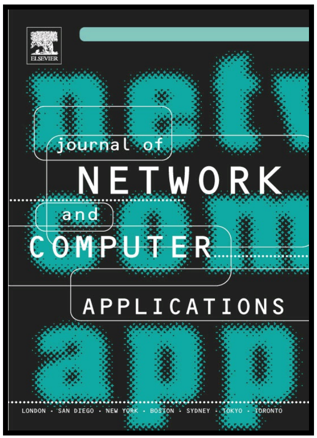
journal of
NETWORK
and
COMPUTER
APPLICATIONS
LONDON • SAN DIEGO • NEW YORK • BOSTON • SYDNEY • TOKYO • TORONTO

www.elsevier.com/locate/jnca

Lightweight Distributed Secure Data Management System for Health Internet of Things

Yang Yang, Xianghan Zheng, Chunming Tang

PII: S1084-8045(16)30285-5
DOI: http://dx.doi.org/10.1016/j.jnca.2016.11.017
Reference: YJNCA1768

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

Received date: 22 September 2016
Revised date: 12 November 2016
Accepted date: 16 November 2016

Cite this article as: Yang Yang, Xianghan Zheng and Chunming Tang, Lightweight Distributed Secure Data Management System for Health Internet o Things, *Journal of Network and Computer Applications* http://dx.doi.org/10.1016/j.jnca.2016.11.017

Lightweight Distributed Secure Data Management System for Health Internet of Things

Yang Yang, Xianghan Zheng*, Chunming Tang

Abstract—Internet of Things (IoT) connects various kinds of sensors and smart devices using the internet to collect data. The adoption of IoT in medical care field will bring great convenient to both doctors and patients for effective illness monitoring and diagnosis. Due to the high value of medical data and the openness character of health IoT, the protection of data confidentiality is of crucial importance. In this paper, we propose a novel distributed secure data management with keyword search system for health IoT. Since the patients are usually managed by diverse medical institutions, the proposed system enables distributed access control of protected health information (PHI) among different medical domains. On the other hand, the accumulation of electronic health records (EHR) makes effective data retrieval a challenge task. Our scheme could provide efficient keyword search function on cross-domain PHI. For the resource limited devices in health IoT, it is an essential requirement to design lightweight algorithms in the secure data management system. The proposed system realizes lightweight data encryption, lightweight keyword trapdoor generation and lightweight data recovery, which leaves very few computations to user's terminal. The security of this system is reduced to the decisional bilinear Diffie-Hellman (DBDH) assumption. The comparison analysis is made between this scheme and other existing systems. The extensive experiments on both laptop and smart phone platforms show that the proposed scheme has greatly improved the computation efficiency and requires much less communication cost.

Index Terms—Health Internet of Things, searchable encryption, distributed access control, attribute based encryption, lightweight computation

1 INTRODUCTION

INTERNET of Things (IoT) has emerged as a pervasive infrastructure of the information society that enables physical sensors, smart phones and smart buildings to interconnect with each other [1]. These electronic devices communicate through wired or wireless channels to gather and exchange data [2]. With the development of IoT, anything can be connected from anywhere, at anytime and could provide almost any service. These advantages of ubiquitous IoT ensure that it can be utilized in a wide range of application scenarios, such as smart homes and cities, smart vehicle networks and smart environment monitoring.

The establishment of e-health record (EHR) system provides a good opportunity to enhance the safety and quality of medical care, improve continuity and health service for patients as well as reduce time and costs. It have permeated in the medical domain due to its convenience in managing and sharing the health information. Great opportunities will be offered by IoT to revolutionize e-health system. The health IoT [3] could connect various health care devices and enable remote physiological information monitoring, chronic diseases diagnosis, rehabilitation training and elderly care. Meanwhile, health IoT can remarkably increase the healthcare quality and decrease the medical cost.

Since the conception of IoT was put forth, widespead concerns are aroused to promote the network performance, transmission speed and smart data analyzing [4], [5]. Nevertheless, the sharing of EHR through IoT arises a series of privacy and security concerns [6], [7]. The gigantic volumes of confidential EHR are stored on a third-party data server and transmitted over IoT. Such system will be vulnerable to eavesdropping and tampering. Although HIPAA (Health Insurance Portability and Accountability Act) [8] mandates the disclosure and secure exchange of electronic health information in USA, the multi-hop wireless communication mode in health IOT can not prevent the eavesdropping attack. How to ensure the privacy and security of the highly sensitive personal health information in IoT without reducing the data usability remains a problem to be solved [9], [10].

In public health IoT, remote access control is a crucial approach to prevent unauthorized entity from accessing the EHR. To protect the information confidentiality, the EHR are usually encrypted to ciphertext and then uploaded to the remote server for storage. If the user's condition satisfies the designated access policy of the protected EHR, the health document can be recovered. Attribute based encryption (ABE) system is a desire approach to implement the

- *Y. Yang works for College of Mathematics and Computer Science, Fuzhou University, Fuzhou, China. She is also affiliated with Key Laboratory of Information Security, School of Mathematics and Information Science, Guangzhou University, Guangzhou 510006, China.*
- *X. Zheng is with College of Mathematics and Computer Science, Fuzhou University, Fuzhou, China.*
- *Chunming Tang is with Key Laboratory of Information Security, School of Mathematics and Information Science, Guangzhou University, Guangzhou, 510006, China.*
- **: Corresponding Author.*

Manuscript received April 19, 2005; revised September 17, 2014.