Future Generation Computer Systems 82 (2018) 422–439

Contents lists available at ScienceDirect

Future Generation Computer Systems

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

An Internet of Things-based health prescription assistant and its security system design

Mahmud Hossain [a], S.M. Riazul Islam [b,*], Farman Ali [c], Kyung-Sup Kwak [c], Ragib Hasan [a]

[a] SECuRE and Trustworthy computing Lab, Department of Computer Science, University of Alabama at Birmingham, AL, USA
[b] Department of Computer Science and Engineering, Sejong University, South Korea
[c] School of Information and Communication Engineering, Inha University, South Korea

HIGHLIGHTS

- A theoretical framework for an IoT-based health prescription assistant is proposed.
- A security system that ensures user authentication and protected access is designed.
- The details of security components, authorization model, and operational model are given.
- A prototype of the proposed security system has been implemented.
- Experimental results that validates the efficiency of the proposed system are provided.

ARTICLE INFO

Article history:
Received 29 June 2017
Received in revised form 30 October 2017
Accepted 12 November 2017
Available online 2 December 2017

Keywords:
Internet of things
Healthcare
Health assistant
Telemedicine
Security system

ABSTRACT

Today, telemedicine has a great reputation because of its capacity to provide quality healthcare services to remote locations. To achieve its purposes, telemedicine utilizes a number of wireless technologies as well as the Internet of Things (IoT). The IoT is redefining the capacity of telemedicine in terms of improved and seamless healthcare services. In this regard, this paper contributes to the set of features of telemedicine by proposing a model for an IoT-based health prescription assistant (HPA), which helps each patient to follow the doctors recommendations properly. This paper also designs a security system that ensures user authentication and protected access to resources and services. The security system authenticates a user based on the OpenID standard. An access control mechanism is implemented to prevent unauthorized access to medical devices. Once the authentication is successful, the user is issued an authorization ticket, which this paper calls a security access token (SAT). The SAT contains a set of privileges that grants the user access to medical IoT devices and their services and/or resources. The SAT is cryptographically protected to guard against forgery. A medical IoT device verifies the SAT prior to serving a request, and thus, ensures protected access. A prototype of the proposed system has been implemented to experimentally analyze and compare the resource efficiency of different SAT verification approaches in terms of a number of performance metrics, including computation and communication overhead.

1. Introduction

In the past decade, the Internet of things (IoT) has become a megatrend in next-generation technologies by offering advanced connectivity to each uniquely identifiable smart device or thing [1]. An IoT-based system provides an intelligent framework with sensing capability, contextual awareness, and device autonomy. IoT devices embedded with sensors and actuators perceive their surroundings, intelligent enough to understand the collected data, and perform accordingly. The sensed data can be processed by a smart device itself or in a cloud. An IoT device can take decision autonomously based on the sensed data or communicate to us.

Every day, hundreds of such physical things are getting connected to the Internet to share local information to cyberspace [2]. A recent research anticipates, every year, on an average, around one million new IoT devices will be deployed to different application domains [3]. In this regard, the IoT has gained a fair share of attention from researchers, developers, and industries, and thus, many different service applications have been proposed and developed. These proposed IoT-based applications can be categorized in many different ways (for example, applications for smart cities, for security, emergency services, and healthcare systems, etc.). Islam

* Corresponding author.
E-mail addresses: mahmud@uab.edu (M. Hossain), riaz@sejong.ac.kr (S.M.R. Islam), farmankanju@gmail.com (F. Ali), kskwak@inha.ac.kr (K. Kwak), ragib@uab.edu (R. Hasan).

https://doi.org/10.1016/j.future.2017.11.020
0167-739X/

et al. [4] introduced various IoT-based application scenarios, where mobile notifications are displayed on a TV screen, different colors of room lighting are applied for emergency recognition, and a health prescription assistant (HPA) is provided. For more profound understanding of the IoT and its application domains, interested readers are referred elsewhere [5–7].

Eventually, the IoT can be thought of as a growing network of physical objects or entities that feature an IP address for Internet connectivity, and the correspondence that happens between pairs of such objects and other Internet-enabled gadgets and frameworks. Introducing automation is feasible in nearly every field, since the IoT comes with a set of benefits, including advanced connectivity that goes beyond machine-to-machine scenarios [8]. One of the main criteria of the IoT is enabling services provided by any network on the World Wide Web to its intended end users and/or things [4]. This feature of the IoT allows the offering of timely, high-quality telemedicine and healthcare services to patients via remote assistance. For example, in the concept of telemedicine, a medical practitioner provides his/her patient with medical services from a distance. The patient might be located in a remote place (the countryside, a ship on the ocean, or even in an aircraft). There are many places on this planet, particularly in developing countries, where access to healthcare services is restricted by distance and a poor transportation infrastructure. However, in some places, healthcare services are inadequate. In such places, the opportunities and possibilities of distributing medical services by telemedicine can be accelerated by mobilizing the potential of the IoT [1].

