Accepted Manuscript

Protecting personal data in IoT platform scenarios through encryption-based selective disclosure

José L. Hernández-Ramos, Salvador Pérez, Christine Hennebert, Jorge Bernal Bernabé, Benoit Denis, Alexandre Macabies, Antonio F. Skarmeta

PII:	\$0140-3664(18)30212-3
DOI:	https://doi.org/10.1016/j.comcom.2018.08.010
Reference:	COMCOM 5766

To appear in: Computer Communications

Received date: 12 March 2018; Revised date: 17 July 2018; Accepted date: 20 August 2018

Please cite this article as:, Protecting personal data in IoT platform scenarios through encryption-based selective disclosure, *Computer Communications* (2018), https://doi.org/10.1016/j.comcom.2018.08.010

This is a PDF file of an unedited manuscript that has been accepted for publication. As a service to our customers we are providing this early version of the manuscript. The manuscript will undergo copyediting, typesetting, and review of the resulting proof before it is published in its final form. Please note that during the production process errors may be discovered which could affect the content, and all legal disclaimers that apply to the journal pertain.



Protecting personal data in IoT platform scenarios through encryption-based selective disclosure

José L. Hernández-Ramos^{a,*}, Salvador Pérez^a, Christine Hennebert^b, Jorge Bernal Bernabé^a, Benoit Denis^b, Alexandre Macabies^b, Antonio F. Skarmeta^a

^aDepartment of Information and Communication Engineering, Computer Science Faculty, University of Murcia, Spain ^bCEA-LETI, Grenoble, France

Abstract

As the Internet of Things evolves, citizens are starting to change the way they share information and communicate with their surrounding environment, enabling a constant, invisible and sometimes unintended information exchange. This trend raises new challenges regarding user's privacy and personal consent about the disclosure of personal data that must be addressed by flexible and scalable mechanisms. Towards this end, this work introduces the concept of bubble, as a coalition or group of smart objects that can be created according to the relationship between their owners. The proposed approach is based on the use of attribute-based encryption to protect the associated data according to users' preferences, and FI-WARE components for deployment purposes. As a scenario example, the solution is integrated with a radio localization system, in order to protect location data in the context of smart buildings. Finally, this work provides implementation details about the required components, as well as their evaluation on real smart environment scenarios.

Keywords: Attribute-Based Encryption, Confidentiality, Internet of Things, Smart Buildings

1. Introduction

The inclusion of *Information and Communications Technology* (ICT) in our everyday environments has motivated the development of different initiatives to encourage the deployment of new services and applications in the scope of Smart Cities [1]. Much of the success of these scenarios is based on the continuous data sharing from a huge amount of heterogeneous data sources, such as smartphones, transport infrastructures or devices physically deployed in our surrounding environment. These devices are currently enabled to share their

Preprint submitted to Computer Communications

July 17, 2018

^{*}Corresponding author

Email address: jose-luis.hernandez-ramos@ec.europa.eu (José L. Hernández-Ramos)

Download English Version:

https://daneshyari.com/en/article/8953606

Download Persian Version:

https://daneshyari.com/article/8953606

Daneshyari.com