



SHARING OF DATA BY ACCOUNTABILITY DISTRIBUTION ON CLOUD BASED STRATEGY

Taj Mohammad Khan¹, K.Rakesh²

¹M.Tech Student, Dept of CSE, Jayaprakash Narayan College of Engineering, Mahaboobnagar, A.P, India

²Associate Professor, Dept of CSE, Jayaprakash Narayan College of Engineering, Mahaboobnagar, A.P, India

ABSTRACT--Internet plays a vital role in the society. Services based on the internet which plays a major role in the human based perspective in the form of the cloud based aspect in a respective fashion. Now a day there are many of the people are getting attracted towards the services based cloud in a respective fashion. There the services based on the cloud are reliable and quite effective in terms of the performance based aspect. Here the complete services are based on the wireless scenario. Where there are a large number of the services where some of them includes software, Infrastructure, and followed by the platform based strategy in a well respective fashion. Here there the services based on the internet based strategy are very much effective and it is also provided with a user friendly environment in a respective fashion. Where the access of the system takes place by the direct access based on the sensitivity of the remote oriented strategy in a automatic fashion without any interference of the user in a well respective fashion. This a lot of advancement in the system takes place where they can the system in a well easy oriented fashion but the main thing is transfer of the data takes place in a wireless based environment in respective fashion. Therefore there is a major problem arise in the system which is related to the privacy oriented phenomena in a respective fashion takes place. So here the system are designed where the privacy oriented assurance has to be provided to the public that they trust the system in a well effective manner. Where the continuous monitoring of the system with respect to the user based strategy in a well respective fashion takes place. Here a method is designed based on the decentralization oriented phenomena where enables the structure oriented with respect to the logging based strategy followed by the policies followed by the structure of the data in a well oriented fashion. Here the control of the strategy takes place by the help of the JAR based phenomena which is mainly for the programming based phenomena in a well respective fashion. Here further a mechanism is implemented for the even more strengthening of the data in a well

respective fashion. Experiments have been conducted on the present method where accurate analysis of the performance takes place in a well efficient fashion respectively. Keywords: Computation based cloud, Database, Sharing data, Accountability, Authentication of the data, Effective measure

I. INTRODUCTION

Interaction of the data plays a vital role for the effective analysis of the data based on the internet oriented strategy based on the efficient fashion. Here in the above phenomena there the internet plays a vital role for the transfer of the data in a well effective manner [1]. Here there is advancement in the system takes place in a well effective fashion where the data are stored in the server oriented fashion with respect only one cloud based scenario takes place. But this is a huge problem whenever there is a requirement of the large amount of the data storage based scenario.

Therefore a cloud of cloud is used where there is an interconnection takes place between one another in a well respective fashion. Where they are connected to one another by the help of help of the cloud based aspect where they all are connected to the third party based oriented strategy in a well respective fashion [2][3]. Here the main problem is due to the wireless oriented phenomena followed by the decentralization based phenomena. Where the data of the user is got stored in the database of the server oriented third party based strategy where the user or the demand of the query is very much concern about the privacy aspects of the data of their own [2][5]. Here security plays a major role where the effective protection has to be given by the system where the complete trust based phenomena of the user has to be done. That is here the system completely takes the burden of the user who ever is storing the data in the cloud based environment in a well respective fashion.

II. METHODOLOGY

In this method a system is designed with a well effective algorithm oriented strategy where it completely overcome the drawbacks of the previous existing techniques in an efficient manner [6]. Here it is designed with a particular framework which must effective and efficient in terms of the performance of the system based strategy followed by the accurate analysis respectively. There is a huge challenge for the present method where in order to over the trust oriented factor apart from the assurance based strategy followed by the privacy as a major concern in the system. Here the present method is explained by the below figure in a fashion of the block diagram based representation oriented strategy which elaborates the system in a well efficient manner [7][8]. In the method we are going to implement the algorithm based on the framework of the CIA based phenomena in a well respective fashion based on the information oriented accountability based framework oriented strategy in a well respective fashion. Here mainly the present algorithm is concerned about the auditing based strategy which is efficient in terms of the security based analysis where the privacy is a major concern related to the issue of the user and also logging in a well automated fashion. CIA oriented phenomena is broadly classified into two major parts they are harmonizer log followed by the log in an well efficient manner [9][10][11]. Where the complete access of the data takes place by the help of the identification number followed by the effective password in a well respective fashion. Therefore the system directly provides the access to the user based on the demand of of the accurate identification number followed by the particular password in a respective fashion where the accurate accessing of their own information in a well respective fashion. Therefore we finally conclude that the present method is effective and efficient in terms of the evaluation of the performance takes place and in the accurate oriented strategy [12][13].

