IJARES/Aug 2013/Volume-1/Issuse-1/Article No-4/20-25

INTERNATIONAL JOURNAL OF ADVANCED RESEARCH IN ENGINEERING AND SCIENCE

MODERNIZATION IN THE CONFIDENTIALITY PROTECTION OF HEALTH RECORDS IN CLOUD COMPUTING

G.Kiran Kumar[1], L.Ravi[2]

[1]Dept of ECE, VVIT Engineering College, Chevella, A.P, India

[2]Dept of ECE, VVIT Engineering College, Chevella, A.P, India

ABSTRACT:

Personal health record is the physical condition record where the health data connecting to the patient uneasiness is maintained by the patient. Assuring the patients control over the access to the personal health records is a competent approach for encrypting the personal health record earlier to the outsourcing process. 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 intension of the personal health record is to make available a complete and perfect check of an individual's medical record which is obtainable online. 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. For the owners and users which are different from preceding works in protected data outsourcing, various data owner scenario were mainly focused and into various security domains users in the personal health record system are separated which greatly reduces the difficulty of key organization. By means of making use of multi-authority attribute based encryption methods, the guaranteeing of a high degree of patient privacy is achieved. As the personal health information is revealed to the third party servers, there have been a wide-ranging privacy concerns in contrast to illegitimate parties.

KEYWORDS: Physical Health Record, Attribute Based Encryption, Third Party Servers, Patient Record.

1. INTRODUCTION:

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 [2]. 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. Encryption of the data earlier to the outsourcing is a capable and feasible approach [8]. The owner of the Personal health record has to decide the procedure to encrypt her files allowing the set of users to attain the access to her 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 [1] [11]. Due to the high cost of maintaining and building the specialized data centres various services of personal health record are provided by means of providers of third party service.

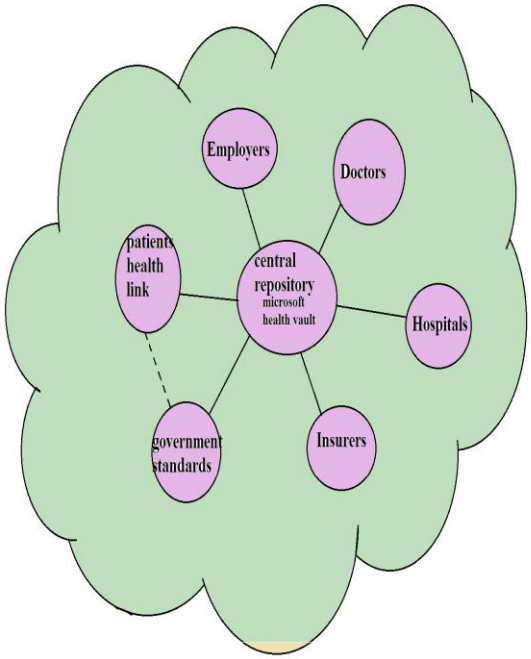

Fig 1: Patient- centric personal health record.

2. PROTECTED ALLOTMENT OF INDIVIDUAL HEALTH RECORDS

The objective of the patient centric privacy shown in fig1 is regularly often in divergence by means of scalability in a system of personal health record. 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] [9]. Probably 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 [14]. 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 [3]. 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 [6] [10]. Personal and specialized users are the two categories of users. 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 [4]. 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. Key generation and decryption which are limply linear are the number of attributes involved in the complexities per encryption [7]. To determine a list of the owners is difficult and the access requests of those requests are generally impulsive.

3. ORGANIZATION OF ATTRIBUTE-BASED ENCRYPTION DATA ACCESS:

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.

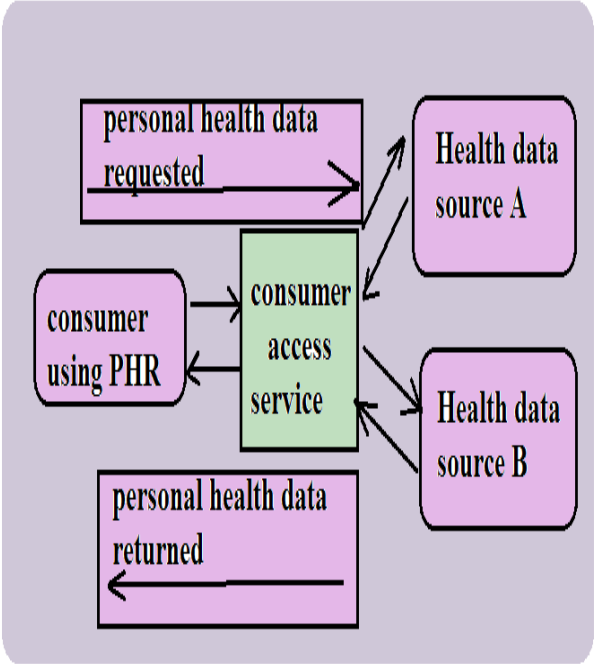

Fig2: An overview of personal health record

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 [15]. Initially the usage of the authority of single trusted is normally assumed in the system. Assigning of the entire responsibilities of the attribute organization to a single trusted authority is not considered sensible in generating the secure keys [12]. 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 [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. As various organizations normally form their own domains, various sets of attributes belonging to their domains become appropriate authorities to certify them. 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. As the previous work having different definitions for attributes distinguish the public and individual domain key organization requirements and issues of scalability.

4. CONFINED PERSONAL HEALTH RECORD ACCESS AND WELL - ORGANIZED KEY MANAGING:

The provision of well organized key organization and the access to the personal health record availability is the important objective of our framework. The users are personally connected by means of the owner of the data and they access the record of personal health shown in fig2 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. 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. There are various attribute authorities for each leading a displace subset of attributes in a public

domain multi authority attribute based encryption. To an autonomous sector in the society like health care, the domains of the public can be mapped. The basic idea of the data access requirements is to separate the system into numerous security and personal domains according to the requirements of the data access to different users. 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.

5. RESULT:

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 scalability and efficiency of our solution have been estimated in terms of storage space, and the costs of communication and computation. 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. 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.

6. CONCLUSION:

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. 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. 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. For the owners and users which are different from preceding works in protected data outsourcing, various data owner scenario were mainly focused and into various security domains users in the personal health record system are separated which greatly reduces the difficulty of key organization. By means of making use of multi-authority

attribute based encryption methods, the guaranteeing of a high degree of patient privacy is achieved.

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.