IJRRECS/July 2014/Volume-2/Issue-7/2698-2702 **ISSN 2321-5461**

INTERNATIONAL JOURNAL OF REVIEWS ON RECENT ELECTRONICS AND COMPUTER SCIENCE

MANAGING OF DATA STABILITY CONCERNING CLOUD USER

Kambham Naveen Kumar[1], Ms.Sri Lakshmi[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 the rapid advancement in the technology of the system based architecture related to the scenario of field of IT under which cost reduction factor plays a crucial role in its applications in a well oriented fashion respectively. Here for the newly established company there the cost factor plays a crucial role for the upgrading of the hardware followed by the software and it is impossible as well as a heavy task and we can simply call as out of bounds respectively. So here the advancement of the internet in the form of computation of the cloud plays a crucial role and it is very much helpful for the newly started companies in terms of the provision of the proper services in the form of the data storage, infrastructure and portability respectively. Here these services are provided mainly on the strategy of pay per use model and the amount is different or in the varies fashion. There are two types of services involved in it they are the public followed by the private. Here the utilization of the services from the cloud by the help of the companies are on the private basis that is mainly on the commercial aspect respectively. Here the cloud has a very advanced technology in which decentralization plays a crucial role for the storage of the data. Then there is a provision of the accessibility of the data by the user and the services I the form of the hardware followed by the software involved in it respectively. Experiments have been conducted on the present method where it is implemented on the large number of

the test beds to order to verify the accuracy of the system's performance related to the evolution of the entire outcome respectively.

KEYWORDS: Data integrity, Data storage, Information technology, Query of the user, Data query, Data retrieval, Data authentication, Data verification, Accessibility of the data, Retrieval proof, Data reinforcement and data verification respectively.

1. INTRODUCTION:

Nowadays clients preferring reduced complexity in the user end that is the modules they are using is simple where there is no chance for the storage of the complex data. Therefore the that sought of the customer is completely reliable on the services of the advancement of the internet that is the cloud based operations respectively [1]. Here apart from the clients of the individual aspect many of the newly started companies are also completely relied on the entire services of the cloud in the form of the software accessibility, data storage and also the portability of the network in the form of the pay per use model in a well oriented fashion respectively [2][3]. Therefore the data of the user is completely protected and under the control of the client where there is a trust maintenance and the privacy is a major concern respectively.

BLOCK DIAGRAM

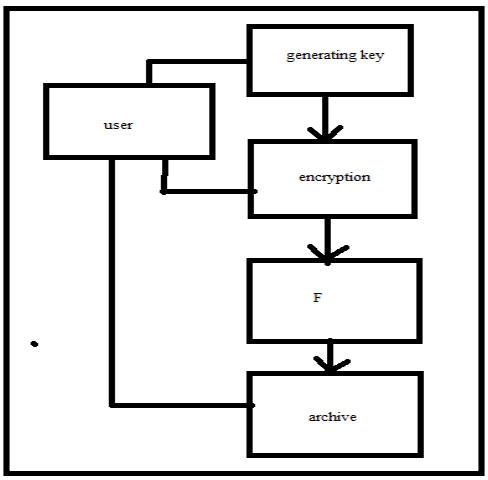

Fig 1: Shows the block diagram of the present method respectively

Fig 2: Shows the encryption of the data mechanism respectively

2. METHODOLOGY:

Here a new technique is proposed where it works n the scenario of the well efficient control complexity of the data included from the large number of the users and providing the privacy is a major concern. Providing the privacy is nothing but the maintenance of the trust among the user in which advanced algorithm is used for the data encryption strategy that is an cryptography is used [4][5]. By which there would be no loss of the data at the time of the encryption and the decryption in a well desired fashion respectively. Here the encryption followed by the proper analysis based aspect in which overhead complexity must be reduced among the different data of the users that is in the terms of the reliability respectively. There should be a minimization of the data overhead of the user and the maintenance is of the form of the clients under the basis of the thin strategy. Here the protocol is designed in a well effective fashion for the maintenance of the integrity of the data and a followed key is used for the purpose of the secret storage in which privacy is a major concern respectively [6][7]. Here there is an automatic generation of the secret code in the form of the key that are generated from the sample of the random scenario respectively. Here and the one more thing is what aver the key and the particular architecture is used for the encryption technique is used and the transmitter end and they are detected in the receiver end by the same reverse fashion respectively [8][9]. Here at the time of the process of the data the data integrity has to be maintained in which there should be no occurrence of the damage for the user data. Then after the detection of the data from the cloud as per the requirement of the accessibility the data has to be matched and should be in an analogous fashion that is a correlation is maintained between them.