III. BLOCK DIAGRAM

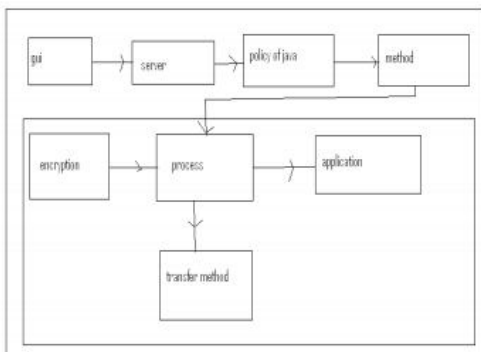


Figure:1 Shows Sharing of Data in Cloud

IV. EXPECTED RESULTS

A lot of analysis has been made on the present system. Where a large number of the experiments have been conducted with a number of the data sets oriented aspect in a well respective fashion. Here the present method completely overcome the drawback of the previous existing techniques in a well respective fashion. Here the comparison of the present method to that of the existing methods are displayed in the below graphical representation in a respective fashion. It completely overcome the huge challenge which was bought from the problem oriented aspect to the previous methods in a respective fashion. Here the main aspect of the user oriented strategy is the privacy towards the data of the user plays a vital role for the effective implementation followed by the trust oriented phenomena which is mainly essential for the development of the business oriented strategy in a well respective fashion

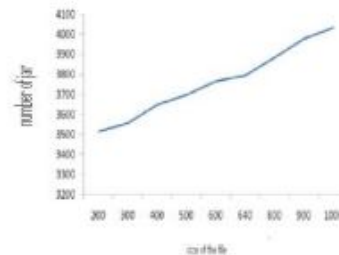


Figure:2 shows the graphical representation of component based logger size respectively

V. CONCLUSION

In this paper a method is designed with a particular framework oriented strategy where the present method is involved in the effective and efficient implementation of the performance based strategy. Here the accurate sharing of the data takes place. Where each and every cloud are interconnected to one another in a well oriented fashion. Here each and every cloud are independent of each other but all of them are relies on the third party oriented phenomena where the decentralization strategy takes place in a well efficient manner. Here we finally conclude that the present method where the data of the user is protected in a efficient manner for the improving of the performance of the system.

VI. REFERENCES

[1] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, "Provable Data Possession at Untrusted Stores," Proc. ACM Conf. Computer and Comm. Security, pp. 598- 609, 2007.



- [2] R. Bose and J. Frew, "Lineage Retrieval for Scientific Data Processing: A Survey," *ACM Computing Surveys*, vol. 37, pp. 1- 28, Mar. 2005.
- [3] B. Chun and A.C. Bavier, "Decentralized Trust Management and Accountability in Federated Systems," *Proc. Ann. Hawaii Int'l Conf. System Sciences (HICSS)*, 2004.
- [4] D. Boneh and M.K. Franklin, "Identity-Based Encryption from the Weil Pairing," *Proc. Int'l Cryptology Conf. Advances in Cryptology*, pp. 213-229, 2001.
- [5] E. Barka and A. Lakas, "Integrating Usage Control with SIP-Based Communications," *J. Computer Systems, Networks, and Comm.*, vol. 2008, pp. 1-8, 2008.
- [6] P.T. Jaeger, J. Lin, and J.M. Grimes, "Cloud Computing and Information Policy: Computing in a Policy Cloud?," *J. Information Technology and Politics*, vol. 5, no. 3, pp. 269-283, 2009.
- [7] W. Lee, A. Cinzia Squicciarini, and E. Bertino, "The Design and Evaluation of Accountable Grid Computing System," *Proc. 29th IEEE Int'l Conf. Distributed Computing Systems (ICDCS '09)*, pp. 145-154, 2009.
- [8] R. Jagadeesan, A. Jeffrey, C. Pitcher, and J. Riely, "Towards a Theory of Accountability and Audit," *Proc. 14th European Conf. Research in Computer Security (ESORICS)*, pp. 152-167, 2009.
- [9] J.W. Holford, W.J. Caelli, and A.W. Rhodes, "Using Self-Defending Objects to Develop Security Aware Applications in Java," *Proc. 27th Australasian Conf. Computer Science*, vol. 26, pp. 341-349, 2004.
- [10] R. Hasan, R. Sion, and M. Winslett, "The Case of the Fake Picasso: Preventing History Forgery with Secure Provenance," *Proc. Seventh Conf. File and Storage Technologies*, pp. 1-14, 2009.
- [11] X. Feng, Z. Ni, Z. Shao, and Y. Guo, "An Open Framework for Foundational Proof-Carrying Code," *Proc. ACM SIGPLAN Int'l Workshop Types in Languages Design and Implementation*, pp. 67-78, 2007.
- [12] S. Etalle and W.H. Winsborough, "A Posteriori Compliance Control," *SACMAT '07: Proc. 12th ACM Symp. Access Control Models and Technologies*, pp. 11-20, 2007.
- [13] Y. Chen et al., "Oblivious Hashing: A Stealthy Software Integrity Verification Primitive," *Proc. Int'l Workshop Information Hiding*, F. Petitcolas, ed., pp. 400-414, 2003.