International Journal of Research
Available at https://edupediapublications.org/journals
p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 03 Issue 11
July2016

A Survey on Provable Multicopy Dynamic Data Possession in Cloud Computing Systems

[1]D.SRILATHA, [2] Mrs.N.SUJATHA

[1] M.Tech(CSE) from JAGRUTI INSTITUTE OF ENGINEERING AND TECHNOLOGY

[2] Associate Professor, Department of Computer Science and Engineering, JAGRUTI INSTITUTE OF ENGINEERING AND TECHNOLOGY, Telangana State, India

ABSTRACT:

In Recent survey on cloud computing tolerate most of data owners worrying whether there data secure in cloud or not and data provides acting according to SLA or not, in order to resolve above issues in cloud the Cloud provider offering MCDDPDS (multi copy dynamic data possession State), Using this MCDDPDS the data user can know the status of data whether his data is secure or not and if any violations are done by others then it gives alert to the data user. The data owner will outsource his data to the could in order minimize local burden and to save the cost , In order to provide security the data owner before outsourcing he has to encrypt and upload to the cloud but due to security threat and loss of data the data owner outsourcing same copy into multiple servers and later whenever he need any dynamics on his data he can do like updating , deleting and appending .

Keywords: Provable data possession (PDP), MCDDPDS, Data Integrity, Multi copy.

Introduction:

Cloud allows to outsource more data remotely and access from any ware .The cloud provide offering services like Iaas,Paas and Saas using these services the data user can use cloud without having his own servers he can use cloud as pay per use . The PDP scheme allows user to check integrity of data on cloud without downloading entire data from cloud , before PDP model the data owner need download data from cloud and he has to check data integrity but this leads big communication burden to the data owner in order to avoid this issue the cloud allows PDP scheme using this scheme the owner can check integrity of data.

In remote data integrity checking protocols, the client can challenge the server about the integrity of a certain data file, and the server

generates responses proving that it has access to the complete and uncorrupted data. The basic requirements are that the client does not need to access the complete original data file when performing the verification of data integrity, and that the client should be able to verify integrity for an unlimited number of times.

An increasing number of clients organization use cloud to store data which has become trend [1]. Cloud service provider (CSP) allows storing much more data than private computer. Once data stored in remote server, authorizer can access all data from any geographical location. Most of the time organization store important data in cloud, without leaving a copy in local computer. Once data is stored in cloud they may not be trustworthy due to losing control on data. So, it is important to ensure data is not lost or corrupted by checking data integrity. In data integrity checking, client challenge remote server and server response by proving that. Many researchers have focused on this problem and find out different technics. PDP is one of the techniques for validating data integrity. In this model, do not need to store all file to local computer to check data integrity. It creates metadata information of each file and that store it in local computer without storing whole file. At the time of verification of data integrity it sends the metadata to the verifier side. PDP model used both static data and dynamic data.

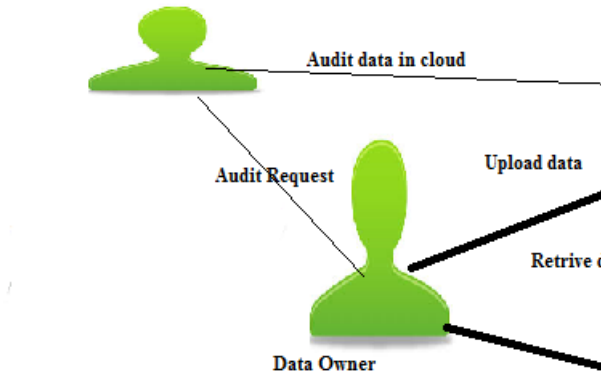
II. RELATED WORK

Ateniese et al. [2] are the first to consider public auditability in their de fined "provable data possession"(PDP) model for ensuring possession of data files on untrusted storages. Their scheme utilizes the RSA-based homomorphic linear authenticators for auditing outsourced data and suggests randomly sampling a few blocks of the file. However, the public auditability in their scheme demands the linear combination of sampled blocks exposed to external auditor. When used directly, their protocol is not provably privacy preserving, and thus may leak user data information to the auditor. Roberto Di Pietro [9] propose a partially dynamic operation like block modification , deletion and append of the prior PDP scheme, using only symmetric key cryptography but with a bounded number of audits. Also, it is unsuitable for public verifiability. Curtmola et al. [10] propose a multiple replica PDP (MR-PDP) which ensures that multiple replicas of the client's data are stored at the cloud storage server, so that the data availability is improved. It can generate further replicas on demand, at little expense, when some of the existing replicas fail. It is not efficient as we would like for integrity issue. Ayad F. Barsoum and M. Anwar HAsan [14] provide a multi-copy dynamic data possession. It provides evidence to customer that CSP store all copies. Also, it support full block level dynamic

International Journal of Research
Available at https://edupediapublications.org/journals
p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 03 Issue 11
July2016

operation by data owner using map version table and allow authorized user seamlessly access data and finally, discussed about to identified list of the corrupted copies.

Proposed System:



To overcome existing problems in this paper proposing new model called MCDDPDS (multi copy dynamic data possession State) ,the Cloud service provider offers to the data owner without downloading entire data from cloud , the data owner can check data integrity in the cloud.

The architecture contains four entities 1. Data Owner 2. Data User 3. Auditor 4. Cloud

1. **Data owner:** data owner outsource his sensitive data to the cloud and in order to protect his data from others he will encrypt the data before outsourcing and whenever he need data integrity he send request to the auditor. And auditor will send auditing result , based on the result data owner check his data integrity.
2. **Data User:** Data user download the file from cloud and if he want to decrypt the file then he has to get the key from corresponding data owner.
3. **Auditor:** auditor will take the audit request from data owner; based on his request the auditor will check integrity of the data in cloud. And auditing result will send to the data owner.
4. **Cloud:** Cloud service provider provides to the data owner storage as service in order to save their data in cloud.

REFERENCES:

[1]. R. Buyya, C.S. Yeo, S.Venugopal, J. Broberg , and I. Brandic, “Cloud computing and emerging IT platforms”, Future generation computer system, vol. 25, no. 6, pp. 599-616, 2009.

[2]. Giuseppe Ateniese, Randal Burns,RezaCurtmola, Joseph Herring, LeaKissner, Zachary Peterson, and Dawn Song, "Provable data possession at untrusted stores", in Proceedings of the 14th ACM Conference on Computer and communications security, Oct 2007.

[3]. F. Sebé, 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. 1034–1038, Aug. 2008

[4]. Giuseppe Ateniese, Roberto Di Pietro, Luigi V.Mancini and Gene Tsudik, "Scalable and Efficient Provable Data Possession", in Proceedings of the 4th international conference on Security and privacy in communication, 2008.

[5] F. Sebé, 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. 1034–1038, Aug. 2008.

[6] 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. 120–135.

[7] 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. 1–6.

[8] M. A. Shah, R. Swaminathan, and M. Baker, "Privacy-preserving audit and extraction of digital contents," IACR Cryptology ePrint Archive, Tech. Rep. 2008/186, 2008.

[9] E. Mykletun, M. Narasimha, and G. Tsudik, "Authentication and integrity in outsourced databases," ACM Trans. Storage, vol. 2, no. 2, pp. 107–138, 2006.

D.SRILATHA is pursuing M.Tech degree in, Computer Science and Engineering from Jagruti Institute of Engineering and Technology, Telangana State, India.

Mrs.N.SUJATHA is presently working as Associate Professor in, Department of computer science and engineering, Telangana State,India.She has published several research papers in both International and National conferences and Journals.