Computers in Human Behavior xxx (2014) xxx–xxx

Contents lists available at ScienceDirect

Computers in Human Behavior

journal homepage: www.elsevier.com/locate/comphumbeh

Human-oriented design of secure Machine-to-Machine communication system for e-Healthcare society

Kashif Saleem [a,*], Abdelouahid Derhab [a], Jalal Al-Muhtadi [b], Basit Shahzad [b]

[a] King Saud University (KSU), Riyadh, Saudi Arabia
[b] College of Computer and Information Sciences (CCIS), King Saud University (KSU), Riyadh, Saudi Arabia

ARTICLE INFO

Article history:
Available online xxxx

Keywords:
e-Healthcare
Machine to Machine communication
Malicious
Psychological
Security
Society

ABSTRACT

In this paper, we propose a Machine to Machine (M2M) Low Cost and Secure (LCS) communication system for e-Healthcare society. The system is designed to take into consideration the psychological issues related to all actors in the e-Healthcare society such as: stress due to high workload, anxiety, and loneliness. The system is capable of performing most of the tasks in an autonomous and intelligent manner, which minimizes the workload of medical staffs, and consequently minimizes the associated psychological stress and improves the quality of patient care as well as the system performance. We show how the different actors in the e-Healthcare society can interact with each other in a secure manner. To ensure data privacy, the mechanism involves intelligent authentication based on random distributive key management, electronic certificate distribution, and modified realm Kerberos. The system handles dynamic assignments of doctors to specific patients. It also addresses the need for patients to share their health information with strangers while dealing with the privacy preservation issue. Finally, the simulation type implementation is performed on Visual Basic .net 2013 that shows the success of the proposed Low Cost and Secure (LCS) algorithm.

1. Introduction

Providing a high quality patient care has always been a concern for healthcare community. There are many factors, which contribute to the high cost and low-quality of support offered to patients. Nursing facilities that assist patients through caregiver intervention and monitoring of the patient's health are costly. In addition, it represents a burden on caregiver who is unable to ensure continuous monitoring of the patient, which incurs low quality of care offered to the patients.

The appearance of e-Healthcare systems has contributed in improving the quality of patient care and reducing the healthcare costs. By e-Healthcare system, we mean a set of electronic tools: software and hardware designed to manage data in the healthcare system. The main components of the e-Healthcare system include telemedicine, electronic health records, communication protocol among the components of the system.

Advances in the fields of sensor technologies, wireless networking technologies such as 3G, Wi-Fi, WiMax, Mesh networking, and personal area technologies such as radio frequency identification (RFID) and Bluetooth have enabled the creation of a smart e-Healthcare system, in which the medical staff can efficiently manage the health of the patients. Connecting tiny, low-power, and wearable smart medical sensor devices (e.g., pulse oximeters (Inc., 2014), electrocardiographs (Fulford-Jones, Gu-Yeon, & Welsh, 2004), and accelerometers (Mathie, Coster, Lovell, & Celler, 2004)) to a human body has advanced the healthcare systems and allowed the appearance of potential applications such as: home monitoring for chronic and elderly patients (Dishman, 2004), real-time continuous patient monitoring in hospitals (Van Laerhoven et al., 2004), automated vital sign analysis to reduce the incidents due to human error (Ohmura et al., 2006), and emergency situations (Lorincz et al., 2004). In these applications, the data collected by biosensors are transmitted to a server located at the hospital. The doctor can access the patient's records locally as well as remotely from these servers and thus can real-time monitor patient's health-conditions. In case of emergency, the doctor is notified by the system, as shown in Fig. 1.

Machine to Machine (M2M) communication is a new and emerging paradigm under telecommunication (Chen, Wan, & Li, 2012). In M2M, the devices communicate and share information with each other autonomously without or with limited human intervention (Yan et al., 2011). M2M communication is used in a wide range of applications such as: smart home, smart e-Health,

* Corresponding author.
E-mail addresses: ksaleem@ksu.edu.sa (K. Saleem), abderhab@ksu.edu.sa (A. Derhab), jalal@ccis.edu.sa (J. Al-Muhtadi), basit.shahzad@gmail.com (B. Shahzad).

