Smart Health 3–4 (2017) 39–74

Contents lists available at ScienceDirect

Smart Health

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

A policy enforcement framework for Internet of Things applications in the smart health

S. Sicari[a], A. Rizzardi[a], L.A. Grieco[b,*], G. Piro[b], A. Coen-Porisini[a]

[a] *"DISTA, Dep. of Theoretical and Applied Science", Universita' degli Studi dell'Insubria, v. Mazzini 5, 21100 Varese, Italy*
[b] *"DEI, Dep. of Electrical and Information Engineering", Politecnico di Bari, v. Orabona 4, 70125 Bari, Italy*

ARTICLE INFO

Keywords:
Internet of Things
Smart health
Security
Policy enforcement

ABSTRACT

Internet of Things (IoT) is characterized by heterogeneous technologies, which concur to the provisioning of innovative services in different application domains. Introducing efficient mechanisms for collecting, processing, and delivering data generated by sensors, medical equipment, wearable devices, and humans, is a key enabling factor for advanced healthcare services. The adoption of IoT in smart health, however, opens the doors to some security concerns. In fact, by considering the confidentiality and sensitivity of medical data, a healthcare system must fulfill advanced access control procedures with strict security and data quality requirements. To this end, a flexible policy enforcement framework, based on the IoT paradigm, is defined hereby. It is able to face security and quality threats in dynamic large scale and heterogeneous smart hearth environments. As a key feature of the proposed framework, cross-domain policies have been defined using a specification language based on XML. In this way, it becomes possible to ease the management of interactions across different realms and policy conflicts. Moreover, to demonstrate the usefulness of the proposed approach, a running example, based on a smart health application, is detailed throughout the manuscript. This helps to highlight the different facets of the conceived enforcement framework. A preliminary performance analysis also demonstrates its feasibility in large scale environments.

1. Introduction

During the last decade, Internet of Things (IoT) approached our lives, thanks to the availability of wireless communication systems (e.g., RFID, WiFi, 4G, IEEE 802.15.x), which have been increasingly employed as central technology for smart monitoring and control applications (Atzori, Iera, & Morabito, 2010; Miorandi, Sicari, De Pellegrini, & Chlamtac, 2012; Palattella et al., 2013). Nowadays, the concept of IoT is many-folded. Since it embraces many different technologies, services, and standards, it is widely perceived as the corner stone of the ICT market in the next ten years (Emmerson, 2010; Boswarthick, Elloumi, & Hersent 2012; Hersent, Boswarthick, & Elloumi, 2012). From a logical point of view, an IoT system can be depicted as a collection of smart devices that interact on a collaborative basis to fulfill a common goal. Whereas, from a technological point of view, IoT deployments may adopt different processing and communication architectures, technologies, and design methodologies, based on their target.

With reference to the smart health context, IoT can be successfully used in monitoring services and biomedical systems including patient monitoring, telemedicine, pervasive healthcare management, detection of clinical issues, management of logistics and maintenance services, and so on (Catarinucci et al., 2015; Laplante and Laplante, 2016; Xu et al., 2014; YIN, Zeng, Chen, & Fan,

[*] Corresponding author.
E-mail addresses: sabrina.sicari@uninsubria.it (S. Sicari), a.rizzardi@uninsubria.it (A. Rizzardi), a.grieco@poliba.it (L.A. Grieco), giuseppe.piro@poliba.it (G. Piro), alberto.coenporisini@uninsubria.it (A. Coen-Porisini).

http://dx.doi.org/10.1016/j.smhl.2017.06.001
Received 19 December 2016; Received in revised form 9 May 2017; Accepted 7 June 2017
Available online 15 June 2017

2016). In such smart health environments, data sources, communication technologies, services' and users' requirements are inherently heterogeneous (YIN et al., 2016; Ullah, Shah, & Zhang, 2016). The high level of heterogeneity can be leveraged by multiple security attacks. But traditional security countermeasures and privacy solutions cannot be directly applied to IoT technologies for various reasons: their computational, memory, communication, and energy consumption requirements could not be supported by constrained devices (Altolini, Lakkundi, Bui, Tapparello, & Rossi, 2013). Moreover, adaptation and self-healing play a key role in IoT infrastructures (including those related to smart health scenarios), which must be able to face normal and unexpected changes of the target environment. Accordingly, privacy and security issues should be treated with a high degree of flexibility (Bandyopadhyay, Sengupta, Maiti, & Dutta, 2011; Chaqfeh & Mohamed, 2012; Ashraf & Habaebi, 2015). Together with conventional security solutions, there is also the need to provide built-in security in the devices themselves (i.e., embedded) in order to pursue dynamic prevention, detection, diagnosis, isolation and countermeasures against successful breaches (Babar, Stango, Prasad, Sen, & Prasad, 2011).

