# 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* - Growing many organization are opting for outsourcing data to remote cloud service provider. Customer can rent cloud service provider storage infrastructure for storing unlimited amount of data. For scalability, availability, durability certain customer may need their data replicated on several server over several data center. Moreover many copy cloud service provider is asked to store additional fees customer are charged. Thus it is important for customer to have powerful assurance that actually getting service as they paid for them. Therefore customer need strong commitment that cloud service provider store entire data copy and entire copy are consistent. We are developing MBPMDDP scheme. It provides confirmation to customer that cloud service provider is not defrauder by storing limited copied. It maintains operation like block modification, insertion, deletion, append. It provides security to our system.**

***Index Terms* – Cloud computing, outsourcing, data replication, dynamic environment**

---

## I.INTRODUCION

The advantage of cloud computing has expand quickly in several organization. Cloud computing is described as kind of computing that depends on dividing the computing resources instead of having localized server or individual equipment to manage the approach. Today numerous individual and institution transfer their data to cloud service provider. The outsourcing data to remote cloud service provider permit organization to store much data on cloud service provider than on personal computer. Additionally several authorized user can access the remotely stored data against various geographic location and creating it more suitable for them.

When data is transferred to cloud service provider that may not at all truthful, data owner lose exact control through there sensible data. This absence of control raising new formidable and difficult task associated to data confidentiality and integrity protection in cloud computing. The confidentiality problem can be treated by encrypting sensitive data since outsourcing to remote server. It is essential need of customer to have strong assurance that the cloud server still possess their data and it is not being change with or partly deleted over time.

Provable data possession (PDP) is procedure for verifying data integrity across the server. In provable data possession data owner introduced certain metadata or information for data file to be utilized afterward for verification reason across challenge-response protocol. The owner transmits the file to be stored on remote server that can be distrustful and deleted the local copy of the file. The basic design principle of outsourcing data is to produce dynamic behaviour of data for different application. That means remotely stored data could be not only access by data owner but also updated and scaled by data owner. While provable data possession strategy has been introduced for multiple copies of static data. To the principle of our understanding this is first provable data possession strategy handle with multiple copies of dynamic data. When authenticating multiple data copies the whole system integrity examine fail if there are corrupted copies. For this problem and identify which copy have been corrupted modification can be applied in this scheme.

## II.LITERATURE SURVEY

Provable data possession at untrusted store [2] In this it proposed model for provable data possession that enable a client that has stored data at untrusted server to confirm that server possesses the actual data without retrieving. It concentrated on issue of verifying server stores client data. It presents a model for provable data possession in which it is useful to reduce the file block approach, computation on the server and client –server communication. Data possession and uncheatable data transfer [5] It defines a protocol depends on hash function which avoids cheating in a data transfer transaction while allocating little burden on trusted third party that controls the protocol. It also specify a cryptographic protocol based on this principle, along which prover can demonstrate possession of arbitrary set of data known to the prover.Efficient remote data possession checking in critical information infrastructures [6] It introduced a new remote data possession checking protocol it permit an unlimited number of file integrity verification and its maximal running time can be select at set-up time and traded off across storage at verifier. Remote data possession checking protocol allow examining that a remote server can approach uncorrupted file in such manner that the verifier does not want to realize before all file is being checked. Scalable and efficient provable data possession [11] this scheme is to provide integrity of outsourced data in multi-cloud environments. To accomplish this it building the use of ranking and confirmable responds. This is built on idea of zero knowledge interactive proof system that can avoid different attacks over cloud. Dynamic provable data possession [13] it represents definitional framework structure and effective construction for dynamic provable data possession, which expand the PDP model to keep provable update to stored data. It manage a new category of authenticated dictionaries establish on rank information.