Consequently, the IoT could give rise to numerous medical applications, including remote health monitoring. For example, based on the patients health data, a healthcare service provider can make a much better diagnosis of the patients condition and can recommend the best possible treatment and early intervention [9]. Consistency in home treatment and medication by the healthcare service provider is another potentially critical application. Hence, different healthcare devices, sensors, and diagnostic and imaging gadgets can be seen as smart objects constituting a pivotal part of the IoT. Thus, the technology of wearable sensors has accelerated the development of new applications and services used in remote healthcare systems, such as controlling patients health conditions, through content service applications and by providing treatment according to the updates [10]. Consequently, IoT-based medical services are expected to decrease costs, to build personal satisfaction, and to improve the client's experience. From the medical service providers point of view, the IoT could diminish device downtime through remote procurement. Integration of the IoT into the aforementioned healthcare systems enables a further increase in intelligence and interoperability [11], which will result in expansion of the IoT at an exponential rate.

In a nutshell, IoT-based healthcare [12] is a promising technology that brings many advantageous applications to reduce costs, increase quality of life, and improve the efficiency of healthcare services, providing easy and correct action, on time.

However, in the healthcare system, devices and applications are expected to deal with important private information, including personal healthcare data. Furthermore, such smart devices will be connected to worldwide information networks for access anytime and anywhere. Subsequently, the IoT healthcare domain may become a target. The personal data collected from resource-constrained wearable sensors are thus vulnerable to privacy concerns [13,14]. Additionally, unauthorized access to the medical devices can jeopardize patients lives [15–20]. Therefore, misuse of healthcare sensors and actuators or privacy concerns with patients medical records may restrict people to utilize IoT-based healthcare applications. In this regard, this paper proposes a model for an IoT-based HPA and designs of a security system to protect unauthorized access to the proposed framework.

Contributions. The contributions of this paper are as follows:

1. We propose a theoretical framework for an IoT-based HPA and present a detailed architectural model for the HPA.
2. We highlight the operation and benefits of the HPA.
3. We design a security system that ensures user authentication and protected access to electronic medical records and medical sensors and actuators.
4. We provide the details of security components, authorization model, operational model, and security access token (SAT) verification.
5. We implement a prototype of the proposed system using IoT devices powered by Contiki operating system.
6. We provide the performance evaluations in terms of various metrics, including communication and computation latency, request completion time, and energy consumption.

Organization. The rest of this paper is organized as follows. Related work and motivation are presented in Section 2. A background on access-control schemes in IoT is provided in Section 3. In Section 4, the proposed HPA is presented. Section 5 provides the proposed security system. The experiment and evaluations are presented in Section 6. A comparative discussion on proposed and existing authorization schemes is presented in Section 7. Finally, we conclude this article in Section 8.

2. Related work and motivation

The advances in cloud and ubiquitous computing, smart sensors and actuators, and IoT Big data and analytics have made remote monitoring of patients more feasible. Recently, several research works on wireless healthcare have been proposed, which aimed at continuous patient monitoring in closed environments, such as home, office, ambulance, and hospital, as well as in open environments such as athlete health monitoring.

2.1. Insecure IoT-based healthcare

An implementation of autonomous wireless body area network for enabling IoT connected healthcare applications was proposed in [21]. The authors in [22] provided a Cloud-IoT based sensing service for health monitoring. The research work [23] presented an intelligent healthcare framework based on IoT technology to provide ubiquitous healthcare to person during his/her workout sessions. To provide an efficient diagnosis, Lomotey et al. [24] proposed a data acquisition architecture for wearable devices. Ali et al. [25] proposed a healthcare system that analyzes physiological information of patients and suggests diabetes-specific prescription. We-care [26] proposed an IoT-based healthcare system for elderly people. iDoctor [27] provided a personalized and professionalized medical recommendations based on hybrid matrix factorization. A facial recognition system that enables doctors and caregivers to constantly monitor patients' feelings remotely and take appropriate action as required was presented in [28]. The article [29] provided an energy-aware cyber–physical therapy system, which incorporates smart things and devices in both the physical and cyber world for therapy sensing. The authors in [30] proposed a smart health care framework for monitoring Parkinson's disease in smart cities. Sood et al. [31] designed an IoT and fog based healthcare system to provide a remote diagnosis of Chikungunya virus based on a user's health symptoms and surrounding environmental conditions. A healthcare monitoring system using radio-frequency identification (RFID) was proposed in [32]. The authors in [33] designed an IoT-aware architecture for smart healthcare coaching systems. An information acquisition model to enable