Chapter 35
Wireless Body Sensor Networks: Security, Privacy, and Energy Efficiency in the Era of Cloud Computing

Wassim Itani
Beirut Arab University, Lebanon

Ayman Kayssi
American University of Beirut, Lebanon

Ali Chehab
American University of Beirut, Lebanon

ABSTRACT

In this paper, the authors provide a detailed overview and technical discussion and analysis of the latest research trends in securing body sensor networks. The core of this work aims at: (1) identifying the resource limitations and energy challenges of this category of wireless sensor networks, (2) considering the life-critical applications and emergency contexts that are encompassed by body sensor network services, and (3) studying the effect of these peculiarities on the design and implementation of rigorous and efficient security algorithms and protocols. The survey discusses the main advancements in the design of body sensor network cryptographic services (key generation and management, authentication, confidentiality, integrity, and privacy) and sheds the light on the prominent developments achieved in the field of securing body sensor network data in Cloud computing architectures. The elastic virtualization mechanisms employed in the Cloud, as well as the lucrative computing and storage resources available, makes the integration of body sensor network applications, and Cloud platforms a natural choice that is packed with various security and privacy challenges. The work presented in this paper focuses on Cloud privacy and integrity mechanisms that rely on tamper-proof hardware and energy-efficient cryptographic data structures that are proving to be well-suited for operation in untrusted Cloud environments. This paper also examines two crucial design patterns that lie at the crux of any successful body sensor network deployment which are represented in: (1) attaining the right balance between the degree, complexity, span, and strength of the cryptographic operations employed and the energy resources they

DOI: 10.4018/978-1-5225-8897-9.ch035

Copyright © 2019, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.

consume. (2) Achieving a feasible tradeoff between the privacy of the human subject wearing the body sensor network and the safety of this subject. This is done by a careful analysis of the medical status of the subject and other context-related information to control the degree of disclosure of sensitive medical data. The paper concludes by presenting a practical overview of the cryptographic support in the main body sensor network development frameworks such and TinyOS and SPINE and introduces a set of generalized guideline patterns and recommendations for designing and implementing cryptographic protocols in body sensor network environments.

INTRODUCTION

The field of implantable medical devices (IMDs) has witnessed a rapid proliferation and increased success in the past decade. Leveraging the technological advancements in the fields of embedded computing, processor design, and wireless radio communications, these devices are now capable of performing vital monitoring and control activities inside the human body. Most of today's sophisticated human implantable devices, such as drug delivery systems, neurological stimulators, cardiac defibrillators, and pacemakers, are equipped with dedicated computing power resources and supported with wireless radio transmission capabilities. Such advanced computing and network communication capabilities allow these devices to deliver critical telemetric remote monitoring services in real time over the Internet. Moreover, the enormous adoption of the Cloud computing model for delivering virtualized services over the Internet has provided IMDs with lucrative processing and storage facilities that suit their data-intensive nature and analysis requirements. A recent Transparency Market Research report (Transparency Market Research, 2013) states that the IMD market in the U.S. reached a $ 25.2 billion in 2012 and were predicted to reach $ 33.6 billion by 2018. According to the same report, the IMD market is anticipated to expand at a CAGR of nearly 4% from 2012 to 2018.

This noticeable success in the field of IMDs and the major advancements in wireless sensor network algorithms and applications have stimulated the emergence of specialized biological networks termed as Body Sensor Networks (BSNs) or Body Area Networks (BANs). BSNs are specialized wireless sensor networks whose nodes are deployed on the human body either in the form of attached/embedded electrode-like patches or wearable as part of the human clothing. In both cases, BSNs consist of a collection of sensor nodes situated at strategic locations in the human body and capable of extracting and wirelessly communicating vital body signals and other context-specific environmental measurements to centralized servers in the Cloud. The centralized storage and processing resources in the Cloud provide hospitals and health care units with a reliable and timely interface to access and analyze the BSN data. Some of the vital body signals that can be monitored by a BSN are Systolic and Diastolic blood pressure, heart rate, ElectroCardioGram (ECG), ElectroMyoGram (EMG), ElectoEncephaloGram (EEG) records, breathing rate, Galvanic Skin Response(GSR), temperature, proximity, etc.

A typical BSN is presented in Figure 1. The body sensor nodes extract a predefined set of physiological body signals and wirelessly transmit the measured values in a hop-by-hop fashion to a BSN controller (usually a smart phone) attached to the human body. The BSN controller relays the collected signal values to a nearby Internet base station or router which in turn delivers the BSN physiological data to a Cloud computing infrastructure for storage and analysis. Employing BSNs in a health care environment together with the centralized storage and processing facilities provided by Cloud computing, will certainly enhance the quality of the health care service provided by supporting the ubiquitous and

31 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage:
www.igi-global.com/chapter/wireless-body-sensor-networks/228753

Related Content

Cloud Computing and Cybersecurity Issues Facing Local Enterprises
Emre Erturk (2019). *Cyber Law, Privacy, and Security: Concepts, Methodologies, Tools, and Applications (pp. 1777-1799).*
www.irma-international.org/chapter/cloud-computing-and-cybersecurity-issues-facing-local-enterprises/228809

Data Protection and BI: A Quality Perspective
Daragh O. Brien (2019). *Cyber Law, Privacy, and Security: Concepts, Methodologies, Tools, and Applications (pp. 1603-1628).*
www.irma-international.org/chapter/data-protection-and-bi/228799

The Future of National and International Security on the Internet
Maurice Dawson, Marwan Omar, Jonathan Abramsonand Dustin Bessette (2019). *Cyber Law, Privacy, and Security: Concepts, Methodologies, Tools, and Applications (pp. 1666-1696).*
www.irma-international.org/chapter/the-future-of-national-and-international-security-on-the-internet/228803

Learner-Developed Case Studies on Ethics: Collaborative Reflection Between School Librarians and Education Technology Learners
Lesley S. J. Farmer (2019). *Emerging Trends in Cyber Ethics and Education (pp. 131-163).*
www.irma-international.org/chapter/learner-developed-case-studies-on-ethics/207665

A Proposal for a General Resolution on Cyborgization
(2022). *Philosophical Issues of Human Cyborgization and the Necessity of Prolegomena on Cyborg Ethics (pp. 307-314).*
www.irma-international.org/chapter/a-proposal-for-a-general-resolution-on-cyborgization/291955