## III.PROPOSED SYSTEM

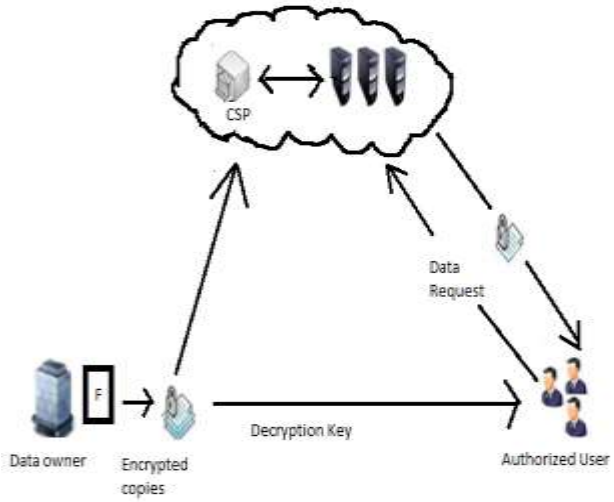



**Fig.System Architecture**

The system consist of data owner, cloud service provider, authorized user. Data owner can be organization basically exhibit sensitive data to be store in cloud. Cloud service provider which control cloud server and distribute paid storing area on its framework to store owner's file. Authorize user these are group of owner's client which is desirable to obtain information. This system framework accepted by many experimental implementations. To give an example such as e-Health application can be considered by this model where patient database that involve huge and sensitive data can be stored on cloud server. In this e-Health organization examined as data owner and physician as authorized user which have right to acquire patient medical record. It depends on handling small data structure called map-version table. Map-version table consists of three columns serial number (SN), block number (BN) and the block version (BV).The SN indicate the physical location of block in data file. The BN indicate logical indexing/numbering. The relationship between serial number and block number can be considered as mapping among logical number and physical position. The BV indicates current version of file blocks. Although data file is at beginning created block version of all block is 1. When certain block is updated block version is increased by 1.

## IV.IMPLEMENTATION DETAILS

This scheme consists of following steps:

Key generation: The data owner runs the keyGen algorithm to produce private key and public key.

Formation of Discrete copy: The file F= {bj}, the data owner execute the CopyGengeration algorithm to build n distinguishable copies F= {Fi}, where copy F= {bij}.The encrypted block bij is divided into s sectors. The authorized user require only to store single secret key k.Later when authorized user collect copy from cloud service provider he decrypt the file block, remove the copy index from blocks and recombined the decrypted block to recreate plain form of the receive file copy.

Formation of tags: Given the distinct file copies F= {Fi}, the data owner select s random element and runs the TagGen algorithm to create tag for each block bij.To minimize the storage burden on the server and interaction value, owner create tags for block at similar indices in every copy Fi.

Dynamic operation: These operations execute at block stage bi by using request. The block operation corresponds to block modification, block insertion, block deletion, block append. Changes in map-version table because of several operation on copy of file F. Preventing the cloud service provider from defraud and applying limited store, the updated or insertion blocks for transferred not either similar.

Challenge: Since challenging the cloud service provider as well as verifying the integrity and consistency of all copy, verifier transmits copy and two keys at every challenge key k1 and key k2.

Response: The cloud service provider executes the Prove method to create set Q of random indexes and values. Cloud service provider still exactly possesses the n copies in an updated and uniform. The cloud service provider replies with proof P.

Check Response: On getting the confirmation through cloud service provider verifier runs the verify algorithm. The verifier manages value of indexes and map-version table to obtain the logical block BNj and BVj.

## V.ALGORITHM

### HASH Algorithm

1. Initialize some variable.
2. Pick a string.
3. Break it into characters.
4. Convert character to ASCII code.
5. Convert numbers into binary.
6. Add '1'to end
7. Append '0' to end
8. Append original message length.
9. Chunk the message.

10. Break the chunk into words.
11. Extend into 80 words.
12. XOR
13. Left rotate.
14. Initialize some variable such as A=ho, B = h1, C = h2, D = h3, E = h4 and. main loop perform.
15. Four choices and put them together and it converted into hex and joined together.

**SHA (Secure hash Algorithm)**
1. Append padding bits.
2. Append length.
3. Prepare processing function.
4. Prepare processing constant.
5. Initialize Buffer.
6. Processing message in 512-bit blocks.

