IJRRECS/June 2014/Volume-2/Issue-6/2517-2522 **ISSN 2321-5461**

INTERNATIONAL JOURNAL OF REVIEWS ON RECENT ELECTRONICS AND COMPUTER SCIENCE

AN APPROACH TOWARDS PRIVACY OF HEALTH RECORDS IN CLOUD COMPUTING

V.Srikanth Reddy[1], G.Charles Babu[2]

[1]M.Tech Student, Dept of CSE, Holy Mary Institute of Technology & Science, Bogaram(V), Keesara(M), R.R.Dist.,T.S, India

[2]Professor, Dept of CSE, Holy Mary Institute of Technology & Science, Bogaram(V), Keesara(M), R.R.Dist., T.S, India

ABSTRACT:

Novel applications such as online social networks and online documents offer very suitable ways for people to accumulate and distribute various data including personal profile, electronic documents on remote online data servers. Data security is a significant issue for remote data storage. A physical condition record where health data and information associated to the patient is preserved by the patient is a personal health record. Disclosure of responsive information, such as health files, stored on remote data servers has to be severely protected before users have freedom to use the data services. Fine-grained data access control mechanisms frequently need to be in place to promise appropriate disclosure of responsive data among multiple users. To encrypt each patient's personal health record file, we control attribute based encryption techniques in order to achieve control for scalable data access intended for personal health records. We mainly focus on the various data owner scenario, and separate the users in the PHR system into various security domains which greatly reduces the key organization difficulty for owners and users which are unlike from previous works in secure data outsourcing. 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.

Keywords: Data security, Physical Health Record, Scalable data access, Attribute based encryption technique.

1. INTRODUCTION:

Cloud Computing has by now drawn great consideration, and its benefits have payed an attention to the increasing number of users to outsource their local data centers to remote cloud servers. Data security is a significant issue for remote data storage. On one hand, revelation of responsive information, such as health files, stored on remote data servers has to be severely protected before users have freedom to use the data services [4]. Modern advances in IT have very much facilitated remote data storage and sharing. Fine-grained data access control mechanisms frequently need to be in place to promise appropriate disclosure of responsive data among multiple users. On the other hand, in remote data storage users do not actually possess their data. Remote data service providers are almost convinced to be outside the users' trust domain, and are not authorized to gain knowledge of users' responsive information stored on their servers [9]. 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 [1] [8]. The exclusive challenges brought by multiple Personal health records owners and users, by the frame addresses in which the complexity of key management is greatly reduced by improving the privacy and guarantees the compared with previous works. 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. 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 [12]. There are many safety and confidentiality threats which could obstruct its wide acceptance while it is exciting to have suitable PHR services for everyone is shown in Fig 1.

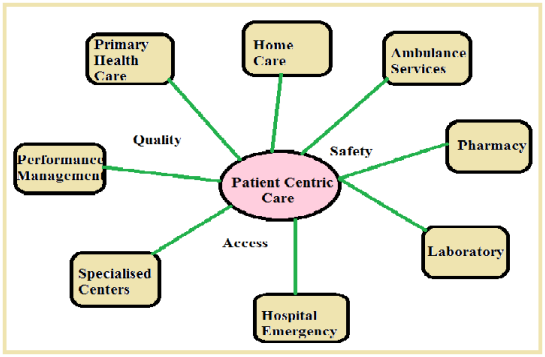

Fig1: An overview of Personal Health Care

2. METHODOLOGY:

In recent times, for electronic healthcare records systems an attribute-based infrastructure is proposed, where each patient's electronic healthcare records files are encrypted using a broadcast variation of cipher text policy attribute-based encryption that allows direct revocation [7]. However, there are numerous frequent limitations of the above works. First, the use of a single trusted authority in the system is usually assumed. 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 [15]. 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. The use of a single trusted authority in the system is usually assumed. In addition, generating secure keys to assign all attribute organization responsibilities to one trusted authority is not sensible, including certifying all users' attributes or roles [2] [13]. In fact, to certify various sets of attributes that fit in their domains become appropriate authorities as dissimilar organizations usually form their own domains. Assigning of the entire responsibilities of the attribute organization to a single trusted authority is not considered sensible in generating the secure keys. 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 [5] [10]. 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 identify the cryptographically imposed access to the patient centric personal health record, attribute based encryption was recognized in both the types of safety domains. To an autonomous sector in the society like health care, the domains of the public can be mapped [14]. 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. 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 [6]. In addition, generating secure keys to assign all attribute organization responsibilities to one trusted authority is not sensible, including certifying all users' attributes or roles. As various organizations normally form their own domains, various sets of attributes belonging to their domains become appropriate authorities to certify them. There are various attribute authorities for each leading a displace subset of attributes in a public domain multi authority attribute based encryption. For dynamic policy updates/changes there still lack an efficient and on-demand user revocation mechanism for attribute-based encryption with the support, which are essential parts of safe personal health record distribution [3] [11]. Finally, most of the previous works have dissimilar attribute definitions as they do not distinguish between the individual and public domains key organization necessities and scalability issues.

3. RESULT:

We have proposed a new framework of protected allocation of health records within cloud computing. We have estimated the scalability and effectiveness of our solution in terms of storage space, communication and computation costs. The scalability and competence of our elucidation 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. 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 computation cost of the server was replicated in the user revocation to measure the performance of the system of the revocation of the user.

4. CONCLUSION:

A novel frame of safe distribution of personal health records in cloud computing has been proposed in this paper. Considering partially trustworthy cloud servers, to allow

fine-grained access, we dispute to fully realize that the patient-centric concept shall have absolute control of their individual confidentiality all the way through encrypting their Personal health records files. 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. 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. By the frame addresses the exclusive challenges brought by multiple Personal health records owners and users, in which the complexity of key management is greatly reduced by improving the privacy and guarantees the compared with previous works. To encrypt the Personal health records data we utilize attribute-based encryption, so that patients can permit right of entry not only by personal users except with various users from public domains.

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.