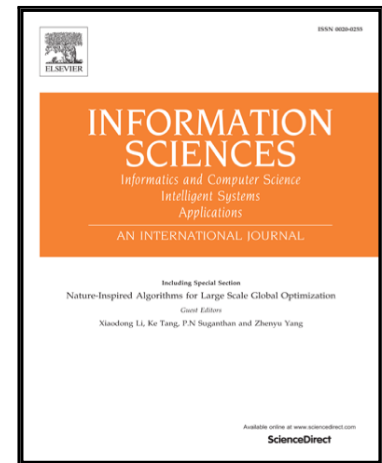


Accepted Manuscript

Dynamic Access Policy in Cloud-Based Personal Health Record (PHR) Systems

Xuhui Liu, Qin Liu, Tao Peng, Jie Wu

PII: S0020-0255(16)30457-1
DOI: [10.1016/j.ins.2016.06.035](https://doi.org/10.1016/j.ins.2016.06.035)
Reference: INS 12309



To appear in: *Information Sciences*

Received date: 15 November 2015
Revised date: 15 June 2016
Accepted date: 23 June 2016

Please cite this article as: Xuhui Liu, Qin Liu, Tao Peng, Jie Wu, Dynamic Access Policy in Cloud-Based Personal Health Record (PHR) Systems, *Information Sciences* (2016), doi: [10.1016/j.ins.2016.06.035](https://doi.org/10.1016/j.ins.2016.06.035)

This is a PDF file of an unedited manuscript that has been accepted for publication. As a service to our customers we are providing this early version of the manuscript. The manuscript will undergo copyediting, typesetting, and review of the resulting proof before it is published in its final form. Please note that during the production process errors may be discovered which could affect the content, and all legal disclaimers that apply to the journal pertain.

Dynamic Access Policy in Cloud-Based Personal Health Record (PHR) Systems

Xuhui Liu^a, Qin Liu^a, Tao Peng^b, Jie Wu^c

^a*College of Computer Science and Electronic Engineering
Hunan University*

Changsha, Hunan Province, P. R. China 410082

^b*School of Information Science and Engineering
Central South University*

Changsha, Hunan Province, P. R. China 410083

^c*Department of Computer and Information Sciences
Temple University
Philadelphia, PA 19122, USA*

Abstract

With the development of cloud computing, an increasing number of users are using cloud-based personal health record (PHR) systems. The PHR is closely tied to patient privacy, and thus existing studies suggest encrypting PHRs before outsourcing. Comparison-based encryption (CBE) was the first to implement time comparison in an attribute-based access policy by means of the forward and backward derivation functions. However, CBE cannot be directly applied to cloud-based PHR environments for the following reasons: First, the cost of encryption grows linearly with the number of attributes in the access policy. Second, policy updating incurs high communication and computation costs for the data owner. To efficiently implement a dynamic access policy for PHRs in clouds, we first propose a hierarchical comparison-based encryption (HCBE) scheme that incorporates an attribute hierarchy into CBE. The HCBE scheme encrypts a ciphertext with a small number of generalized attributes at a higher level rather than many specific attributes at a lower level, greatly improving the encryption performance. Using the HCBE scheme as a foundation, we then develop a dynamic policy updating (DPU) scheme by utilizing the proxy re-encryption (PRE) technique. The DPU scheme can avoid the transmission of ciphertexts and minimize the computation overhead on the data owner by delegating the policy updating operations to the cloud. Extensive experiments have been conducted using

Download English Version:

<https://daneshyari.com/en/article/4944807>

Download Persian Version:

<https://daneshyari.com/article/4944807>

[Daneshyari.com](https://daneshyari.com)