Secure and Efficient E-health Scheme Based on the Internet of Things

Zaid Alaa Hussien[1,2], Hai Jin[1], Zaid Ameen Abduljabbar[1,3], Mohammed Abdulridha Hussain[1,3],
Ali A. Yassin[3], Salah H. Abbdal[1], Mustafa A. Al Sibahee[4], Deqing Zou[1]
[1]Cluster and Grid Computing Laboratory
Services Computing Technology and System Laboratory
School of Computer Science and Technology
Huazhong University of Science and Technology, Wuhan, 430074, China
[2]Southern Technical University, Basrah, Iraq
[3]University of Basrah, Basrah, Iraq
[4]Huazhong University of Science and Technology
zaidpc2005@gmail.com, hjin@hust.edu.cn

***Abstract*—Internet of Things is a new generation of network service platform that allows everyday objects including small devices in sensor networks to be capable of connecting to the internet. Such an innovative technology can lead to positive changes in human life. An e-health service based on the Internet of Things has great potential. The popularity of intelligent mobile medical devices, wearable bio-medical sensor devices, cloud computing, and big data analysis have dramatically changed the usage pattern and business rule of e-health services based on the Internet of Things. The rapid development of e-health services based on the Internet of Things poses risks in security and privacy. In this study, we propose a new security scheme for an e-health service. This scheme allows both the local base station and hospital cloud server to authenticate each other, to secure the collection of health data. Our scheme uses the crypto hash function to check the integrity of authentication exchanges. In addition, it provides mutual authentication with anonymity and terminates with a session key agreement between each local base station and the hospital cloud server. To assess our scheme, we conduct performance and security analysis. Results show that our scheme is secure, lightweight, and resistant to different types of attacks.**

***Keywords*—Internet of Things; e-health; data privacy; anonymity; key session agreement**

I. INTRODUCTION

The *Internet of Things* (IoT) refers to a recent paradigm that has rapidly gained ground in the area of modern wireless telecommunications. IoT is a new technological trend alongside new computing and communications paradigms [1]. This new trend consists of intelligent devices that have a digital entity and are ubiquitously interconnected to a network and to the global Internet [2]. Everyday objects may integrate intelligence and the ability to sense, interpret, and react to their environment, combining the Internet with emerging technologies, such as *radio-frequency identification* (RFID) [3], real-time location, and embedded sensors. The IoT concept is based on the idea of a universal presence of things or objects, such as RFID tags, sensors, actuators, mobile phones, with digital identification and addressing schemes that enable them to cooperate with neighbours to achieve some common goals. In the business sector, the most apparent consequences of IoT may arise in industrial automation and manufacturing, logistics, business or process management, and intelligent schemes for transporting people and goods. Therefore, the term IoT generally refers to any type of device interconnected by means of object-to-object communications, each of which may be identified through a unique ID and defined through a virtual representation within the Internet [4].

The deployment of IoT opens doors to a huge number of applications that can significantly improve our daily life. Among them, e-health applications are gaining more and more attention [5]. An e-health system is a radio frequency-based wireless networking system that provides ubiquitous networking functionalities. It is based on the interconnection of tiny nodes enhanced with sensing and/or actuating capabilities planted in, on, or around a human body. E-health applications are context-aware, personal, dynamic, and anticipative. Given that IoT meets all these characteristics, it provides a suited environment for their efficient deployment. In fact, extensive research on the use of the IoT paradigm in e-health has recently been reported [6]. Population aging and the increase of survival chances from disabling illnesses lead to an increased demand from the current population, which requires continuous e-health [7].

E-health applications could spare a patient from long stays in hospitals, which is especially sought in emerging countries that lack medical infrastructure and well-trained personnel. Additionally, continuous monitoring anticipates emergency situations, thereby allowing the rapid and effective intervention of health teams. Moreover, early stage diagnostics can also be achieved remotely [8]. In summary, e-health applications in the context of IoT constitute a cost-effective and unobtrusive solution, without interrupting the patients everyday activities. Nevertheless, their deployment can be hindered when privacy challenges are not addressed efficiently. Given that health data are highly sensitive [9] [10] have underlined that e-health applications may be more vulnerable to attacks than other IoT applications. In fact, health-related data are private in nature, and any breach in the confidentiality of personal captured data seriously repels patients from adopting e-health solutions. For instance, many people do not like their health personal information, such as the early stage of pregnancy or details of

978-1-5090-2708-8/16/$31.00 ©2016 IEEE