IJRRECS/March 2014/Volume-2/Issue-3/2104-2109 **ISSN 2321-5461**

INTERNATIONAL JOURNAL OF REVIEWS ON RECENT ELECTRONICS AND COMPUTER SCIENCE

AN ACCOMPLISHING OF SECURE DATA ACCESS CONTROL FOR HEALTH RECORDS

K Md Mohsin Ashfaqh[1], Syed Asadullah Hussaini[2]

[1]M.Tech Student, Dept of CSE, Hi-Point College of Engineering & Technology, Moinabad, R.R Dist, A.P, India

[2]Professor, Dept of CSE, Hi-Point College of Engineering & Technology, Moinabad, R.R Dist, A.P, India

ABSTRACT:

Cloud computing put up on established trends and offers a variety of services that can profit its customers, by means of providing quick access to their data, scalability, data storage, data recovery and guard against various hackers, and usage of the network and infrastructure conveniences. 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. To make available an entire and accurate outline of an individual's medical history which is available online is the objective of a personal health record. There have been a wide-ranging discretion concerns as personal health information could be uncovered to those third party servers and to prohibited parties. The storage, retrieval, and sharing of the medical information has become more efficient as the PHR service allows a patient to generate, control, and administer personal health data in one place all the way through the web. 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. A new patient-centric construction and a collection of systems were proposed for data access control to the stored personal health record in semi-trusted servers.

Keywords: Cloud computing, Patient-centric, Data reliability, Personal health records.

1. INTRODUCTION:

Cloud computing construct on established trends for motivating the cost out of the delivery of services while growing the speed and agility with which services are deployed [4]. The patient centric model of exchanging the health information has emerged in the recent times and more over there are many risks regarding the security and privacy concerns which can obstruct the extensive acceptance to have the convenient records services for everyone [10]. Based on the attributes of the users enabling a patient to share her record of personal health selectively between a set of users under a set of attributes access policies are expressed by encrypting the file by means of attribute based encryption devoid of knowing the complete list of users. Several personal health record services are outsourced or provided by third-party service providers [8]. Personal and specialized users are the two categories of users. 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 [13]. 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 [1]. 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 [6]. Based on the attributes of the users enabling a patient to share her record of personal health selectively between a set of users under a set of attributes access policies are expressed by encrypting the file by means of attribute based encryption devoid of knowing the complete list of users. 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 by means of attribute based encryption [11]. As the previous work having different definitions for attributes distinguish the public and individual domain key organization requirements and issues of scalability. Various sets of attributes belonging to their domains become appropriate authorities to certify them as

various organizations normally form their own 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 with the intention of controlling the accessibility from the users of the public domains [3].

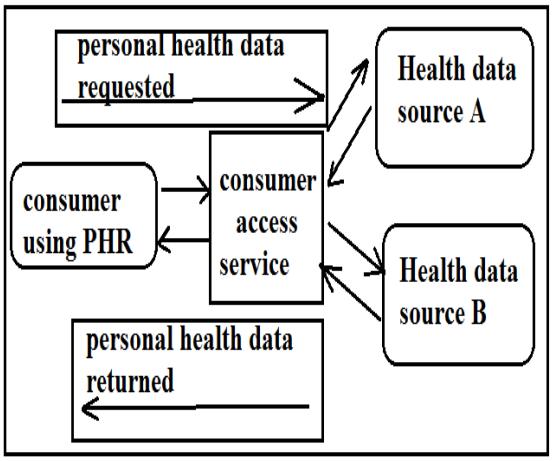

Fig1: An overview of personal health record

2. METHODOLOGY:

Personal health record shown in fig1 is the physical condition record where the health data connecting to the patient uneasiness is maintained by the patient. In order to guarantee the controlling of the patient centric privacy over the records of personal health, it is essential to have the fine grained data access control schemes with the semi trusted servers [14]. 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. 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 with the intention of controlling the accessibility from the users of the public domains [9]. Personal and specialized users are the two categories of users. The provision of well organized key organization and the access to the personal health record availability is the important objective of our framework [7]. Based on the attributes of the users enabling a patient to share her record of personal health selectively between a set of users under a set of attributes access policies are expressed by encrypting the file by means of attribute based encryption devoid of knowing the complete list of users. By means of different sets of cryptographic keys, the multiple owners who may possibly encrypt and are different from the single data owner who is considered in most of the works in the system of personal health record [2] [15]. Based on the attributes of users the data

access policies are expressed using attribute based encryption. The objective of the patient centric privacy is regularly often in divergence by means of scalability in a system of personal health record. 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 [12]. The significant dissimilarity 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. The user to whom the related description key was given remains confidential to the rest of users and the availability of the personal health record was made available [5]. 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.

3. RESULTS:

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. To measure the performance of the system of the revocation of the user, the computation cost of the server was replicated in the user revocation. The expenditure of revocation was to a great extent 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. In order to guarantee the controlling of the patient centric privacy over the records of personal health, it is essential to have the fine grained data access control schemes with the semi trusted servers.

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. As various organizations normally form their own domains, various sets of attributes belonging to their domains become appropriate authorities to certify them. To encrypt the Personal health records data we utilize attribute-based encryption. 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. In a Personal health records system, the objective of patient-centric privacy is often in conflict with scalability. 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. The self protecting electronic medical records are generated and later on stored on the cloud servers by means of attribute based encryption with the intention of accessing the attribute based encryption during the offline of the health provider. 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.