IJRRECS/July 2014/Volume-2/Issue-7/2664-2667 **ISSN 2321-5461**

INTERNATIONAL JOURNAL OF REVIEWS ON RECENT ELECTRONICS AND COMPUTER SCIENCE

DESIGN OF SECURITY MODEL FOR DATA PROTECTION BASED CLOUD

Vinay Bomma[1], S.Gayathri Devi[2]

[1]M.Tech Student, Dept of CSE, RRS College of Engineering & Technology, Muthangi (V), Patancheru (M), Hyderabad, T.S, India

[2]Associate Professor, Dept of CSE, RRS College of Engineering & Technology, Muthangi (V), Patancheru (M), Hyderabad, T.S, India

ABSTRACT:

In the upcoming advanced generation scenario here the architecture of the enterprise related to the field of information technology plays a crucial role in its application oriented to the computation of the cloud in a well oriented fashion respectively. Here the applicability of the computation of the cloud includes the scenario of the software related to the applications point of view followed by the data center oriented database and followed by the data management related to the trust based services respectively. Here this is one of the advanced feature in which it supposed to face a lot of challenges in the field of IT is a major concern. Here the provision of the data is completely under the control of the cloud based server but on the user module or the system of the user. The services provided by the cloud are both data as well as the software in terms of the software update followed by the storage capabilities depending on the requirement of the user choice. There is a huge concern for the security related aspect for the storage of the user data which is on the cloud is one of the major dilemmas for the user about his data privacy. Here the computation of the cloud has the security of the single phenomena depending on the demand of the user. So here the problem of the user is solved by the service provider which is cloud by the proper utilization of the data encryption techniques respectively. Simulations have been conducted on the present method where there is a lot of analysis takes place in the system in which experiments have been conducted on the large number of the datasets in a well oriented fashion respectively.

Keywords: Computation of cloud, Scalability, Data encryption strategy and Blowfish respectively.

1. INTRODUCTION:

There is a lot of advancement takes place in the system where the complete data followed by the services provided is under the control of the service provider that is the computation of the cloud and its maintenance respectively[1][4]. Here the technique is readymade utilization of the proper resources in a well oriented fashion by which there is no necessity of the installation of the software followed by the application supporting file everything is controlled by the cloud and the complete maintenance is under the control of the cloud based service provider respectively. As of before there is a complete necessity of the hardware that is the hard disk with proper utilization capability followed by the software depending on the utilization scenario whatever the application is used that particular software has to be installed but now there is no necessity of the installation and also the updating process is under the surveillance of the cloud based service provider respectively[6].

BLOCK DIAGRAM

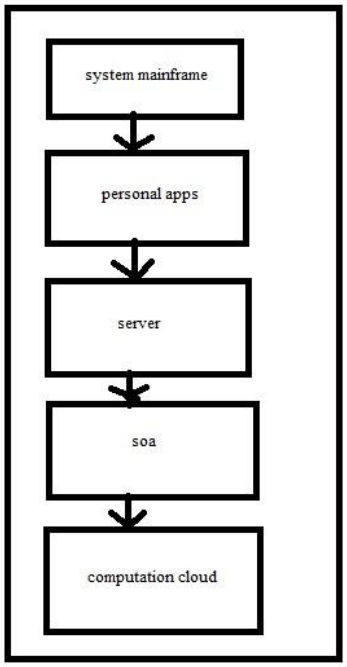

Fig 1: Shows the block diagram of the proposed method

2. METHODOLOGY

In this paper a new technique is proposed where it is related to the privacy based aspect for the user satisfaction of the user requirement and the implementation of the present method is shown by the above block diagram in the summarized fashion respectively[7][8]. Here the services of the cloud includes the services of the software, infrastructure and platform respectively.

Here the present method is completely concentrated on the security based aspect where the security includes structure of three layer aspect where the authentication is related to the layer one, Encryption is of the layer two followed by the final layer includes accurate data recovery process[9]. Here the above algorithm includes all the three layer so that the efficient algorithm is designed in a well oriented fashion respectively[10].

