reserve the owner's data. Authorized users these are a format of the owners clients which have the legal to approach the remote data. As a result data owner require to be convinced that data are properly saved in the cloud. In this we are introducing ensuring transferring of multiple copies of data over cloud. It give the assurance that cloud service provider contain that all copies that are grant upon service bond. It provides the dynamic activities like as block modification, insertion, deletion, and append. We examine security of our system across the cloud server. The usage of clouds storage is performed by uploading file, multiple copies, view and delete. The file is uploaded to cloud storage for the multiple operations on the files. The file is copied to multiple cloud location for easier, effective and efficiency access or the operation on the files. The list of the file

can be viewed. In this we are using map version table that consist of serial number, block version, and block number. Exact copies permit the
Cloud service provider to directly for owner by saving single copy and assume that it saves multiple copies. Applying a easy organized method, the proposed strategy create definite copies use the expansion feature of some protected encryption system. Furthermore, the identifier should be alive of the block basis to assurance that the cloud service provider has count the new blocks at that location.

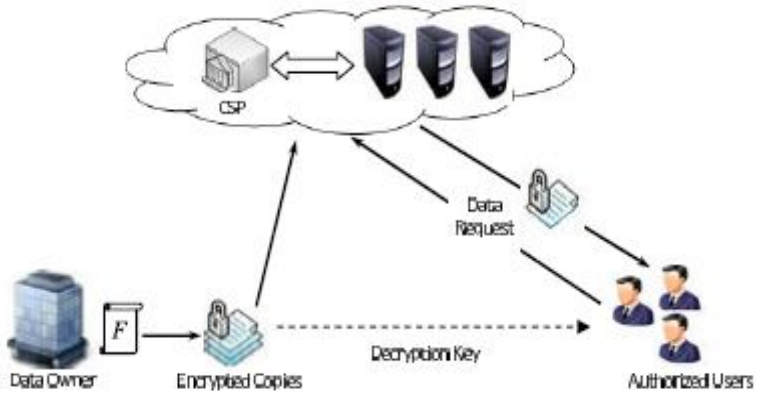

Fig. Cloud computing data storage model

III. SCOPE

The cloud storage model benefit in this system can be supported by several realistic implementations. For instance e- health application can be intended by this system where e-health structure can deal with data owner and specialist as the legal user which have licence to approach the patient's data. Many other mathematical, experimental, economical functionality can be viewed.

IV.DISADVANTAGES

When the data has been transfer to cloud service provider which may not be certainty data owner miss the direct control over their data. This absence of control causes the appalling and claiming burden to the data secret and principle assurance over the cloud. Customer can pay rent for cloud service provider framework to save and recover about unconditional extent of data. When checking multiple data copies the total structure integrity fail.

V.ADVANTAGES

Whereas provable data possession have been given for many copies of constant data, to the perfect of our ability this job is the first conformable data possession design directly attend with many copies of dynamic data. Proof for the utilization of spaces allocated. Utilization is very effective and accomplished. It assures the safety across colluding server.

VI.CONCLUSION

In this we are introducing the new provable data possession, which guides the transfer of multiple copies of dynamic data, where the data owner is able of not only extracts and admittance the data copy savings by the cloud service provider, but also restoring and scaling these copies on the remote server. To the perfect of our ability, the proposed system is the first to direct the multiple copies of dynamic data. The communication between the authorized user and cloud service provider is taking into account, where the authorized user can approach a data copy accept from the cloud service provider private key measure with the data owner. In addition, it gives public confirmable, provide random number of analysis, and allow possession free support where the authenticate has the potential to support the data integrity although he no more possesses nor restore the file block from the server. In this we have examined the issue of producing the multiple copies of dynamic data and modify those copies supply on the cloud server.

ACKNOWLEDGMENT

The very Thankful to my Family members, they helps me a lot for Collecting all relevant data which is helpful for a Survey and if Suggestion any required given were ever required. We are also thankful to Pravara Rural Engineering College for providing all the requirements at each stage.

REFERENCES

[1] R. Curtmola, O. Khan, R. Burns, and G. Ateniese, "MR-PDP: Multiple-Replica Provable Data Possession," *Proc. of ICDCS '08*, pp. 411–420, 2008.
[2] F. Seb´e, J. Domingo-Ferrer, A. Mart´ınez-Ballest´e, Y. Deswarte, J. Quisquater, "Efficient Remote Data Integrity checking in Critical Information Infrastructures", IEEE Transactions on Knowledge and Data Engineering, 20(8), pp. 1-6, 2008.
[3] C. C. Erway, A. Kupcu, C. Papamanthou, R. Tamassia, "Dynamic Provable Data Possession", CCS'09, pp. 213-222, 2009.

[4] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, "Provable data possession at untrusted stores," in *CCS '07: Proceedings of the 14th ACM Conference on Computer and Communications Security*, New York, NY, USA,2007, pp. 598–609.
[5] A. F. Barsoum and M. A. Hasan, "Provable possession and replication of data over cloud servers," Centre For Applied Cryptographic Research (CACR), University of Waterloo, Report 2010/32, 2010, http://www.cacr.math.uwaterloo.ca/techreports/2010/cacr2010-32.pdf.
[6] G. Ateniese, R. D. Pietro, L. V. Mancini, and G. Tsudik, "Scalable and efficient provable data possession,"in *SecureComm'08: Proceedings of the 4th International Conference on Security and Privacy in Communication Networks*, New York, NY, USA,2008, pp. 1–10.
[7] K. D. Bowers, A. Jules, and A. Opera, "Proofs of Retrievability: Theory and Implementation," Cryptology ePrint Archive, Report 2008/175, 2008, http://eprint.iacr.org/.
[8] D. L. G. Filho and P. S. L. M. Barreto, "Demonstrating Data Possession and Uncheatable Data Transfer," Cryptology ePrint Archive, Report 2006/150, 2006, http://eprint.iacr.org/.
[9] M. A. Shah, M. Baker, J. C. Mogul, and R. Swaminathan, "Auditing to Keep Online Storage Services Honest," *Proc. 11th USENIX Workshop on Hot Topics in Operating Systems (HOTOS '07)*, pp. 1–6, 2007.
[10] Y. Deswarte, J.-J. Quisquater, and A. Saidane, "Remote Integrity Checking," Integrity and Internal Control in Information Systems VI, pp. 1-11. Kluwer Academic Publishers, Nov. 2003
[11] C. E. Shannon, "Communication theory of secrecy systems," *Bell Syst.Tech. J.*, vol. 28, no. 4, pp. 656–715, 1949.
[12] K. D. Bowers, A. Jules, and A. Opera, "HAIL: A high-availability and integrity layer for cloud storage," in *Proc. 16th ACM Conf. Comput. Commun. Secur. (CCS)*, New York, NY, USA, 2009, pp. 187–198.
[13] C. Wang, Q. Wang, K. Ren, and W. Lou. (2009). "Ensuring data storage security in cloud computing," IACR Cryptology ePrint Archive, Tech.Rep. 2009/081.
[14] G. Ateniese, S. Kamara, and J. Katz, "Proofs of storage from homomorphic identification protocols," in *Proc. 15th Int. Conf. Theory Appl. Cryptol. Inf. Secur. (ASIACRYPT)*, Berlin, Germany, 2009, pp. 319–333.
[15] C. Martel, G. Nuckolls, P. Devanbu, M. Gertz, A. Kwong, and S. G. Stubblebine, "A general model for authenticated data structures," *Algorithmic*, vol. 39, no. 1, pp. 21–41, Jan. 2004.