IJRRECS/June 2014/Volume-2/Issue-6/2477-2482 **ISSN 2321-5461**

INTERNATIONAL JOURNAL OF REVIEWS ON RECENT ELECTRONICS AND COMPUTER SCIENCE

IMPLEMENTATION OF SECLUDED HEALTH DATA IN CLOUD ENVIRONMENT

Pelluri Rama[1], K.Anusha[2]

[1]**M.Tech Student, Dept of CSE, RRS College of Engineering & Technology, Muthangi (V), Patancheru (M), Hyderabad, T.S, India**

[2]**Assistant Professor, Dept of CSE, RRS College of Engineering & Technology, Muthangi (V), Patancheru (M), Hyderabad, T.S, India**

ABSTRACT:

The objective of patient-centric privacy is regularly in variance with scalability in a personal health record system. There has been a growing concentration in applying attribute based encryption to safe electronic healthcare records. A novel attribute based encryption based structure was introduced for patient-centric secure contribution of health records in cloud computing setting, under situation of multi-owner. The introduced system put into effect write access control, handles active policy updates, and makes available break-glass access to health records under emergence situation and makes available protected patient-centric health record access and well-organized key management. In a public domain multi-authority attribute based encryption is employed, where numerous attribute authorities in which each governing a disjoint subset of aspect. The multi-domain scheme best models dissimilar user category and access needs in a health record system. In public domain, we make use of multi-authority attribute based encryption to recover the protection and keep away from key escrow difficulty. To accomplish patient-centric health record sharing, a core prerequisite is that every patient can manage who are allowed to access to their health records documents.

Keywords: Electronic healthcare records, Access control, Public domain, Multi-authority attribute based encryption.

1. INTRODUCTION:

To recognize fine-grained access control, the conventional public key encryption based systems moreover acquire high key management transparency, or necessitate encrypting numerous copies concerning file by various users' keys [4]. Quite a lot of efforts used attribute based encryption to understand fine-grained accession control in support of outsourced data. A practicable approach is to encrypt data earlier than outsourcing. Service of personal health record permit a patient to generate, supervise, and manage individual health information at particular place all the way through the web, which has made accumulating, recovery, and sharing of medical information more resourceful. Due to high value of responsive personal health information, third-party storage servers are regularly targets of a variety of malevolent behaviours which might guide to spotlight of personal health information [8]. The objective of patient-centric privacy is regularly in variance with scalability in a personal health record system. The authorized users might either necessitate accessing the personal health record for individual use or specialized purposes. dissimilar from particular data owner situation measured in existing works in a personal health record system, there are numerous owners who might encrypt consistent with their individual ways, perhaps using dissimilar sets of cryptographic keys. There has been a growing concentration in applying attribute based encryption to safe electronic healthcare records [1]. To defend personal health information accumulated on a semi-trusted server, attribute-based encryption was adopted as most important encryption primitive. To put together attribute based encryption into an extensive personal health record system as shown in fig1, significant issues such as scalability of key management, updates of dynamic policy, and resourceful on-demand revocation are non-trivial to stay on largely open state-of-the-art [11].

