Service Intelligence and Communication Security for Ambient Assisted Living

Dmitry G. Korzun, Petrozavodsk State University, Petrozavodsk, Russia
Ilya Nikolaevskiy, Aalto University, Espoo, Finland
Andrei Gurtov, Linköping University, Linköping, Sweden & ITMO University, Saint Petersburg, Russia

ABSTRACT

Mobile health (m-Health) scenarios and Internet of Things (IoT) technologies form an important direction for enhancing medical systems for Ambient Assisted Living (AAL). Yet current development meets with two challenges: 1) use of patient’s health data with strong security guarantees in mobile network and resource-constrained assumptions and in emergency situations, 2) inclusion of personal data to the entire system for “smart” service construction and delivery. This paper presents a smart space based architectural model that adopts emerging IoT technologies to enable security of personal mobile data and their intelligent utilization in health services. To support the service intelligence, the authors employ the smart spaces approach with its prominent technologies adopted from IoT and Semantic Web. The intelligence and security solutions are considered symbiotic to present better user-experience, security level, and utility of a system.

Keywords: Ambient Assisted Living, Information Security, Medical Sensor Network, Mobile Health, Personalization, Service Intelligence, Smart Spaces

1. INTRODUCTION

The recent advances in bioengineering and the proliferation of wireless sensor platforms have allowed the realization of pervasive and mobile health (m-Health) systems for ambient assisted living (AAL) (Alemdar and Ersoy, 2010, Mukhopadhyay, 2015, Acampora et al., 2013a, Kumar and Lee, 2012). Sensors, wearable by a patient or implantable within the body, form a medical sensor network (MSN) accessible to medical personnel and the patient herself. The mobile terminal centric view states that end-user device (such as smartphone) becomes a personalized access point and service hub from the patient’s MSN to enhanced healthcare system.

Being dynamic, rich of multi-source data and dependent on surrounding environment, health services must be made smart (Demirkan, 2013). It requires a possibility to understand the

DOI: 10.4018/IJERTCS.2015010104
recent situation and latest sensed data, and then to react in a best-effort manner. This intelligence challenge becomes crucial in emerging solutions for health IT. Intelligent access to patient data offers many opportunities to enhance the delivery of services, improve the patient experience, and advance integrated health (Mandl et al., 2012, Yang et al., 2013, Acampora et al., 2013a).

Since a mobile patient typically uses public networks, data collecting and transferring must be secured (Kumar and Lee, 2012). In fact, preserving privacy and integrity of medical data is a crucial legal requirement imposed, for instance by the Health Insurance Portability and Accountability Act. This security challenge becomes complex due to the dynamicity and heterogeneity of networked digital environments. Many medical devices available on the market are still vulnerable, see examples of successful attacks in (Radcliffe, 2011, Halperin et al., 2008). Medical personnel may act as an MSN user in addition to or on behalf of the patient.

This paper considers these two challenges of healthcare and AAL system design to be symbiotic. Our approach is based on technologies of Internet of Things (IoT) and Semantic Web. We systematize recent results on service intelligence (Korzun et al., 2015c, Korzun et al., 2015a) and communication security (Gurtov et al., 2012, Nikolaevskiy et al., 2014) in smart spaces applications for healthcare. We present an architectural model for healthcare systems where selected technologies are integrated to support intelligence and security in attached personalized MSN-based m-Health systems. The model is specifically focused on the following objectives, reflecting the demands of enhanced healthcare and AAL systems (Demirkan, 2013, Alemdar and Ersoy, 2010, Mingyu et al., 2012, Mukhopadhyay, 2015):

- **Dependability**: Patient’s MSN is mobile and available regardless of location. In particular, accessibility and its security aspects are preserved in case of emergency and other abnormal situations;
- **Semantics**: Support for making intelligent decisions as reaction to recognized meaning of available multi-source data. In particular, services become adaptive to suit best the observed situation and context, provide personalization of operation with users, and allow proactive activation and delivery;
- **Capacity**: The system requires as little as possible overhead for resource-constrained devices. In particular, complex processing is delegated to powerful components of the system (e.g., servers or even clouds), leaving small devices the role of data providers and service consumers.

Our solutions for service intelligence provide smart space based support for service adaptation, personalization, and proactive delivery. Dynamic relation of multi-source data forms a smart space (Korzun et al., 2013, Vergari et al., 2011). It supports semantics-based analysis of collected data and derived knowledge directly in this space. The smart space allows feeding health services with non-medical data. Enhanced health applications are enabled, which are not based purely on electronic health records (Mandl et al., 2012, Hovenga et al., 2010, Nee et al., 2008). Our approach is based on principles developed in the open research pilot for smart spaces—Smart-M3 platform (Honkola et al., 2010). The platform is oriented to a wide class of IoT-aware multi-domain applications.

Our solutions for communication security provide confidentiality of data transmission over insecure network, access control, fallback mechanism, revocation procedure, and certificate-based user authorization including temporary role delegation and authenticity of communications of patients with healthcare services and medical personnel. We have implemented a prototype system to show feasibility of the proposed security mechanisms on constrained devices. The security approach is based on a standardized protocol for Internet—Host Identity Protocol, HIP.

---

Copyright © 2015, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.
Related Content

Fractal Geometry and Computer Science
Nicoletta Sala (2009). *Selected Readings on Telecommunications and Networking* (pp. 385-404).
[www.igi-global.com/chapter/fractal-geometry-computer-science/28736?camid=4v1a](www.igi-global.com/chapter/fractal-geometry-computer-science/28736?camid=4v1a)

A Secure Home Healthcare System Based on 6LoWPAN WSN
[www.igi-global.com/article/a-secure-home-healthcare-system-based-on-6lowpan-wsn/124793?camid=4v1a](www.igi-global.com/article/a-secure-home-healthcare-system-based-on-6lowpan-wsn/124793?camid=4v1a)
A Complete Spectrum Sensing and Sharing Model for Cognitive Radio Ad Hoc Wireless Networks Using Markov Chain State Machine
www.igi-global.com/chapter/complete-spectrum-sensing-sharing-model/72425?camid=4v1a

High-Speed Cable Replacement for Multimedia Streaming in Wireless Personal and Local Area Networks
www.igi-global.com/chapter/high-speed-cable-replacement-multimedia/58698?camid=4v1a