3. EXPECTED RESULTS

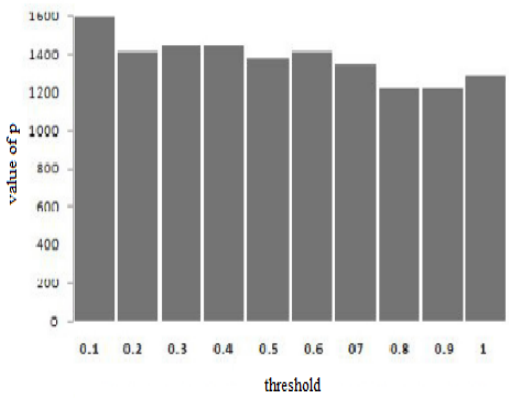

Fig 2: Shows the graphical representation of the P Value histogram

Here the present method is effective and efficient on comparison with respect to the drawbacks of the several previous methods and it completely overcome the drawbacks of it by proper implementation of the model related to the strict security scenario of the model of multi layer which includes level three structure in a ordered fashion respectively. Here the performance of the present method is shown by the above results and the plotting takes place with respect to the threshold followed by the values of P in a well efficient manner. Here the system is shown the perfect results where it satisfies the dilemma of the user related to the privacy is a major concern respectively.

4. CONCLUSION

In this paper a new technique is proposed which is related to the data authentication where it utilizes the algorithm of the latest encryption standard technique which is an advancement in the system for the complete protection of the data from the hackers respectively. Here in the present model it utilizes the scenario of the level three model which it includes authentication, design followed by the data recovery in a well oriented fashion respectively. Here the protection of the data takes place and followed by the provision of the services in a well efficient manner and some of them includes software, infrastructure followed by the platform dependent is a major concern spectively. Here we finally conclude that the

in terms of the performance followed by the outcome of the entire system in a well stipulated fashion respectively.

REFERENCES

[1] R. Curtmola, O. Khan, R. Burns, and G. Ateniese, "MR-PDP: multiple-replica provable data possession," in 28th IEEE ICDCS, 2008, pp. 411–420.

[2] A. F. Barsoum and M. A. Hasan, "On verifying dynamic multiple data copies over cloud servers," Cryptology ePrint Archive, Report 2011/447, 2011, 2011, http://eprint.iacr.org/.

[3] K. D. Bowers, A. Juels, and A. Oprea, "HAIL: a high-availability and integrity layer for cloud storage," in CCS '09: Proceedings of the 16th ACM conference on Computer and communications security. New York, NY, USA: ACM, 2009, pp. 187–198.

[4] Y. Dodis, S. Vadhan, and D. Wichs, "Proofs of retrievability via hardness amplification," in Proceedings of the 6th Theory of Cryptography Conference on Theory of Cryptography, 2009.

[5] A. Juels and B. S. Kaliski, "PORs: Proofs of Retrievability for large files," in CCS'07: Proceedings of the 14th ACM conference on Computer and communications security. ACM, 2007, pp. 584–597.

[6] H. Shacham and B. Waters, "Compact proofs of retrievability," in ASIACRYPT '08, 2008, pp. 90–107.

[7] P. S. L. M. Barreto and M. Naehrig, "Pairing-friendly elliptic curves of prime order," in Proceedings of SAC 2005, volume 3897 of LNCS. Springer-Verlag, 2005, pp. 319–331.

[8] D. L. G. Filho and P. S. L. M. Barreto, "Demonstrating data possession and uncheatable data transfer," Cryptology ePrint Archive, Report 2006/150, 2006.

[9] D. Naor, M. Naor, and J. B. Lotspiech, "Revocation and tracing schemes for stateless receivers," in Proceedings of the 21st Annual International Cryptology Conference on Advances in Cryptology, ser. CRYPTO '01. Springer-Verlag, 2001, pp. 41–62.

[10] F. Seb´e, J. Domingo-Ferrer, A. Martinez-Balleste, Y. Deswarte, and J.-J. Quisquater, "Efficient remote data possession checking in critical information infrastructures," IEEE Trans. on Knowl. And Data Eng., vol. 20, no. 8, 2008.