IJRRECS/March 2014/Volume-2/Issue-3/2080-2085 **ISSN 2321-5461**

INTERNATIONAL JOURNAL OF REVIEWS ON RECENT ELECTRONICS AND COMPUTER SCIENCE

SUSTAINING OF HEALTH RECORD CONFIDENTIALITY WITHIN CLOUD ENVIRONMENT

K.Lakshmi Bhargavi[1], M.Narendhar[2]

[1]M.Tech Student, Dept of CSE, Bandari Srinivas Institute of Technology, Chevella, R.R Dist., A.P, India

[2]Associate Professor & HOD, Dept of CSE, Bandari Srinivas Institute of Technology, Chevella, R.R Dist., A.P, India

ABSTRACT:

Broad range of the internal and external pressures for data reliability exists even though the cloud infrastructures are considerably more dominant and consistent than personal computing strategies. Even if the utilization of cloud computing has rapidly improved; the safety of cloud computing is still considered the most important issue in the environment of cloud computing. Well-organized methods which permit on-demand data accuracy confirmation on behalf of cloud users have to be considered in order to attain the assurances of cloud data integrity and accessibility and apply the excellence of cloud storage service. An attribute-based infrastructure is proposed, for the purpose of electronic healthcare records systems where by means of a broadcast difference of cipher text policy attribute-based encryption allows straight revocation for record files of each patient's electronic healthcare records. For the owners and users which are different from preceding works in protected data outsourcing, various data owner scenario were mainly focussed and into various security domains users in the personal health record system are separated which greatly reduces the difficulty of key organization.

Keywords: Attribute Based Encryption, Cloud computing, Personal health record.

1. INTRODUCTION:

For personal or professional purposes, the authorized users may possibly moreover need to access the Personal health record. In view of the fact that patients are not always online, every user get hold of keys from each possessor, whose record of Personal health they want to read would edge the ease of access. Assigning of the entire responsibilities of the attribute organization to a single trusted authority is not considered sensible in generating the secure keys [4]. Key generation and decryption which are limply linear are the number of attributes involved in the complexities per encryption. To realize the access control for the fine grained, attribute based encryption was used for the outsourced information in order to make safe about the records of the electronic healthcare and there has been an escalating concentration in validating the attribute-based encryption [8] [13]. The important difference in a single trusted authority is still understood to manage the complete specialized domain on the notion of separating the scheme into two categories of provinces is theoretically comparable. In the cloud computing, a novel structural design was proposed for the purpose of protecting and sharing of the personal health records and is both scalable and well-organized all the way through functioning and simulation [1]. An attribute-based infrastructure is proposed, for the purpose of electronic healthcare records systems where by means of a broadcast difference of cipher text policy attribute-based encryption allows straight revocation for record files of each patient's electronic healthcare records. To an alternative way to is to employ a central ability to carry out the important administration on behalf of each and every one Personal health record owners, other than this requires too much faith on a meticulous authority [6] [11]. An efficient and on-demand user revocation mechanism was lacked for the purpose of updates of dynamic policy for the attribute-based encryption by means of the support which forms necessary parts of distribution of the protected Personal health record.

2. METHODOLOGY:

The provision of well organized key organization and the access to the personal health record availability is the important objective of our framework. As various organizations normally form their own domains, various sets of attributes belonging to their domains become appropriate

authorities to certify them [3] [10]. In order to defend the individual health information stocked up on a semi trusted server, the encryption process of attribute-based was adopted as the most important encryption primordial [14]. The use of a single trusted authority in the system is usually assumed, generating secure keys to assign all attribute organization responsibilities to one trusted authority is not sensible, including certifying all users' attributes or roles. To realize the access control for the fine grained, attribute based encryption was used for the outsourced information in order to make safe about the records of the electronic healthcare and there has been an escalating concentration in validating the attribute-based encryption [9]. By means of attribute based encryption the self protecting electronic medical records are generated and later on stored on the cloud servers with the intention of accessing the attribute based encryption during the offline of the health provider. Assigning of the entire responsibilities of the attribute organization to a single trusted authority is not considered sensible in generating the secure keys. The important difference in a single trusted authority is still understood to manage the complete specialized domain on the notion of separating the scheme into two categories of provinces is theoretically comparable [5] [7]. The users are personally connected by means of the owner of the data and they access the record of personal health for every personal domain on the basis of the access rights which are allocated by the owner. In order to control the accessibility from the users of the public domains, the role based fine grained access policies were specified for the files of the personal health record at the same time do not need to be familiar with the authorized users list when performing the encryption [2] [15]. To an autonomous sector in the society like health care, the domains of the public can be mapped. The objective of the patient centric privacy is regularly often in divergence by means of scalability in a system of personal health record shown in fig1. To identify the cryptographically imposed access to the patient centric personal health record, attribute based encryption was recognized in both the types of safety domains [12]. The users in the public domains attain the secret keys of attribute based officials without interacting directly with the owners. The domains of the public consist of users who access it on the basis of their professional roles. There are various attribute authorities

for each leading a displace subset of attributes in a public domain multi authority attribute based encryption.

