Accepted Manuscript

Cross-domain dynamic anonymous authenticated group key management with symptom-matching for e-health social system

Yang Yang, Xianghan Zheng, Ximeng Liu, Shangping Zhong,
Victor Chang

PII: S0167-739X(17)30554-X
DOI: http://dx.doi.org/10.1016/j.future.2017.06.025
Reference: FUTURE 3523

To appear in: *Future Generation Computer Systems*

Received date : 4 April 2017
Revised date : 8 May 2017
Accepted date : 20 June 2017

Please cite this article as: Y. Yang, X. Zheng, X. Liu, S. Zhong, V. Chang, Cross-domain dynamic anonymous authenticated group key management with symptom-matching for e-health social system, *Future Generation Computer Systems* (2017), http://dx.doi.org/10.1016/j.future.2017.06.025

Cross-domain Dynamic Anonymous Authenticated Group Key Management with Symptom-matching for E-health Social System

Yang Yang[a,b,c], Xianghan Zheng[a,*], Ximeng Liu[a,b], Shangping Zhong[a,b], Victor Chang[d]

[a] *College of Mathematics and Computer Science, Fuzhou University, Fuzhou, China, 350116.*
[b] *University Key Laboratory of Information Security of Network Systems (Fuzhou University), Fujian Province, China, 350116.*
[c] *Fujian Provincial Key Laboratory of Information Processing and Intelligent Control (Minjiang University), Fuzhou China, 350121.*
[d] *IBSS, Xian Jiaotong-Liverpool University, Suzhou, China, 215123.*

Abstract

Electronic health (e-health) social system provides an effective way for the patients to share their treatment experience, exchange medical information and build a supportive relationship. In this paper, we propose a novel symptom-matching based group key management scheme for the e-health social system supporting dynamic group membership change. The patients in this system are diagnosed and treated by different medical institutions. This proposed schemes allows a group of patients from different healthcare domains (cross-domain) to securely establish a group session key to protect the group disease discussion. The scheme supports patient anonymity and traceability since the identities of the patients are hidden in an anonym and their medical institution is able to recover the real identity. The group agreement protocol ensures that only the authenticated patient with the same symptom could derive the group session key. The privacy of patient's symptom is also protected since the patient can not know the other patients' symptoms if they do not have the same symptom. The security of this scheme is proved and the performance is evaluated theoretically

[*] Corresponding author
Email addresses: yang.yang.research@gmail.com (Yang Yang), xianghan.zheng@fzu.edu.cn (Xianghan Zheng), snbnix@gmail.com (Ximeng Liu), spzhong@fzu.edu.cn (Shangping Zhong), ic.victor.chang@gmail.com (Victor Chang)