Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 2, February 2014, pg.617 – 625

RESEARCH ARTICLE

Scalable and Secure Sharing of Personal Health Records in Cloud Computing using Attribute-Based Encryption

Prof. Y. B. Gurav[1], **Manjiri Deshmukh**[2]

[1]Computer&Pune university, India

[2]Computer&Pune university, India

1 ybgurav@gmail.com 2 manjirideshmukh15@gmail.com

***Abstract**: Personal health record is maintain in the centralize server to maintain patient's personal and diagnosis information. Personal health record (PHR) is an emerging patient-centric model of health information exchange, which is often outsourced to be stored at a third party, such as cloud providers. However, there have been wide privacy concerns as personal health information could be exposed to those third party servers and to unauthorized parties. The security schemes are used to protect personal data from public access. To assure the patients' control over access to their own PHRs, it is a promising method to encrypt the PHRs before outsourcing .In this paper we propose novel patient-centric framework and suite of mechanism for data access control to PHR's stored in semi-trusted servers Yet, issues such as risks of privacy exposure, scalability in key management, flexible access and efficient user revocation, have remained the most important challenges toward achieving fine-grained, cryptographically enforced data access control. To achieve fine-grained and scalable data access control for PHRs, we leverage attribute based encryption (ABE) techniques to encrypt each patient's PHR file. Data owner update the personal data into third party cloud data centers. Multiple data owners can access the same data values. Different from previous works in secure data outsourcing, we focus on the multiple data owner scenario, and divide the users in the PHR system into multiple security domains that greatly reduces the key management complexity for owners and users. A high degree of patient privacy is guaranteed simultaneously by exploiting multi-authority ABE. Our scheme also enables dynamic modification of access policies or file attributes, supports efficient on-demand user/attribute revocation and break-glass access under emergency scenarios.*

Keyword—*Personal health records; cloud computing; data privacy; fine-grained access control; attribute-based encryption*

Full Text: http://www.ijcsmc.com/docs/papers/February2014/V3I2201499a29.pdf