IJRRECS/October 2013/Volume-1/Issue-6/1246-1249 **ISSN 2321-5461**

INTERNATIONAL JOURNAL OF REVIEWS ON RECENT ELECTRONICS AND COMPUTER SCIENCE

DESIGN OF THE ATTRIBUTE BASED ENCRYPTION OF SHARING PERSONAL HEALTH RECORDS

Shanoob P.M[1], B.V Janaki Savithri[2]

[1]M.Tech Student, Dept of CSE, Aurora's Technological and Research Institute, Parvathapur, Uppal, Hyderabad, A.P, India

[2]Associate Professor, Dept of CSE, Aurora's Technological and Research Institute, Parvathapur, Uppal, Hyderabad, A.P, India

ABSTRACT:

Here the design of the well effective model takes place in the system based on the phenomena of the records of the personal health of the model of the patient centric strategy for the exchange of the information related health by the help of the cloud relative outsourcing plays a crucial role as a service provider respectively. There is a huge problem and there is a lot of frustration related to the scenario of the information of the relative personal health by the servers of the thirs party based strategy of the unauthorized phenomena respectively. Therefore many of the patients are worried about the storage of their data in the cloud by the technique of the decentralization plays a crucial role in its relative aspect respectively. Here in order to overcome the above problem a new technique is proposed by the novel framework of the patient centric model plays a crucial role in its relative strategy oriented aspect by the control access of the data based mechanism plays a crucial role of the servers of the semi trusted environment respectively. For the purpose of the fine grains health record of the personalized environment plays a crucial role of the techniques of the attributes oriented encryption plays a crucial role of the file oriented scenario of the PHR respectively. Simulations have been conducted on the present method where there is a lot of analysis and the number of experiments has been conducted on the large number of the datasets in a well oriented fashion with respect to the unknown environments respectively. Here there is an accurate analysis takes place in the system in terms of the improvement in the

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

Keywords: Data encryption, Personal health record strategy, Computation of the cloud, Encryption based on the attributes, Control of the fine access and Privacy of the data. respectively.

1. INTRODUCTION:

There is a lot of advancement takes place in the system followed by the research oriented strategy plays a crucial role in its relative aspect of the maintenance of the personal health record respectively [1]. Here mainly the file involve the scenario of the manipulation by the own password for the privacy as a major concern followed by the stipulated aspect of the modification of the represented data of the system of the record relative to the personal health as a major concern respectively [2][3]. Here some of the manipulations includes control manage and create are the major responsibilities respectively.

BLOCK DIAGRAM

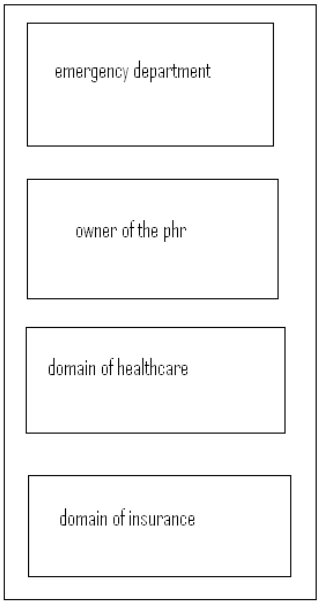

Fig 1: Shows the block diagram of the present method respectively

2. METHODOLOGY

Here the present method is shown in the above figure in the form of the block diagram based representation and explains in an elaborative fashion respectively. In this paper a method is designed with an efficient

framework oriented strategy in which it is used for accurate analysis based strategy followed by the powerful implementation in a well oriented aspect respectively [4]. There is a huge challenge for the present method in which the designed method is implemented in such a way that it should be in a position to accurately analyze the problems of the previous methods in a well oriented fashion followed by the degradation of the performance in a controlled strategy where there is an improvement in the outcome of the system in a well oriented fashion respectively[5][6]. Here the present method completely overcome the drawbacks of the several previous methods in a well efficient fashion followed by the improvement in the performance based strategy and also the degradation of the performance of the several previous methods in a controlled fashion respectively. Here we finally conclude that the present method is effective in terms of the analysis followed by the outcome of the entire system followed by the improvement in the performance in the strategy and which is benefitted for the application in related to the real time environment respectively [7][8]

.

3. EXPECTED RESULTS

A comparative analysis is made between the present method to that of the several previous methods is shown in the below figure in the form of the graphical representation and explains in a brief elaborative fashion respectively. There is a huge challenge for the present method where it is supposed to improve the performance of the system followed by the overall system based analysis with respect to the outcome of the entire system respectively. A lot of analysis is made on the present method and the huge number of the simulations have been conducted on the large number of the data sets in a well oriented fashion respectively.

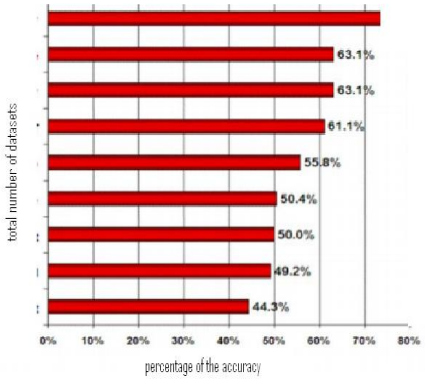

Fig 2: Shows the graphical representation of the present method respectively

4. CONCLUSION

In this paper a method is designed with a well effective framework oriented strategy where there is a lot of research oriented strategy takes place in the system and plays a crucial role for the improvement of the outcome followed by the performance of the system respectively. Here in the present system oriented scenario where the sharing of the data takes place based on the records of the personal health of the records oriented with the relative computation of the cloud as a major challenge respectively. Here by the help of the servers of the cloud there is a huge realization of the model of the phenomena relative to the model of the patient centric strategy plays a crucial role in its irrelativeness of the system of the own system based privacy as a major concern of the data encryption as a major aspect in terms of the data storage in the secured nature respectively. There is a huge challenge for the present developed method in which is from the end of the user related to the records of the physical health oriented aspect in a predictive fashion where to reduce the complexity of the system respectively.

REFERENCES

[1] J. A. Akinyele, C. U. Lehmann, M. D. Green, M. W. Pagano,Z. N. J. Peterson, and A. D. Rubin, "Self-protecting electronic medical records using attribute-based encryption," Cryptology ePrint Archive, Report 2010/565, 2010, http://eprint.iacr.org/.

[2] M. Chase and S. S. Chow, "Improving privacy 20and security in multi-authority attribute-based encryption," in CCS '09, 2009, pp.121–130.

[3] X. Liang, R. Lu, X. Lin, and X. S. Shen, "Ciphertext policy attribute based encryption with efficient revocation," Technical Report, University of Waterloo, 2010.

[4] J. Hur and D. K. Noh, "Attribute-based access control with efficient revocation in data outsourcing systems," IEEE Transactions on Parallel and Distributed Systems, vol. 99, no. PrePrints, 2010.

[5] S. Jahid, P. Mittal, and N. Borisov, "Easier: Encryption-based access control in social networks with efficient revocation," in ASIACCS, Hong Kong, March 2011.

[6] S. Ruj, A. Nayak, and I. Stojmenovic, "Dacc: Distributed access control in clouds," in 10th IEEE TrustCom, 2011.

[7] A. Lewko and B. Waters, "Decentralizing attribute-based encryption,"Advances in Cryptology–EUROCRYPT, pp. 568–588, 2011.

[8] S. D. C. di Vimercati, S. Foresti, S. Jajodia, S. Paraboschi, andP. Samarati, "Over-encryption: management of access control evolution on outsourced data," in VLDB '07, 2007, pp. 123–134.