**VI.RESULTS**
Result Snapshot

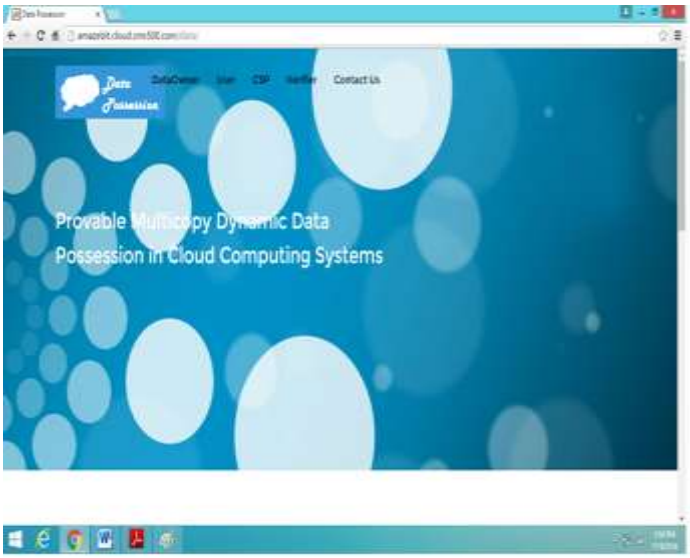



**Fig.Homepage**

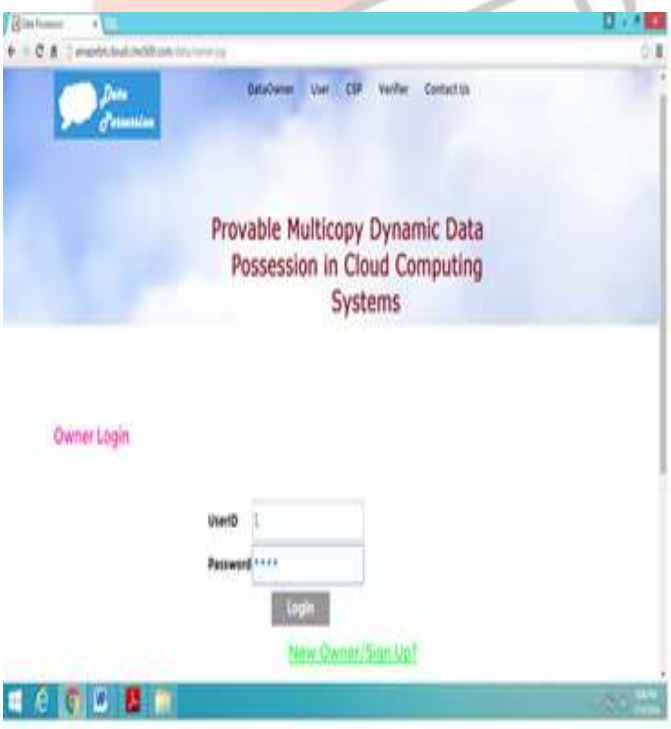



**Fig.Owner login**


**Fig.File Upload**


**Fig.Auditing**

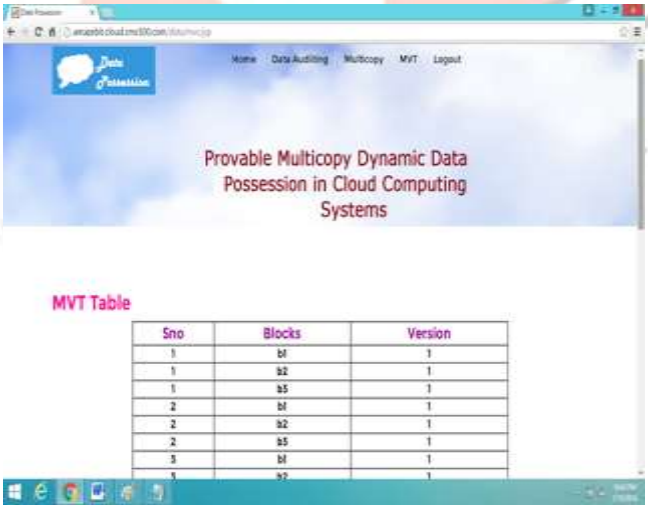
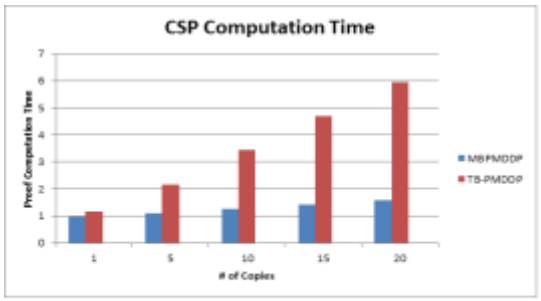



