Future Generation Computer Systems 55 (2016) 266–277

Contents lists available at ScienceDirect

Future Generation Computer Systems

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

Healing on the cloud: Secure cloud architecture for medical wireless sensor networks

Ahmed Lounis *, Abdelkrim Hadjidj, Abdelmadjid Bouabdallah, Yacine Challal

Université de Technologie de Compiègne, HEUDIASYC UMR CNRS 7253, BP 20529, Compiègne Cedex, France

HIGHLIGHTS

- We propose a new cloud-based architecture for medical wireless sensor networks.
- We ensure the security of medical data without patients/doctors interventions.
- We develop an access control that supports complex and dynamic security policies.
- We extend our access control to support emergency situations.
- Simulations show that our access control is efficient, fine-grained and scalable.

ARTICLE INFO

Article history:
Received 14 October 2013
Received in revised form
18 November 2014
Accepted 19 January 2015
Available online 4 February 2015

Keywords:
Wireless sensor networks
Healthcare
Cloud computing
Attribute based encryption
Emergency access control

ABSTRACT

There has been a host of research works on wireless sensor networks (WSN) for medical applications. However, the major shortcoming of these efforts is a lack of consideration of data management. Indeed, the huge amount of high sensitive data generated and collected by medical sensor networks introduces several challenges that existing architectures cannot solve. These challenges include scalability, availability and security. Furthermore, WSNs for medical applications provide useful and real information about patients' health state. This information should be available for healthcare providers to facilitate response and to improve the rescue process of a patient during emergency. Hence, emergency management is another challenge for medical wireless sensor networks. In this paper, we propose an innovative architecture for collecting and accessing large amount of data generated by medical sensor networks. Our architecture overcomes all the aforementioned challenges and makes easy information sharing between healthcare professionals in normal and emergency situations. Furthermore, we propose an effective and flexible security mechanism that guarantees confidentiality, integrity as well as fine-grained access control to outsourced medical data. This mechanism relies on Ciphertext Policy Attribute-based Encryption (CP-ABE) to achieve high flexibility and performance. Finally, we carry out extensive simulations that allow showing that our scheme provides an efficient, fine-grained and scalable access control in normal and emergency situations.

1. Introduction

Recent advances in medical sensors, wireless technologies and Micro-Electro-Mechanical systems have enabled the development of sensor nodes capable of sensing, processing and communicating several physiological signs. These lightweight miniaturized nodes collaborate to form a wireless sensor network (WSN) that simplifies the supervision of patients' health. The major breakthrough of this technology is providing continuous remote patient supervision both in and out of hospital conditions. Consequently, it reduces health cost and improves the quality of life of patients as well as the treatment efficiency.

There has been a host of research works on medical WSN for patient supervision [1–3]. Proposed solutions have adopted a common architecture with three main components as described in Fig. 1: Body Area Networks (BAN), gateways, and remote monitoring system. The BAN is a set of sensor nodes carried by the patient to collect different health information. Collected data is sent via wireless communication channel to the gateway which serves as a relay node to the monitoring system through a backbone network (ADSL, WiFi, or satellite). The remote monitoring system, usually

* Corresponding author. Tel.: +33 760518311.
E-mail addresses: lounisah@utc.fr (A. Lounis), ahadjidj@utc.fr (A. Hadjidj), bouabdal@utc.fr (A. Bouabdallah), ychallal@utc.fr (Y. Challal).

http://dx.doi.org/10.1016/j.future.2015.01.009
0167-739X/

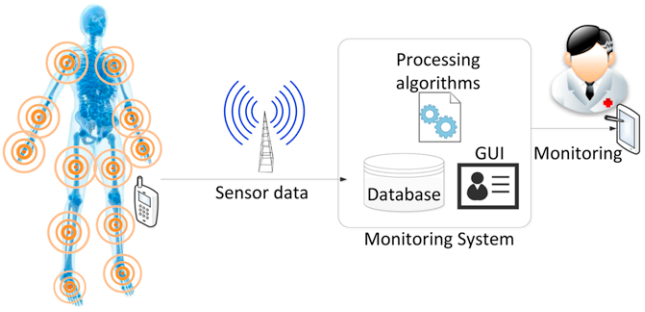

Fig. 1. Remote monitoring system architecture.

a server hosted by the healthcare provider, is the heart of the architecture at which the collected data is stored, processed and accessed.

