Future Generation Computer Systems 64 (2016) 108–124

Contents lists available at ScienceDirect

Future Generation Computer Systems

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

End-to-end security scheme for mobility enabled healthcare Internet of Things

Sanaz Rahimi Moosavi[a,*], Tuan Nguyen Gia[a], Ethiopia Nigussie[a], Amir M. Rahmani[a], Seppo Virtanen[a], Hannu Tenhunen[a,b], Jouni Isoaho[a]

[a] Department of Information Technology, University of Turku, Turku, Finland

[b] Department of Industrial and Medical Electronics, KTH Royal Institute of Technology, Stockholm, Sweden

ARTICLE INFO

Article history:
Received 1 October 2015
Received in revised form
15 February 2016
Accepted 24 February 2016
Available online 3 March 2016

Keywords:
End-to-end security
Internet of Things
Smart healthcare
Mobility
Session resumption

ABSTRACT

We propose an end-to-end security scheme for mobility enabled healthcare Internet of Things (IoT). The proposed scheme consists of (i) a secure and efficient end-user authentication and authorization architecture based on the certificate based DTLS handshake, (ii) secure end-to-end communication based on session resumption, and (iii) robust mobility based on interconnected smart gateways. The smart gateways act as an intermediate processing layer (called fog layer) between IoT devices and sensors (device layer) and cloud services (cloud layer). In our scheme, the fog layer facilitates ubiquitous mobility without requiring any reconfiguration at the device layer. The scheme is demonstrated by simulation and a full hardware/software prototype. Based on our analysis, our scheme has the most extensive set of security features in comparison to related approaches found in literature. Energy-performance evaluation results show that compared to existing approaches, our scheme reduces the communication overhead by 26% and the communication latency between smart gateways and end users by 16%. In addition, our scheme is approximately 97% faster than certificate based and 10% faster than symmetric key based DTLS. Compared to our scheme, certificate based DTLS consumes about 2.2 times more RAM and 2.9 times more ROM resources. On the other hand, the RAM and ROM requirements of our scheme are almost as low as in symmetric key-based DTLS. Analysis of our implementation revealed that the handover latency caused by mobility is low and the handover process does not incur any processing or communication overhead on the sensors.

1. Introduction

Recent advances in information and communication technologies have given rise to a new technology: Internet of Things (IoT) [1–3]. IoT enables people and objects in the physical world as well as data and virtual environments to interact with each other, hence realizing smart environments such as smart transport systems, smart cities, smart healthcare, and smart energy. The rising cost of healthcare, and the prevalence of chronic diseases around the world urgently demand the transformation of healthcare from a hospital-centered system to a person-centered environment, with a focus on citizens' disease management as well as their wellbeing [4]. It has been predicted that in the following decades, the way healthcare is currently provided will be transformed from hospital-centered, first to hospital-home-balanced in the 2020's, and then ultimately to home-centered in 2030's [5]. This essential transformation necessitates the fact that the convergence and overlap of the IoT architectures and technologies for smart spaces and healthcare domains should be more actively considered [4,6–8].

Security is a major concern wherever networks are deployed at large scales. IoT-based healthcare systems deal with human-related data. Although collected from innocuous wearable sensors, such data is vulnerable to top privacy concerns [9–12]. In IoT-based healthcare applications, security and privacy are among major areas of concern as most devices and their communications are wireless in nature [13]. An IP-enabled sensor in a Medical Sensor Network (MSN), for instance, can transmit medical data of patients to a remote healthcare service. However, in such scenarios, the conveyed medical data may be routed through an untrusted network infrastructure, e.g. the Internet. Hence, in healthcare IoT, security and privacy of patients are among major areas of concern. In this regard, the authentication and authorization of remote healthcare centers/caregivers and end-to-end data protection are

[*] Corresponding author.
E-mail address: saramo@utu.fi (S.R. Moosavi).

http://dx.doi.org/10.1016/j.future.2016.02.020
0167-739X/© 2016 Elsevier B.V. All rights reserved.

critical requirements as eavesdropping on sensitive medical data or malicious triggering of specific tasks can be prevented [14]. Due to direct involvement of humans in IoT-based healthcare applications, providing robust and secure data communication among healthcare sensors, actuators, patients, and caregivers are crucial. Misuse or privacy concerns may restrict people to utilize IoT-based healthcare applications.

Conventional security and protection mechanisms including existing cryptographic solutions, secure protocols, and privacy assurance cannot be re-used due to resource constrains, security level requirements, and system architecture of IoT-based healthcare systems [15]. To mitigate the aforementioned risks, strong network security infrastructures for a short and long-range communication are needed. There are significant security solutions to current wireless networks which are not directly applicable to IoT-based healthcare applications due to the following challenges [16]: (i) security solutions must be resource-efficient as medical sensors have limited processing power, memory, and communication bandwidth. (ii) Medical sensors can be easily lost or abducted as they are tiny in terms of size.

