IJRRECS/July 2014/Volume-2/Issue-7/2754-2757 **ISSN 2321-5461**

INTERNATIONAL JOURNAL OF REVIEWS ON RECENT ELECTRONICS AND COMPUTER SCIENCE

DELEGATION OF SUPERIOR ACCESS CONTROL IN CLOUD SYSTEM

Nadipelli Preethirao[1], A.Srilakshmi[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:

Here the implementation of one of the most advanced technique under the standard of the encryption in the scenario of the fine grain basis relative to the cloud by the hosted data which includes the authentication followed by the controlled access and enforcement of the approach respectively. Under the above stated mechanism data is encrypted by the owners of the data and then after the encryption it is uploaded to the cloud and after the downloading from the cloud the followed prescribed decryption process is involved in it. Due to the process mentioned above it is a computation oriented strategy in terms of the working scenario followed by the cost oriented fashion. This is one of the major problem as of stated from the above mechanism which is previously stated and in order to over the stated problem a new technique is proposed based on the encryption of the two layers respectively which includes the strategy of the encryption from the owner is a course gain fashion and the encryption of the cloud grained from the cloud plays a crucial role in the system in a well effective manner respectively. There is a huge challenge oriented strategy takes place in the present method of the system where the decomposition of the policies of the access control under the performance of the two layered encryption strategy respectively. Experiments have been conducted on the present method where the test beds are conducted on the large number of the data sets and the evaluations are done in the prescribed fashion on each and every outcome in a well accurate scenario respectively.

Keywords: Data identification, Data authentication, Privacy orientation, Data encryption strategy, Control of the access, Decomposition of the policy and policy of control respectively.

1. INTRODUCTION:

Under the scenario of the lot of advancement in the system there is a huge concern from the users of the clouds that is the customer of the cloud are privacy based aspect is a major concern respectively. As there are several previous method which did a lot of research on the present proposed problem but even though there are some or the other problems existing in the system in a well oriented scenario respectively [1][2]. Here there is a huge challenge for the present method in which it includes the protection of the data of the user and the customer is a major concern respectively. Here there is an implementation of the one of the most advanced technique called encryption where it plays a crucial role in the maintenance of the confidentiality of the data respectively. Due to the further advancement in the technology there are a lot of the advancement in the techniques for the protection of the data in a secured fashion which includes the encryption is one among them respectively [6].

BLOCK DIAGRAM

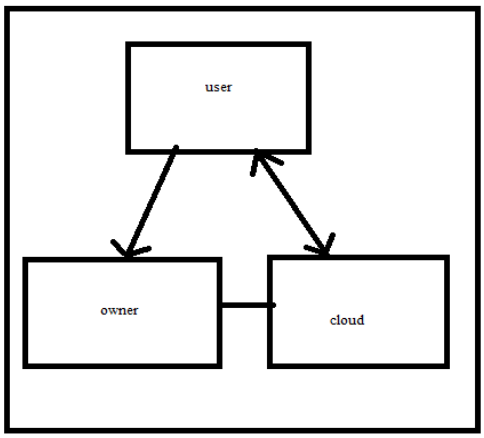

Fig 1: Shows the block diagram of the present method respectively

2. METHODOLOGY

In this paper a new technique is proposed where it is illustrated in the brief oriented fashion in terms of the block diagram respectively. Here the architecture is explained in a detailed fashion where the proposed system consists of the cloud, USR, owner and idp respectively. Here the acp's are enforced by the help of the integration of the cloud and the owner respectively. Where it includes the data encryption standard respectively. Here it is a dual hierarchy in which at one end there is a load reduction followed by control of the access in the

system where the updating of the data handling is easily done under the change of the dynamics respectively [5][7]. Here the stated architecture is completely explained by the above block diagram in a brief descriptive fashion respectively.