3. EXPECTED RESULTS:

Experiments have been conducted on the present method where it is related to the particular aspects in the form of the privacy preservation is a major concern followed by the complexity maintenance by the accurate server that is utilization of the technique of the decentralization plays a crucial role in the system. Here the present designed method completely analyzes the drawbacks of the several previous methods where here the same mistakes are not supposed to be repeated so that the entire outcome of the

system is manipulated by which the performance of the system is analyzed. Here the process of the data takes place in the segmentation steps and are included as follows they are phase of setup where it includes the generation of the key that is the meta data in the randomized fashion followed by the encryption of the data by the proper data cryptography technique I which the integrity of the data is maintained followed by the effective protection is maintained respectively. Here at the process of the encryption of the data there are number of the switching techniques in which the logic is created for the well accurate protection in which the original data and the secrete data are manipulated by the proper operations respectively. Next the second phase is the verification of the data that is after the detection the correlation has to be maintained between the stored data and the retrieved data without any error respectively.

4. CONCLUSION:

In the present paper data integrity plays a crucial role as from the user end where the trust of the user is a major concern. Apart from that here a new technique includes a structural algorithm I which it works sequentially step by step and completely overcomes the problems of the several previous methods in which some of the methods are efficient in data protection and failure in the handling of the data complexity while in the other end the other techniques or the mechanism includes the scenario of the system in shich they are accurate in the handling of the accuracy of the data while they are failure in the protection is a major concern. So the present method completely satisfies the problems of the above techniques in which the protection is provides followed by the computations are also reduced in a well efficient manner so that the present method is reliable in its operability respectively. Here we finally conclude that the present method is effective and efficient in terms of the performance followed by the outcome of the entire system in a well oriented fashion respectively.

REFERENCES

[1] D. X. Song, D. Wagner, and A. Perrig, “Practical techniques for searches on encrypted data,” in SP ’00: Proceedings of the 2000 IEEE Symposium on Security and Privacy. Washington, DC, USA : IEEE Computer Society, 2000, p. 44.

[2] A. Juels and B. S. Kaliski, Jr., “Pors: proofs of retrievability for large files,” in CCS ’07: Proceedings of the 14th ACM conference on

Computer and communications security. New York, NY, USA: ACM, 2007, pp. 584–597.

[3] D. G. Mead, "Newton's identities," Amer. Math. Monthly, vol. 99, no. 8, pp. 749–749, Oct. 1992.

[4] H. Dörrie, "Sturm's problem of the number of roots," in 100 Great Problems of Elementary Mathematics: Their History and Solutions. New York: Dover, 1965, pp. 112–116.

[5] V. Prasolov and S. Ivanov, Problems and Theorems in Linear Algebra, ser. Translations of Mathematical Monographs. Providence, RI: Amer. Math. Society, 1994.

[6] C. M. Grinstead and J. L. Snell, "Chapter 11:Markov chains," in Introduction to Probability, 2nd ed. Providence, RI: Amer. Math. Society, 1997, pp.510–510.

[7] P.-J. Courtois and P. Semal, "Bounds for transient characteristics of Markov chains with large or infinite state spaces," in Proc. First Int.

Conf. Numerical Solutions of Markov Chains, Raleigh, NC, Jan. 8–10, 1990, Numerical Solution ofMarkov Chains, W. J. Stewart, Ed. New York: Marcel Dekker, 1991, pp. 413–434.

[8] V. I. Romanovskii, DiscreteMarkov Chains. Translated From the Russian by E. Seneta. Groningen: Wolters-Noordhoff, 1970.

[9] T. P. Pedersen, "A threshold cryptosystem without a trusted party," in Proc. 10th Ann. Int. Conf. Theory and Application of Cryptographic Techniques (EUROCRYPT'91), Berlin, Heidelberg, 1991, pp.522–526, Springer-Verlag.

[10] R. Canetti, C. Dwork, M. Naor, and R. Ostrovsky, "Deniable encryption," in CRYPTO, ser. Lecture Notes in Computer Science, B. S. K. Jr., Ed. New York: Springer, 1997, vol. 1294, pp. 90–104.