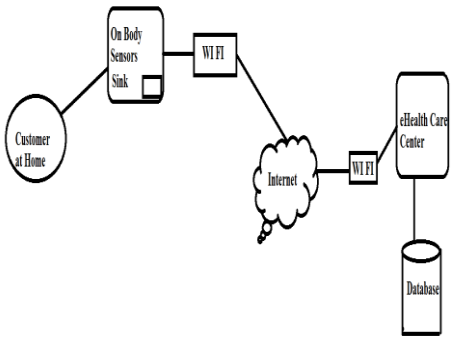

Fig 1: Secure Sharing of Personal Health Care Records

2. METHODOLOGY:

In the recent times, personal health record has come into view as representation of patient-centric concerning health information exchange [6]. Due to extreme outlay of maintaining specific data centers, numerous health record services are offered by means of providers of third-party service. A novel attribute based encryption based structure was introduced for patient-centric secure contribution of health records in cloud computing setting, under situation of multi-owner [3]. Introduced structure handle various types of health record sharing applications' needs, while incur negligible key management transparency for owner as well as users. The introduced system put into effect write access control, handles active policy updates, and makes available break-glass access to health records under emergence situation and makes available protected patient-centric health record access and well-organized key management [14]. Division of system into numerous security domains consistent with different users' data access needs is the conception. For every personal domain, its users are individually connected through a data owner, and they build access to health records based on access rights allocated by the owner [13]. The public domain consists of users who make accession based on specialized roles. A public domain is mapped to an autonomous sector. In a public domain multi-authority attribute based encryption is employed, where numerous attribute authorities in which each governing a disjoint subset of aspect [9]. Role attributes are described for public domain representing the specialized responsibility of a public domain user. As public domain contains bulk of users, it to a great extent reduces key management transparency for the owner in addition to users. For persona domain, data attributes are described referring towards intrinsic property of health record data. For the function of personal domain access, every health record file is labelled with its data features; while key size is merely linear with file category a user can access [7]. Users in public domain get hold of their attribute-based secret keys from attribute authority, devoid of interacting with owners. To control access from public domain users, owners are open to identify access policies of role-based fine-grained for files of health records, while do not require to recognize listing of approved users when undertaking encryption [2]. Every data owner is a confidential authority of

individual personal domain, making use of a KP-ABE scheme to handle the undisclosed keys and access rights concerning users in individual personal domain. In view of the fact that the users are known by health record owner, to understand patient-centric access, possessor is at finest position to grant user access rights on case-by-case basis. The multi-domain scheme best models dissimilar user category and access needs in a health record system [16]. The use of attribute based encryption makes encrypted health records service defensive. In public domain, we make use of multi-authority attribute based encryption to recover the protection and keep away from key escrow difficulty. Each attribute authority in it manage a disjoint subset concerning user role attributes, as none of them alone is capable to manage the protection of complete system [12]. In personal domain, owners unswervingly allocate access privileges in support of personal users and encrypt file of health record under its data aspects. To accomplish patient-centric health record sharing, a core prerequisite is that every patient can manage who are allowed to access to their health records documents. The security needs are: Data privacy in which unauthorized users who does not hold adequate attributes fulfilling the access policy or do not contain appropriate key access privileges have to be prohibited from decrypting a health record document, still under user collusion [5]. Fine-grained accession control is enforced; dissimilar users are approved to read various sets of documents. Scalability as well as efficiency: health record system should support users from personal and public domains. Since set of users from public domain could be huge in size and changeable, the system has to be extremely scalable, in terms of difficulty in key management and storage [15]. Write access control: the unauthorized contributors were prevented to expand write-access towards owners' health records, while lawful contributors have to access server with responsibility. On-demand revocation: when a user's quality is no longer applicable the user has to not be capable to access upcoming health records files by means of that quality [10]. This is typically called attribute revocation, and equivalent protection asset is forward secrecy.

3. RESULTS:

Security of introduced health record was analysed and it attain data confidentiality, by

means of confirming enhanced multi authority attribute based encryption system to be protected under representation of attribute-based selective-set. The security of introduced system was measured in terms of privacy assurance, access control granularity with quite a lot of existing works. Introduced structure particularly addresses the access needs in cloud-based systems of health record management by rationally dividing system into public and personal domains, which consider individual and specialized health record users. Enhanced multi authority attribute based encryption system assurance data privacy of health record information against unofficial users and curious provider of cloud service. Introduced system attains forward confidentiality and protection of write access control and achieves high confidentiality assurance as well as on demand revocation.

4. CONCLUSION:

To put together attribute based encryption into an extensive personal health record system, significant issues such as scalability of key management, updates of dynamic policy, and resourceful on-demand revocation are non-trivial to stay on largely open state-of-the-art. Introduced structure handle various types of health record sharing applications' needs, while incur negligible key management transparency for owner as well as users. Division of system into numerous security domains consistent with different users' data access needs is the conception of the system and for every personal domain, its users are individually connected through a data owner, and they build access to health records based on access rights allocated by the owner. For the function of personal domain access, every health record file is labelled with its data features, while key size is merely linear with file category a user can access. To control access from public domain users, owners are open to identify access policies of role-based fine-grained for files of health records, while do not require to recognize listing of approved users when undertaking encryption. Introduced structure particularly addresses the access needs in cloud-based systems of health record management by rationally dividing system into public and personal domains, which consider individual and specialized health record users.

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] Scalable and Secure Sharing of Personal Health Records in Cloud Computing using Attribute-based Encryption Ming Li, Shucheng Yu,Yao Zheng, Kui Ren, and Wenjing Lou,,2012

[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.

[16] 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/.