**Fig MVT**

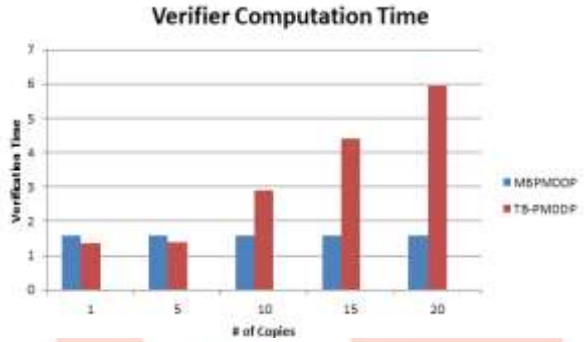
CSP Computation Time

| # of Copies | MB-PMDDP | TB-PMDDP |
|---|---|---|
| 1 | 0.9616 | 1.178 |
| 5 | 1.093 | 2.152 |
| 10 | 1.259 | 3.434 |
| 15 | 1.425 | 4.687 |
| 20 | 1.591 | 5.941 |



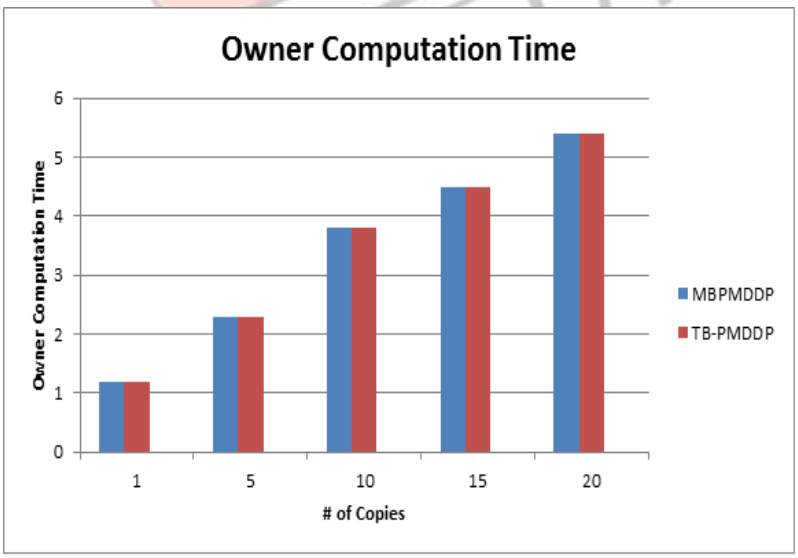

Verifier Computation Time

| # of Copies | MB-PMDDP | TB-PMDDP |
|---|---|---|
| 1 | 1.57528 | 1.3575 |
| 5 | 1.57534 | 1.3951 |
| 10 | 1.57543 | 2.8883 |
| 15 | 1.57553 | 4.4197 |
| 20 | 1.57562 | 5.951 |




Owner Computation Time

| # of Copies | MB-PMDDP | TB-PMDDP |
|---|---|---|
| 1 | 1.2012 | 1.2013 |
| 5 | 2.359 | 2.361 |
| 10 | 3.818 | 3.821 |
| 15 | 4.525 | 4.528 |
| 20 | 5.448 | 5.452 |




**VI.CONCLUSION**

We conclude that the issue of producing multiple copies of dynamic data and validating those copies stored on untrusted cloud server. We proposed new provable data possession which provide outsourcing of multiple copies of dynamic data, where data owner is suitable of not only archive and access data copies keep by cloud service provider but also modify and scale those copies on server. To principle of our understanding, this scheme is to address multiple copies of dynamic data. The communication

between authorized user and cloud service provider is taking into account, where authorized user can access data copy accept from CSP using separate key distribute with data owner. It maintains the feature of determining indices of corrupted copies.