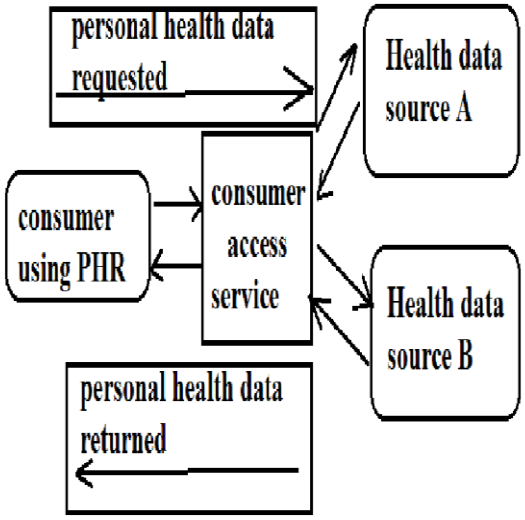

Fig1: An overview of personal health record

3. RESULT:

An attribute-based infrastructure is proposed, for the purpose of electronic healthcare records systems where by means of a broadcast difference of cipher text policy attribute-based encryption allows straight revocation for record files of each patient's electronic healthcare records. The scalability and competence of our elucidation have been estimated in terms of storage space, and the costs of communication and computation. The computation cost of the server was replicated in the user revocation to measure the performance of the system of the revocation of the user. In the cloud computing, a novel structural design was proposed for the purpose of protecting and sharing of the personal health records and is both scalable and well-organized all the way through functioning and simulation. The cost of revocation was greatly reduced by the method of lazy revocation due to the reason that it aggregates the operations of multiple cipher text update that amortizes the computation after a while.

4. CONCLUSION:

For the past few years, the technology of cloud computing has the extreme growth sections in the field of infrastructure and permits the consumers to make usage of applications devoid of installation and by means of internet access the personal files. Encryption of the data earlier to the outsourcing is a capable and feasible approach. For the owners and users which are different from preceding works in protected data outsourcing, various data owner scenario were mainly focussed and into various security domains users in the personal health record system are separated which greatly reduces the difficulty of key organization. In the cloud computing, a novel structural design was proposed for the

purpose of protecting and sharing of the personal health records and is both scalable and well-organized all the way through functioning and simulation. An attribute-based infrastructure is proposed, for the purpose of electronic healthcare records systems where by means of a broadcast difference of cipher text policy attribute-based encryption allows straight revocation for record files of each patient's electronic healthcare records. By means of making use of multi-authority attribute based encryption methods, the guaranteeing of a high degree of patient privacy is achieved. An innovative patient-centric construction and a collection of systems were proposed for data access control to the stored personal health record in semi-trusted servers. Encryption of the data earlier to the outsourcing is a capable and feasible approach. In order to achieve fine grained and access control to scalable data intended for individual health records we make usage of attribute based encryption technique for encrypting the personal health record of every file. The third party storage space servers are frequently becoming targets for numerous hateful behaviours leading to the discovery of the personal health data due to the high value of the vulnerable personal health data.

REFERENCES:

[1] L. Ibraimi, M. Petkovic, S. Nikova, P. Hartel, and W. Jonker, "Ciphertext-policy attribute-based threshold decryption with flexible delegation and revocation of user attributes," 2009.

[2] H. L¨ohr, A.-R. Sadeghi, and M. Winandy, "Securing the e-health cloud," in Proceedings of the 1st ACM International Health Informatics Symposium, ser. IHI '10, 2010, pp. 220–229.

[3] "At risk of exposure – in the push for electronic medical records, concern is growing about how well privacy can be safeguarded," 2006. [Online]. Available: http://articles.latimes.com/2006/jun/26/health/he-privacy26

[4] 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/.

[5] 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 VLDB '07, 2007, pp. 123–134.

[6] M. Pirretti, P. Traynor, P. McDaniel, and B. Waters, "Secure attribute-based systems," Journal of Computer Security, vol. 18, no. 5, pp. 799–837, 2010.

[7] H. Yang, H. Luo, F. Ye, S. Lu, and L. Zhang, "Security in mobile ad hoc networks: challenges and solutions," Wireless Communications,
IEEE, vol. 11, no. 1, pp. 38 – 47, feb 2004.

[8] C. Dong, G. Russello, and N. Dulay, "Shared and searchable encrypted data for untrusted servers," in Journal of Computer Security, 2010.

[9] 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.

[10] S. Narayan, M. Gagn´e, and R. Safavi-Naini, "Privacy preserving ehr system using attribute-based infrastructure," ser. CCSW '10, 2010, pp. 47–52.

[11] S. M¨ uller, S. Katzenbeisser, and C. Eckert, "Distributed attributebased encryption," Information Security and Cryptology–ICISC 2008,
pp. 20–36, 2009.

[12] J. Benaloh, M. Chase, E. Horvitz, and K. Lauter, "Patient controlled encryption: ensuring privacy of electronic medical records," in CCSW '09, 2009, pp. 103–114

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

[14]"Privacy-preserving personal health record system using attribute-based encryption," Master's thesis, WORCESTER POLYTECHNIC
INSTITUTE, 2011.

[15] L. Ibraimi, M. Asim, and M. Petkovic, "Secure management of personal health records by applying attribute-based encryption," Technical Report, University of Twente, 2009.