Scalability is a challenge that WSNs for medical applications should tackle. Indeed, the sampling of medical sensors is performed at high frequency which increases the amount of collected data. In addition, the frequency of sensor sampling is often increased if the condition of patients being monitored gets worse. The data's size and heterogeneity demand more storage capacity and processing capability. Besides scalability issues, medical data could be life saving and must be accessible at any time and from everywhere. Existing solutions rely on a centralized paradigm to store and process sensed data, they cannot tackle the aforementioned challenges. We definitely need new innovative solutions to meet the great challenges of handling the exponential growth in data generated by sensors.

Considering social, ethical and legal aspects of medical systems [4,5], data collected by sensor networks is highly sensitive and should be managed properly to guarantee patients' privacy. Therefore, it is essential to ensure security of collected data during transmission as well as during storage. Access to patient information must be strictly limited to authorized users in order to guarantee the confidentiality. Since data is vital for medical diagnosis, data integrity should be verified to prevent wrong treatments because of malicious or erroneous modifications. Access to medical data is often governed by complex policies that distinguish between each part of data and each user privileges. Therefore, providing fine-grained access control that supports dynamic and complex organizational policies is a very hard challenge. Practical issues, such as security management, overhead and scalability of the access control with the number of users, also need to be considered. While a lot of research works have been carried out in medical wireless sensor networks, only few studies have been achieved regarding security and existing solutions are far from mature [6].

Emergency management is another challenge in medical applications. WSNs for medical applications is a means to detect and provide useful and real time information about patients' health state to the doctors and emergency staff. Moreover, WSNs facilitate response in case of emergency which can save patients' lives. In emergency intervention, medical information of victims is required by emergency staff who may not have enough privileges to access this information. Traditional solutions suggest disabling security system in emergency situations in order to allow emergency staff to access full victim's medical information for controlling emergency. Given the sensitivity of WSNs medical information, an access control solution that supports emergency access to some information without disabling security is then required.

In this paper, we address the challenge of data management in wireless sensor networks for patients supervision. We propose a secure and scalable architecture for collecting and accessing large amount of data generated by medical sensor networks. We leverage cloud computing technology to dynamically scale storage resources via on demand provisioning. Furthermore, we propose an innovative security scheme that eliminates potential security threats of medical data outsourcing and guarantees confidentiality, integrity as well as fine grained access control, while guaranteeing a secure emergency access.

Our contributions in this work are many folds:

1. We propose a new cloud based architecture for medical wireless sensor networks.
2. We show how we guarantee the confidentiality and the integrity of outsourced medical data without involving patients or doctors interventions.
3. We propose an efficient access control which allows implementing complex and dynamic security policies compliant with medical administrative organization while reducing the management and processing overhead.
4. We provide emergency management with two options: (A) In proactive manner, our solution relies on sensor networks to detect emergency. Thereafter, our system determines responders and give them temporal access. (B) Emergency reporting, where our system enables individual (the victim himself, emergency staff, etc.) to report emergency situations that WSNs cannot detect.
5. Finally, we carried out extensive simulations that allowed showing that our scheme provides an efficient, fine-grained and scalable access control in normal and emergency situations.

The rest of the paper is organized as follows. In Section 2, we review some related works. In Section 3, we present our proposed architecture. Then, in Section 4, we explain attribute-based encryption basics necessary to understand our proposed access control scheme, and we describe the security services ensured by our architecture in Section 5. In Section 6, we present our emergency management solution. After that, in Section 7, we analyze the security of our solution. Also, we provide simulation and performance evaluation results. Finally, in Section 8, we conclude the paper.

2. Related works

Scalability via on-demand resource provisioning and virtually infinite data storage capacity makes the cloud computing [7–9] compelling for managing data generated by WSNs. Cloud computing eases storage, processing and sharing of sensor data and provides anywhere/anytime access to supervision applications. Research works on coupling WSN and the cloud are still in their early infancy. A recent paper [10] tried to identify the opportunities and challenges of connecting wireless sensor networks to the Cloud. Also, few papers introduced cloud computing to different WSN applications such as industrial supervision [11], patient data collection [12,13], energy monitoring [14] and environmental monitoring [15]. However, all these papers described preliminary works and ignored the challenges induced by combining WSN and cloud computing. In [16], the authors proposed a new architecture of cloud-based Wireless Body Area Network (WBAN) with its underlying query processing algorithm for secure and powerful storage, energy-efficient and real-time data processing. This work combined cloud and WBAN (i.e. medical WSN) to address several challenges of WBAN but did not tackled the issues of confidentiality of sensitive data and access control on untrusted cloud.

Another approach to tackle the challenges of data management on WSNs, called the distributed database for sensor networks is studied in [17]. This approach focuses on how to manage the large amount of sensed data in an energy-efficient way.

Authors in [18] proposed a framework based on a publish/subscribe model which facilitates WSN-Cloud connection. In another paper [19], they used this framework to monitor human