**VII.ACKNOWLEDGMENT**

First and the foremost I, express my deep sense of gratitude, sincere thanks and deep sense of appreciation to my Project Guide Prof.N.B.Kadu, Department of Computer Engineering, Pravara Rural Engineering College, Loni for his precious and helpful guidance. I would also like to thank Prof.K.R.Pathak, P.G. Coordinator for his great understanding and support.

I am sincerely thankful to my H.O.D., Prof. S. D. Jondhale, Department of Computer Engineering for the systematic guidance and providing necessary facilities and the best support I ever had. Your opinion, views, comments and thoughts have really brought meaning to my hard-work. I would like to express my sincere gratitude to Dr. R.S. Jahagirdar, Principal, Pravara Rural Engineering College, Loni for providing a great platform to complete the thesis within scheduled time.

**REFERENCES**

[1] AyadF.Barsoum and M.Anwar Hasan, Provable Multicopy Dynamic Data possession in Cloud Computing System,pp.485-497,2015.

[2] G. Ateniese et al., Provable data possession at untrusted stores, in Proc. 14th ACM Conf. Comput. Commun. Secur.(CCS), New York, NY, USA, 2007, pp. 598609.

[3] K. Zeng, Publicly verifiable remote data integrity, in Proc.10th Int.Conf. Inf. Commun. Secur. (ICICS), 2008, pp.419434.

[4] Y. Deswarte, J.-J. Quisquater, and A. Sadane, Remote integrity checking, in Proc. 6thWorking Conf. Integr. Internal Control Inf.Syst. (IICIS), 2003, pp. 111.

[5] D. L. G. Filho and P. S. L. M. Barreto, Demonstrating data possession and uncheatable data transfer,IACR (International Association for Cryptologic Research) ePrint Archive, Tech. Rep. 2006/150, 2006.

[6] F. Seb, J. Domingo-Ferrer, A. Martinez-Balleste, Y.Deswarte, and J.-J. Quisquater, Efficient remote data possession checking in critical information infrastructures,IEEE Trans. Knowl. Data Eng., vol. 20, no. 8, pp. 10341038,Aug. 2008.

[7] P. Golle, S. Jarecki, and I. Mironov, Cryptographic primitives enforcing communication and storage complexity, in Proc. 6th Int. Conf. Financial Cryptograph. (FC), Berlin, Germany, 2003, pp. 120135.

[8] M. A. Shah, M. Baker, J. C. Mogul, and R. Swaminathan, Auditing to keep online storage services honest, in Proc.11th USENIX Workshop Hot Topics Oper. Syst. (HOTOS),Berkeley, CA, USA, 2007, pp. 16.

[9] M. A. Shah, R. Swaminathan, and M. Baker, Privacy preserving audit and extraction of digital contents, IACRCryptology ePrint Archive, Tech. Rep. 2008/186, 2008.

[10] E. Mykletun, M. Narasimha, and G. Tsudik, Authentication and integrity in outsourced databases, ACM Trans.Storage, vol. 2, no. 2, pp. 107138, 2006.

[11] G. Ateniese, R. D. Pietro, L. V. Mancini, and G. Tsudik,Scalable and efficient provable data possession, in Proc. 4thInt. Conf. Secur.Privacy Commun. Netw. (SecureComm),New York, NY, USA, 2008,Art. ID 9.

[12] 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. [Online].Available: http://eprint.iacr.org/

[13] C. Erway, A. Kp, C. Papamanthou, and R. Tamassia, Dynamic provable data possession, in Proc. 16th ACM Conf.Comput. Commun.Secur. (CCS), New York, NY, USA, 2009,pp. 213222.