IJRRECS/July 2014/Volume-2/Issue-7/2758-2761 **ISSN 2321-5461**

INTERNATIONAL JOURNAL OF REVIEWS ON RECENT ELECTRONICS AND COMPUTER SCIENCE

MAINTAINING OF STABLE DATA SERVICES IN CLOUD PARADIGM

Thota Nareshkumar[1], B.Dhanalakshmi[2]

[1]M.Tech Student, Dept of CSE, Aurora's Scientific And Technological Institute, Aushapur(V), Ghatkesar(M), R.R Dist, T.S, India

[2]Assistant Professor, Dept of CSE, Aurora's Scientific And Technological Institute, Aushapur(V), Ghatkesar(M), R.R Dist, T.S, India

ABSTRACT:

In this paper a new technique is proposed by the modern mechanism of the auditing of the storage based distribution in which utilization of token similarity and coded data distribution respectively. In this method auditing of the user data takes place with a reduced cost of computation followed by the flexible complexity. The effective outcome of the above process orientation of the system result in the accurate storage in the cloud followed by the localization of the data error in an analogous fashion respectively. Error of the data takes place is nothing but the server misbehavior and its identification. In the improvement in the technology enables the access of the data from the storage of cloud by the user in a remote oriented fashion in which there is a reduction in the complexity of the form hardware followed by the managing software is got nullified by the advancement in the new technology by the name of the cloud. Here the preparation is up to the mark as pr the choice of the user and their benefits. But there is a major problem from the clients of the user end they are worried about the trust and is a major concern. If the newly developed system overcome the problem then it will become one of the best technology in terms of the service provision relative to the user. Experiments have been conducted on the present method where evaluations takes place on the large number of the datasets under which performance of the proposed method is evaluated in a well accurate manner respectively.

Keywords: Storage dependence, Integrity, Dynamics, Localization, Identification of error, Data distribution, Service provision, Cloud elasticity and explicit knowledge respectively.

1. INTRODUCTION:

Due to the innovative and the advancement in the technology of the cloud the complete burden of the user is nullified and the burden includes hardware complexity is under the complete control of the cloud. There are some of the vendors in this provision of the services includes the amazon.com, salesforce.com, service storage of Amazon and elastic computation of Amazon respectively [1]. These new technology provides the services of the storage and provision for the accessing of the efficient resources. There is a flexibility in the integration of the data followed by the provision of the services. Compared to the devices of the computation he infrastructure of the cloud is more powerful by the existence of the threats relative to the factors of the internal and externalities of integration plays a crucial role respectively. Here the infrastructure of the cloud is very much powerful and well oriented with the devices of the personal computations and its reliability respectively [2][3]. Here there is a complete protection of the data of the user in terms of the manipulation and other errors followed by the privacy is maintained in a well efficient manner respectively. As compared to the previous methods there are a lot of problems relative to the service provider of the cloud in an unfaithful manner respectively.

BLOCK DIAGRAM

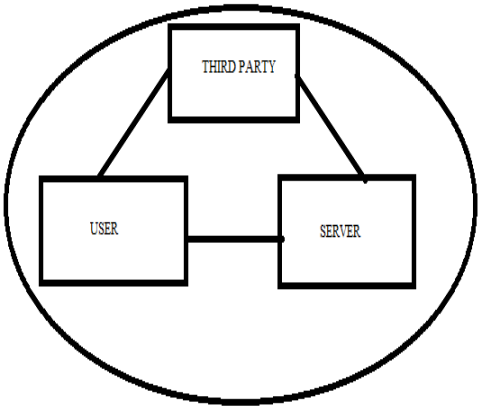

Fig 1: Shows the block diagram of the present method respectively

2. METHODOLOGY:

In this paper a detailed architecture is designed for the service storage based on the cloud. For the purpose of identification the different network entities are placed in the system. And the entities includes third party,

server of the cloud and user respectively. For the efficient storage of the data on cloud by the user mainly dependent on the service oriented computations respectively [4]. Here the cloud based provision of the service takes place by the help of the service provider involvement includes the storage space and its significance followed by the resource computation respectively. Here mainly up to this there is no problem for the user to storage of the data but they are mainly concerned about the trust based privacy of the data is a major concern respectively. So in order to overcome this problem a new mechanism is implemented by the help of the design of the TPA (auditor of the third party) here the decentralization plays a crucial role in which there is provided with a huge protection for the data of the user in a well oriented fashion respectively [6][7]. Here in the system is implemented in the structure of the matrix layout and that too in a systematic fashion by which there is a provision for the downloaded data reconstruction from m number of the servers respectively. Here the implementation of the proposed method is shown in the above figure in the form of the block diagram and is illustrated in the descriptive fashion respectively.