As a consequence, as a first step towards the development of a comprehensive IoT-based architecture, it is mandatory to define valid security and privacy frameworks suitable for IoT applications (Miorandi et al., 2012; Weber, 2010; Roman, Zhou, & Lopez, 2013; Yan, Zhang, & Vasilakos, 2014; Premarathne et al., 2016; Khan & Sakamura, 2015; Barua, Liang, Lu, & Shen, 2011; Pussewalage & Oleshchuk, 2016). They should address: (i) the guarantee of confidentiality and integrity of data; (ii) the provision of authentication and authorization mechanisms in order to prevent unauthorized users (i.e., a nurser cannot access to sensitive data available for doctors only) from accessing the system; (iii) the assurance of anonymity of users personal information, since devices may manage sensitive information (e.g., patient details) (Porisini, Colombo, & Sicari 2011).

Besides security, healthcare services should provide accurate and complete information. In many scenarios, in fact, errors or missing values might have critical impact on actions or decisions. Accordingly, an IoT-based smart health system needs to guarantee well-defined levels of data quality. Four data quality dimensions can be considered (i.e., accuracy, timeliness, completeness, and source reputation), in order to inform users of the reliability of the accessed information. This is an innovative aspect since, as pointed out in Barbagallo et al. (2012), current available services provide the same information to each requesting user, often without considering his/her requirements and without specifying the level of security and data quality of the provided data.

Last but not least, it is important to remember that in the smart health context, the number of violation attempts can be significant. Therefore, it is fundamental to define and develop proper enforcement mechanisms.

In literature, several works begin to address some of the issues described above. But, as emerges in Sicari, Grieco, and Coen-Porisini (2015), Sicari, Hailes, Turgut, Sharaffedine, and Desai (2013), few efforts are currently made regarding the enforcement of security and data quality policies. Except for the work presented in Neisse, Steri, and Baldini (2014) and Sicari, Rizzardi, Miorandi, Cappiello and Coen-Porisini (2016a, 2016b), there are no specific solutions addressing policy enforcement in IoT applications. To the best of the authors knowledge, no specific enforcement solutions for IoT-based smart health systems are currently available. Some attempts have been already done to define the proper languages for the specification of policies (for instance, the contribution presented in El-Aziz and Kannan (2012), Anwar and Imran (2015), Wu and Wang (2011). A solution which addresses the definition of flexible and standardized access control mechanisms for protecting both quality and security of sensitive data across multiple, heterogeneous domains is still missing.

Based on these premises, this paper proposes a policy enforcement system for IoT that adopts a cross-domain policy specification language, able to manage the interactions among the involved entities under well-defined policies. To this end, XML syntax is used, due to its general-purpose and a highly customizable nature. The defined solution has to guarantee security and data quality in case of policy violation attempts, thus dealing with the large number of critical situations which typically characterize IoT deployments. To demonstrate the usefulness of the proposed approach, a running example, based on a smart health application, is detailed throughout the manuscript. This highlights that the adoption of enforcement mechanisms provides a flexible and effective access control to IoT resources. In addition, a preliminary performance analysis demonstrates that the conceived approach requires less than 150 Mbps of aggregate bandwidth, thus becoming feasible in large scale environments.

As a final comment, it is expected that the enforcement framework proposed hereby could be used in the future as a secure wrapper for managing policies in existing IoT architectures, such as OneM2M[1], OpenIoT[2], FIWARE[3], and MOBIUS[4], already adopted by many companies.

The paper is organized as follows. Section 2 analyzes the state of the art about the existing policy enforcement mechanisms. Section 3 provides a big picture of the conceived IoT Policy Enforcement Framework. Section 4 describes the conceptual model used for the definition of the involved entities and their relationships within the IoT scenario. Section 5 presents the reference scenario along with a running example based on a smart health application, and deeply discusses the policy enforcement framework, the policy language specification, and the adopted access control model. Section 6 analyzes storage, software/hardware, and bandwidth requirements characterizing the conceived IoT Policy Enforcement Framework. Finally, Section 7 ends the paper and provides some hints for future works.

[1] http://www.onem2m.org

[2] http://www.openiot.eu

[3] https://www.fiware.org

[4] http://iotmobius.com