IEEE Transactions on Industrial Informatics, Vol:13, June 2017

Private and Secured Medical Data Transmission and Analysis for Wireless Sensing Healthcare System

Haiping Huang, *Member, IEEE*, Tianhe Gong, Ning Ye, Ruchuan Wang and Yi Dou

***Abstract*—The convergence of Internet of Things (IoT), cloud computing and wireless body-area networks (WBANs) has greatly promoted the industrialization of e-/m-healthcare (electronic-/mobile-healthcare). However, the further flourishing of e-/m-Healthcare still faces many challenges including information security and privacy preservation. To address these problems, a healthcare system (HES) framework is designed that collects medical data from WBANs, transmits them through an extensive wireless sensor network infrastructure and finally publishes them into wireless personal area networks (WPANs) via a gateway. Furthermore, HES involves the GSRM (Groups of Send-Receive Model) scheme to realize key distribution and secure data transmission, the HEBM (Homomorphic Encryption Based on Matrix) scheme to ensure privacy and an expert system able to analyze the scrambled medical data and feed back the results automatically. Theoretical and experimental evaluations are conducted to demonstrate the security, privacy and improved performance of HES compared with current systems or schemes. Finally, the prototype implementation of HES is explored to verify its feasibility.**

***Index Terms*—Internet of Things, healthcare system, wireless sensor network, security, privacy protection, key distribution**

I. Introduction

THE rapid technological convergence of Internet of Things (IoT), wireless body-area networks (WBANs) and cloud computing has caused e-healthcare (electronic-healthcare) to emerge as a promising information-intensive industrial application domain that has significant potential to improve the quality of medical care [1]. Therefore, how to achieve medical data collection, transmission, processing and presentation has become a critical issue in e-healthcare applications, in which a variety of wireless sensor nodes and terminal devices play important roles in network data aggregation and communications. Furthermore, the evolution of m-health (mobile-health) technology has made it possible for people to gather information concerning their health status easily, anytime and anywhere using smart mobile devices [2]. However, these medical data consist of personal private information that should not be susceptible to eavesdropping or malicious tampering during transmission. Therefore, the privacy protection and secure transmission of e-/m-healthcare (electronic-/mobile-healthcare) data has drawn more attention from many researchers. A secure and reliable e-/m-healthcare framework to defend against hostile attacks and threats is highlighted for available applications of the informationalized healthcare industry. Moreover, a challenge remains concerning how to effectively process the ever-growing volume of healthcare data and protect data privacy but maintain low sensor network overhead [3]. Due to the resource-strained characteristics (such as limited power) of mobile devices and sensors, the tradeoff between efficiency and privacy or security must be further balanced for the commercial promotion of e-/m-healthcare. Therefore, a meaningful concern of this paper is the design of a feasible, efficient and privacy-guaranteed e-/m-healthcare information system employing wireless sensor networks.

Most current e-/m-healthcare systems require doctors (or system administrators) to participate in medical information processing, which brings two problems: low effectiveness caused by manual operations and privacy breaches due to doctors' acquaintance with users' private data. A medical expert system that can automatically analyze users' scrambled private data but minimize doctors' participation can address these two problems, particularly for the application of general physical examinations. Even with perfect access control mechanisms, frequent human intervention will always cause a higher risk of privacy disclosure in e-/m-healthcare. As a major component of e-/m-healthcare systems, the development of a medical expert system is another focus of this paper.

Various implantable and network-oriented medical devices such as medical sensors and body-area network components are considered in e-/m-healthcare systems [4]. However, a practical market survey on medical instruments illustrates that most current wearable medical devices and nodes cannot be directly

This work was supported by the National Natural Science Foundation of P. R. China (No. 61672297, 61373017 and 61373138), the Key Research and Development Program of Jiangsu Province (Social Development Program, No.BE2015702), Postdoctoral Foundation (No. 2015M570468 and 2016T90485), The Sixth Talent Peaks Project of Jiangsu Province (No. DZXX-017), Jiangsu Natural Science Foundation for Excellent Young Scholar(No. BK20160089).

H. P. Huang, T. H. Gong, N. Ye and R. C. Wang are with the School of Computer Science and Technology, Nanjing University of Posts and Telecommunications, Nanjing 210003, China (e-mail: hhp@njupt.edu.cn; g405252865@163.com; yening@njupt.edu.cn; wangrc@njupt.edu.cn; corresponding author: H. P. Huang, phone: 86-13813826704; fax: 86-25-83492152; e-mail: hhp@njupt.edu.cn).

Y. Dou is with the Department of Computing, The Hong Kong PolyTechnic University, Hung Hom, Kowloon, Hong Kong (e-mail: csydou@comp.polyu.edu.hk).