Accepted Manuscript

Secure smart health with privacy-aware aggregate authentication and access control in Internet of Things

Yinghui Zhang, Robert H. Deng, Gang Han, Dong Zheng

PII: S1084-8045(18)30293-5

DOI: 10.1016/j.jnca.2018.09.005

Reference: YJNCA 2205

To appear in: *Journal of Network and Computer Applications*

Received Date: 18 June 2018

Revised Date: 20 August 2018

Accepted Date: 14 September 2018

Please cite this article as: Zhang, Y., Deng, R.H., Han, G., Zheng, D., Secure smart health with privacy-aware aggregate authentication and access control in Internet of Things, *Journal of Network and Computer Applications* (2018), doi: https://doi.org/10.1016/j.jnca.2018.09.005.

Secure Smart Health with Privacy-Aware Aggregate Authentication and Access Control in Internet of Things

Yinghui Zhang[a,b,c,d], Robert H. Deng[c], Gang Han[a,e,*], Dong Zheng[a,d]

[a] *National Engineering Laboratory for Wireless Security, Xi'an University of Posts and Telecommunications, Xi'an 710121, China*
[b] *State Key Laboratory of Cryptology, P.O. Box 5159, Beijing 100878, P.R. China*
[c] *School of Information Systems, Singapore Management University, Singapore*
[d] *Westone Cryptologic Research Center, Beijing 100070, China*
[e] *School of Electronics and Information, Northwestern Polytechnical University, Xi'an 710129, China*

Abstract

With the rapid technological advancements in the Internet of Things (IoT), wireless communication and cloud computing, smart health is expected to enable comprehensive and qualified healthcare services. It is important to ensure security and efficiency in smart health. However, existing smart health systems still have challenging issues, such as aggregate authentication, fine-grained access control and privacy protection. In this paper, we address these issues by introducing SSH, a Secure Smart Health system with privacy-aware aggregate authentication and access control in IoT. In SSH, privacy-aware aggregate authentication is enabled by an anonymous certificateless aggregate signature scheme, in which users' identity information is protected based on symmetric encryption mechanisms. In addition, privacy-aware access control is based on anonymous attribute-based encryption technologies. Our formal security proofs indicate that SSH achieves batch authentication and non-repudiation under the Computational Diffie-Hellman assumption. Extensive experimental results and performance comparisons show that SSH is practical in terms of computation cost and communication overheads.

Keywords: Smart health, Security, Privacy, Aggregate authentication,

*Corresponding author.
Email addresses: yinghuizhang@smu.edu.sg (Yinghui Zhang), robertdeng@smu.edu.sg (Robert H. Deng), hangang021@gmail.com (Gang Han), zhengdong@xupt.edu.cn (Dong Zheng)