3. EXPECTED RESULTS:

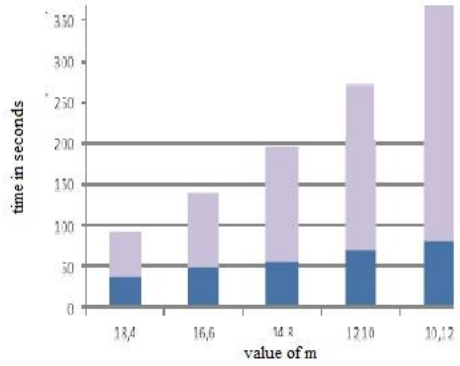

Fig 2: Shows the graphical representation of the present method respectively

The performance of the present method is shown is the above graphical representation in which there is a comparison takes place between the present method and the several previous methods by which it completely analyses the drawbacks of the several previous methods in a well oriented fashion and overcome the problems of the previous methods in the present method where there is a complete improvement in the performance of the system. Here in the process of the proposed method where the mechanism of the strategy of the auditing mainly concentrates on the distribution of the file preparation followed by the generation of the tokens respectively. In the preparation of the distribution of the file includes the scenario of the parity vector

generation followed by the blind parity structure respectively [8][9]. Here the experiments have been conducted on the different number of the datasets and analysis of the performance takes place on the data sets where the performance are related to the data sharing strategy respectively.

4. CONCLUSION:

In this paper a new technique is presented related to the concern of the security of the data related to the cloud plays a crucial role and it is one of the major problem by which the users are very much frustrated about their data stored in the cloud and followed by the aspects of the privacy plays a crucial role respectively. So due to this for the proper maintenance of the integrity followed by the quality oriented service a new technique or the mechanism is implemented in a well efficient fashion oriented with a distributed scheme under the support of the explicit data respectively. Here the data oriented with the strategy of the explicit scenario includes the append, delete and the updating of the data takes place effectively. Here we are completely dependent upon the code correction erasure for the preparation of the distributed file of the parity vector provision and maintenance of the redundancy.

REFERENCES

[1] A. Juels and J. Burton S. Kaliski, "Pors: Proofs of retrievability for large files," in Proc. of CCS'07, Alexandria, VA, October 2007, pp. 584–597.

[2] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, "Provable data possession at untrusted stores," in Proc. of CCS'07, Alexandria, VA, October 2007, pp. 598–609.

[3] M. A. Shah, M. Baker, J. C. Mogul, and R. Swaminathan, "Auditing to keep online storage services honest," in Proc. of HotOS'07. Berkeley, CA, USA: USENIX Association, 2007, pp. 1–6.

[4] M. A. Shah, R. Swaminathan, and M. Baker, "Privacy-preserving audit and extraction of digital contents," Cryptology ePrint Archive, Report 2008/186, 2008, http://eprint.iacr.org/.

[5] G. Ateniese, R. D. Pietro, L. V. Mancini, and G. Tsudik, "Scalable and efficient provable data possession," in Proc. of SecureComm'08, 2008, pp. 1–10.

[6] Q. Wang, C. Wang, J. Li, K. Ren, and W. Lou, "Enabling public verifiability and data dynamics for storage security in cloud computing," in Proc. of ESORICS'09, volume 5789 of LNCS. Springer- Verlag, Sep. 2009, pp. 355–370.

[7] C. Erway, A. Kupcu, C. Papamanthou, and R. Tamassia, "Dynamic provable data possession," in Proc. of CCS'09, 2009, pp. 213–222.

[8] H. Shacham and B. Waters, "Compact proofs of retrievability," in Proc. of Asiacrypt'08, volume 5350 of LNCS, 2008, pp. 90–107.

[9] K. D. Bowers, A. Juels, and A. Oprea, "Proofs of retrievability: Theory and implementation," in Proc. of ACM workshop on Cloud Computing security (CCSW'09), 2009, pp. 43–54.

[10] R. Curtmola, O. Khan, R. Burns, and G. Ateniese, "Mr-pdp: Multiple-replica provable data possession," in Proc. of ICDCS'08. IEEE Computer Society, 2008, pp. 411–420.