To deal with the mentioned challenges, Constrained Application Protocol (CoAP) [17] proposes Datagram Transport Layer Security (DTLS) [18] to be used for resource-constrained services/applications. DTLS is a complete security protocol as it offers authentication, key exchange, and protection of application data. An IoT-enabled application may be in one of the following four security modes: (i) *NoSec*, meaning that the DTLS is disabled and there is no protocol level security. However, the use of *IPsec* as network layer security is recommended. (ii) *Symmetric Key-based DTLS*, meaning that DTLS is enabled and symmetric key-based authentication is utilized. (iii) *Public Key-based DTLS*, meaning that DTLS is enabled and the resource constrained device has an asymmetric key pair. The public key is not embedded in an X.509 certificate. (iv) *Certificate-based DTLS*, meaning that DTLS is enabled and the constrained device has an asymmetric key pair. The X.509 certificate is signed by a Certificate Authority (CA). Medical sensors used in healthcare IoT have limited ROM, RAM, CPU and energy resources. Thus, new challenges arise when using certificates on such resource-constrained devices.

In [19], as shown in Fig. 1, we presented a secure and efficient authentication and authorization architecture for IoT-based healthcare systems using smart e-health gateways in a distributed fashion. More precisely, we proposed to exploit the smart gateways' advantageous property of being non-resource constrained for outsourcing the processing burden of end-user authentication and authorization from tiny medical sensors. The system architecture of our proposed IoT-enabled healthcare system includes the following main components: (i) *Device Layer*: enabled with ubiquitous identification, sensing, and communication capacity, in which bio-medical and context signals are captured from home/hospital room(s) or patients' body to be used for treatment and diagnosis of medical states. (ii) *Fog Layer*: consists of a network of distributed smart e-health gateways where those gateways support various communication protocols and acts as a touching point between the device layer and cloud layer. (iii) *Cloud Layer*: this layer is composed of the remote healthcare server and patients' classified health data. (iv) *Web Interface*: as a graphical user interface to be used by remote caregivers for final visualization and apprehension.

Recently, there have been efforts in designing *Smart e-Health Gateways* for Healthcare Internet of Things (Health-IoT) systems [4]. In a smart home/hospital, where the mobility and location of patients are confined to hospital facilities or buildings, gateways can play a key role. The stationary nature of such gateways enables them with the exclusivity of being non-resource constrained in terms of power consumption, memory, and communication bandwidth. By providing the necessary security context to the medical sensors, smart gateways remove the need to authenticate and authorize remote healthcare centers/caregivers from the sensors. Therefore, any malicious activity can be blocked before entering to a medical constrained domain. For this purpose, we employed the certificate-based DTLS handshake as it is the main transport layer security solution for IoT.

In healthcare IoT systems, improving patients' quality of life is important to mitigate the negative effects of being hospitalized. Providing patients with the possibility to walk around the medical environments knowing that the monitoring of their health condition is not interrupted is an important feature. Enabling mobility support for patient monitoring systems offers a high quality of medical service as it allows patients to move around freely within the premises. Patients do not need to be worried about moving around as the system can enable mobility while monitoring their vital signs continuously.

In our previous work [19], the main focus was on the analysis and development of authentication and authorization between peers rather than end-to-end security. In [20], we proposed a session resumption-based end-to-end security scheme for healthcare IoT systems to securely and efficiently manage the communication between medical sensors and remote healthcare centers/caregivers. The proposed scheme relied on the certificate-based DTLS handshake between non-resource-constrained distributed smart gateways and end-users at the start of the communication (initialization phase). To provide end-to-end security, the session resumption technique without server-side state is utilized. The session resumption technique has an abbreviated form of the DTLS handshake and it neither requires heavy-weight certificate-related nor public-key operations as it relies on the previously established DTLS connection.

In this article, an end-to-end security scheme for mobility enabled healthcare IoT is proposed. The main contributions of this article, which is a major extension of our recent works published in [19,20], are twofold. First, we propose an end-to-end security scheme for healthcare IoT with the explicit consideration of mobility for medical sensors. We exploit the concept of fog layer in IoT for realizing efficient and seamless mobility since fog extends the cloud paradigm to the edge of the network. Second, we analyze the characteristics of the proposed scheme in terms of security and energy-performance on a prototype of a healthcare IoT system through simulation and hardware/software prototype.

The remainder of the article is organized as follows: in Section 2, the related work and motivation are discussed. Section 3 presents our proposed system architecture for healthcare IoT. In Section 4, the requirements of secure and efficient communication for healthcare IoT system are presented and discussed. Section 5 presents the proposed end-to-end security scheme for healthcare IoT systems. Fog layer-based mobility for our proposed end-to-end security scheme is presented in Section 6. Experimental results including energy-performance and security evaluations are provided and discussed in Section 7. Finally, Section 8 concludes the article.

2. Related work and motivation

For the discussion of related work, we recognize three main research directions: (i) IoT-based Healthcare Security, (ii) Smart Gateways, and (iii) Mobility solutions for IoT systems.

2.1. IoT-based healthcare security

CodeBlue is one of the most popular healthcare research projects that has been developed at the Harvard sensor network Lab [21]. In this approach, several medical sensors are placed on a patients' body. CodeBlue has been expected to be deployed in in-hospital emergency care, stroke patient rehabilitation and