3. EXPECTED RESULTS

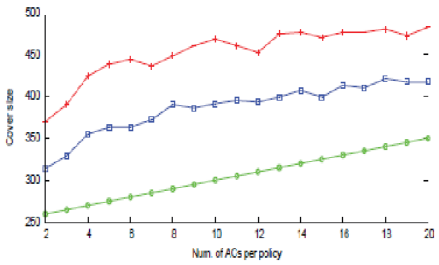

Fig 2: Shows the graphical representation of the present method respectively

In this paper a new method is implemented by the well efficient study of the several previous methods and its complete in depth analysis of the drawbacks of the previous methods in a well oriented fashion respectively. A comparative analysis is given between the present method and the previous methods in the above figure where the performance is evaluated and it is better than the previous methods respectively. Here the analysis of the experiment followed by the well effective comparison takes place between the approach of the TLE followed by the SLE respectively [4][9]. Here the credentials are attributed at a rate of the margin of the 5 % respectively. Here the operation relative to the arithmetic scenario under the field of the finite strategy was implemented. Here the expressions are generated which belongs to the strategy of the Boolean phenomena under the random fashion respectively. The attributes are specified by the help of the logic related to the Boolean scenario respectively. Here the conditioning of the attributes is shown in the above figure in the form of the comparative analysis.

4. CONCLUSION

As previously there are a lot of techniques used for the protection of the data but there are some or the other problem included in it and the problems is of the form of the time complexity followed by the complexity in the methodology and so that the efficiency is completely reduced by the help of the increase in the complexity of the system in a well oriented fashion respectively. In order to overcome the above problem new technique is proposed which includes the scenario of the advancement in the standards of the encryption plays a crucial role respectively. Here in the case of the proposed method it is a layer of the

coupled architecture of the standards of the encryption plays a crucial role by which the problem of the delegating strategy is solved where the exposure of the information is get reduced udder the similarity in the conditions under the USR collision related to the cloud.

REFERENCES

[1] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in CCS '06: Proceedings of the 13th ACM conference on Computer and communications security. New York, NY, USA: ACM, 2006, pp. 89–98.

[2] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," in SP '07: Proceedings of the 2007 IEEE Symposium on Security and Privacy. Washington, DC, USA: IEEE Computer Society, 2007, pp. 321–334.

[3] G. Ateniese, K. Fu, M. Green, and S. Hohenberger, "Improved proxy re-encryption schemes with applications to secure distributed storage," ACM Transaction on Information System Security, vol. 9, pp. 1–30, February 2006.

[4] X. Liang, Z. Cao, H. Lin, and J. Shao, "Attribute based proxy re-encryption with delegating capabilities," in Proceedings of the 4th International Symposium on Information, Computer, and Communications Security, ser. ASIACCS '09. New York, NY, USA: ACM, 2009, pp. 276–286.

[5] C.-K. Chu, J. Weng, S. Chow, J. Zhou, and R. Deng, "Conditional proxy broadcast re-encryption," in Proceedings of the 14th Australasian Conference on Information Security and Privacy, 2009, pp. 327–342.

[6] J.-M. Do, Y.-J. Song, and N. Park, "Attribute based proxy reencryption for data confidentiality in cloud computing environments," in Proceedings of the 1st International Conference on Computers, Networks, Systems and Industrial Engineering. Los Alamitos, CA, USA: IEEE Computer Society, 2011, pp. 248–251.

[7] S. D. C. di Vimercati, S. Foresti, S. Jajodia, S. Paraboschi, and P. Samarati, "Over-encryption: Management of access control evolution on outsourced data," in Proceedings of the 33rd International Conference on Very Large Data Bases, ser. VLDB '07. VLDB Endowment, 2007, pp. 123–134.

[8] M. Nabeel and E. Bertino, "Towards attribute based group key management," in Proceedings of the 18th ACM conference on Computer and communications security, Chicago, Illinois, USA, 2011.

[9] A. Fiat and M. Naor, "Broadcast encryption," in Proceedings of the 13th Annual International Cryptology Conference on Advances in Cryptology, ser. CRYPTO '93. London, UK: Springer-Verlag, 1994, pp. 480–491.

[10] 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. London, UK: Springer-Verlag, 2001, pp. 41–62.

[11] J. Li and N. Li, "OACerts: Oblivious attribute certificates," IEEE Transactions on Dependable and Secure Computing, vol. 3, no. 4, pp. 340–352, 2006.