Accepted Manuscript

Verifiable keyword search for secure big data-based mobile healthcare networks with fine-grained authorization control

Zehong Chen, Fangguo Zhang, Peng Zhang, Joseph K. Liu, Jiwu Huang, Hanbang Zhao, Jian Shen

PII: S0167-739X(17)30073-0
DOI: https://doi.org/10.1016/j.future.2017.10.022
Reference: FUTURE 3761

To appear in: *Future Generation Computer Systems*

Received date : 16 January 2017
Revised date : 30 September 2017
Accepted date : 14 October 2017

Please cite this article as: Z. Chen, F. Zhang, P. Zhang, J.K. Liu, J. Huang, H. Zhao, J. Shen, Verifiable keyword search for secure big data-based mobile healthcare networks with fine-grained authorization control, *Future Generation Computer Systems* (2017), https://doi.org/10.1016/j.future.2017.10.022

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.

ACCEPTED MANUSCRIPT

Verifiable Keyword Search for Secure Big Data-based Mobile Healthcare Networks with Fine-Grained Authorization Control

Zehong Chen[a], Fangguo Zhang[b], Peng Zhang[c,*], Joseph K. Liu[d], Jiwu Huang[a], Hanbang Zhao[c], Jian Shen[e]

[a] *College of Information Engineering and Shenzhen Key Laboratory of Media Security, Shenzhen University, Shenzhen, China*
[b] *School of Data and Computer Science and Guangdong Key Laboratory of Information Security, Sun Yat-sen University, Guangzhou, China*
[c] *College of Information Engineering and ATR Key Laboratory of National Defense Technology, Shenzhen University, Shenzhen, China*
[d] *Faculty of Information Technology, Monash University, Melbourne, Australia*
[e] *College of Computer and Software, Nanjing University of Information Science and Technology, Jiangsu, China*

Abstract

Mobile healthcare networks (MHNs) are increasingly viewed as potential applications for further improving the quality and efficiency of healthcare, with the rapid development of wearable devices. Wearable devices can generate a huge amount of health data, causing big data to be one of the most prominent features. The privacy and security of big data-based MHNs are major concerns of users, and these are the overriding obstacles that stand in the way of the wider adoption of MHNs. For the sake of security, health data is encrypted and stored on an untrusted server. However, the flexibility of the data is thereby affected, such as a search over encrypted health data, or authorization control for a search and verification of the search result. To address these problems, we propose a verifiable keyword search scheme for big data-based MHNs with fine-grained authorization control. In the proposed scheme, when sending the search request to the healthcare provider for the first time, the user needs to check whether he or she has the right to search within encrypted health data. Only authorized users can generate valid trapdoors for searching. Our verification technique is constructed based on an invertible Bloom lookup table and a Merkle hash tree, which can verify the completeness and correctness of the search result even if an empty set is returned by a dishonest healthcare provider. The security analysis shows that the proposed scheme is secure against chosen keyword attacks. The proposed scheme is efficient with low computation load, which can be used to perform keyword searches and verify the search results quickly in a big data environment.

Keywords: Mobile healthcare networks, big data, verifiable keyword search, authorization control, invertible Bloom lookup table.

*Corresponding author
Email addresses: zhchen@szu.edu.cn (Zehong Chen), isszhfg@mail.sysu.edu.cn (Fangguo Zhang), zhangp@szu.edu.cn (Peng Zhang), joseph.liu@monash.edu (Joseph K. Liu), jwhuang@szu.edu.cn (Jiwu Huang), elifezhao@gmail.com (Hanbang Zhao), s_shenjian@126.com (Jian Shen)

Download English Version:

https://daneshyari.com/en/article/6872957

Download Persian Version:

https://daneshyari.com/article/6872957

Daneshyari.com