http://dx.doi.org/10.1016/j.chb.2014.10.010
0747-5632/

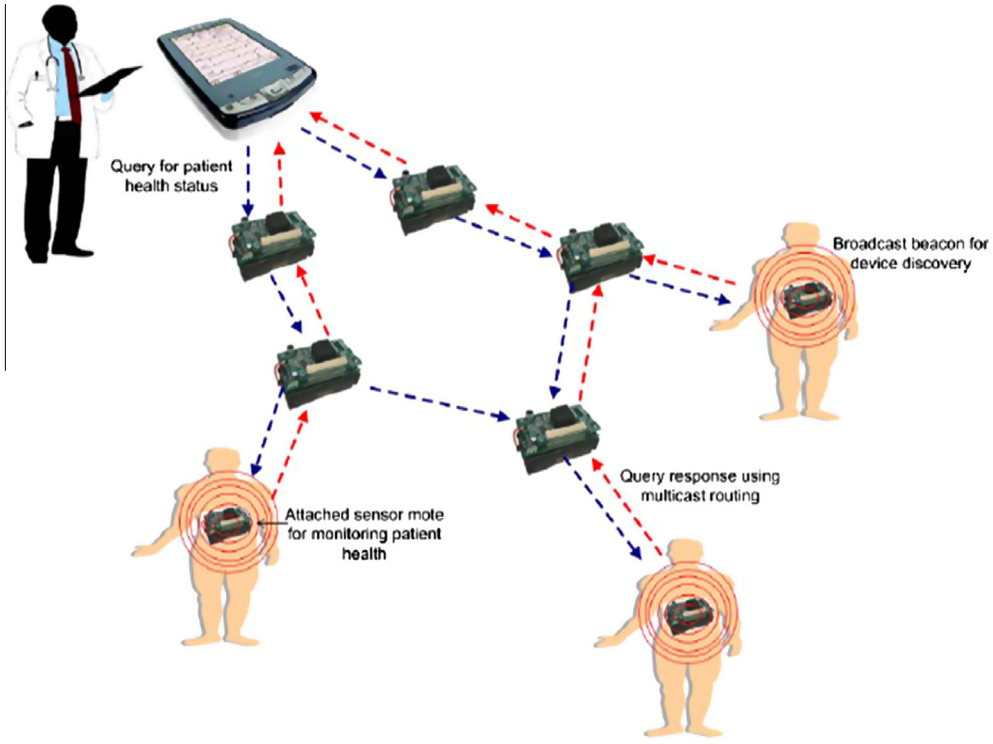

Fig. 1. Architecture of e-Healthcare system (Egbogah & Fapojuwo, 2011).

smart grid, and smart harvesting (Booysen, Gilmore, Zeadally, & Van Rooyen, 2012; Yan et al., 2011). In the literature, M2M communication has been proposed in many e-Healthcare systems (Jung, Ahn, Hwang, & Kim, 2012; Jung, Myllyla, & Chung, 2013; Min, Jiafu, Gonzalez, Xiaofei, & Leung, 2014; Park, Jung, Shin, Kim, & Yoon, 2014).

The above e-Healthcare systems can significantly benefit both the medical staff and the patients. Firstly, it can ensure continuous and real-time monitoring of patient's conditions and solve the problem of inability to constantly monitor a patient's health. Secondly, the patients can minimize the cost of hospitalization while being monitored at their homes as effectively as in hospitals. Thirdly, remote and real-time monitoring helps identifying the emergency conditions for patients in an easy and fast manner. Fourthly, it is possible to resolve the problem of unavailability of beds in hospitals by remotely monitoring some patients at their home instead.

All the above benefits offered by the e-Healthcare system focus on the efficiency aspect, which is reducing the work overload on the medical staff and getting early responses in case of emergency. However, the psychological issues, which come along with the illness, are not considered when designing e-Healthcare system. Physical illness is stressful experience and often puts emotional pressure, and burden on all the members of the healthcare society including the medical staff, patients and their families. It is known that physical symptoms often have an underlying psychological component. All illnesses have a psychological impact because illness is a threat to self. Depression loneliness and anxiety are common in illness, especially in chronic or life-threatening illnesses. The patients also need social support and share their feelings and concerns about the illness usually to strangers without the need to reveal their identities. On the other hand, medical staff are experiencing high level of stress caused by the heavy workload.

In this paper, we propose a M2M Low Cost and Secure (LCS) communication system, which considers the psychological issues of medical staff and patients when designing the healthcare system. A part of this work as a preliminary report has been presented previously in (Saleem, Derhab, & Al-Muhtadi, 2014). The main contributions of this paper are the following: Firstly, we define the different interactions in M2M e-Healthcare system, which can interact with each other in a secure manner. The security is ensured by involving intelligent authentication based on random distributive key management scheme, electronic certificate distribution, and modified realm Kerberos, while handling dynamic assignment of doctors to specific patient. Secondly, the M2M system is designed to maximize the automated tasks, which reduces the workload of medical staffs, and further reduces the associated stress. Thirdly, the system also provides access to online support groups and addresses the need for patients to share their health information with strangers while dealing with the privacy preservation issue. The Low Cost and Secure (LCS) Framework is implemented in Visual Basic .net 2013 to analyze the effectiveness of the complete system.

The rest of the paper is organized as follows: Section 2 gives an overview of Machine to Machine (M2M) communication and presents related work on secure M2M communication systems. In Section 3, we describe the Human-centered design of our proposed M2M communication system for e-Healthcare society. Section 4 describes the security design of the proposed system. In Section 5, the prototype implementation is described. Finally, Section 6 concludes the paper and outlines perspectives for further works.

2. Machine to Machine (M2M) communication

Machine to Machine (M2M) communication is a new and emerging paradigm under telecommunication (Chen et al., 2012). M2M communication is used in a wide range of applications such as: smart home, smart e-Health, smart grid, and smart harvesting (Booysen et al., 2012; Yan et al., 2011). The general architecture of M2M communication is shown in Fig. 2, and is composed of the following components: M2M device, M2M domain, and Internet domain. M2M device can be computers, sensors, actuators, embedded and mobile devices that communicate and share information with each other autonomously without or with limited

Please cite this article in press as: Saleem, K., et al. Human-oriented design of secure Machine-to-Machine communication system for e-Healthcare society. *Computers in Human Behavior* (2014), http://dx.doi.org/10.1016/j.chb.2014.10.010