Computer Networks 143 (2018) 112–125

Contents lists available at ScienceDirect

Computer Networks

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

Decentralizing privacy enforcement for Internet of Things smart objects

Gokhan Sagirlar*, Barbara Carminati, Elena Ferrari

DISTA, University of Insubria, Italy

ARTICLE INFO

Article history:
Received 15 January 2018
Revised 3 July 2018
Accepted 9 July 2018
Available online 10 July 2018

Keywords:
Internet of Things (IoT)
Smart objects
Privacy
Privacy preferences
Decentralization

ABSTRACT

Internet of Things (IoT) is now evolving into a loosely coupled, decentralized system of cooperating smart objects, where high-speed data processing, analytics and shorter response times are becoming more necessary than ever. Such decentralization has a great impact on the way personal information generated and consumed by smart objects should be protected, because, without centralized data management, it is more difficult to control how data are combined and used by smart objects. To cope with this issue, in this paper, we propose a framework where users of smart objects can specify their *privacy preferences*. Compliance check of user individual privacy preferences is performed directly by smart objects. Moreover, acknowledging that embedding the enforcement mechanism into smart objects implies some overhead, we have extensively tested the proposed framework on different scenarios, and the obtained results show the feasibility of our approach.

1. Introduction

Internet of Things (IoT) technologies are revolutionizing our daily lives [1], building around us a pervasive environment of smart objects able, not only to sense data, but also to interact with other objects and to aggregate data sensed through different sensors. This allows smart objects to locally create new knowledge, that could be used to make decisions, such as quickly trigger actions on environments, if needed. Smart objects are very heterogeneous in terms of data sensing and data processing capabilities. Some of them can only sense data, others can perform basic or complex operations on them. Such a scenario enacts the transition from the Internet of Things to the Internet of Everything, a new definition of IoT seen as a loosely coupled, decentralized system of cooperating smart objects, which leverages on alternative architectural patterns with regards to the centralized cloud-based one, such as fog computing. Such a trend towards decentralization reduces the amount of data that is transferred to the cloud for processing and analysis, and can also be instrumental to improve security and privacy of the managed data, a major concern in the IoT scenario. However, decentralization, if not properly governed, might also imply loss of control over the data, with consequences on individual privacy.

In this paper, we focus on the challenging issue of designing a decentralized privacy enforcement mechanism, where compliance check of user individual privacy preferences is performed directly by smart objects, rather than by a central entity. Restrictions on devices' capabilities let us discard existing proposals for decentralized access control (e.g., [2–5]), as these heavily rely on cryptographic primitives. Previously, in [6], we addressed the problem of specifying and enforcing privacy preferences in the IoT scenario, but for a centralized architecture, that is, a scenario where devices have only the capability to sense data and send them to a data center for being analyzed. In this setting, the enforcement monitor analyzes every consumer query and decides if the privacy policy of the consumer satisfies the privacy preferences specified by owners of devices generating the data.Compared to this approach, decentralized privacy enforcement scenario requires to address several new important research challenges, as smart objects are characterized by heterogeneous processing capabilities. To address these challenges, in this paper, we extend the privacy preference model proposed in [6], by designing a set of privacy meta-data that are used by smart objects for locally checking and enforcing user privacy preferences at smart object level. Smart objects are thus able to derive privacy meta-data for newly created data items, keep track of the operations performed over data items, denoted as *history*, in order to ease privacy preference enforcement, and, finally, check compliance of the privacy policy of the data consumer with the privacy preferences associated with data items. To the best of our knowledge, this is the first work proposing a decentralized en-

* Corresponding author.
E-mail addresses: gsagirlar@uninsubria.it (G. Sagirlar), barbara.carminati@uninsubria.it (B. Carminati), elena.ferrari@uninsubria.it (E. Ferrari).

https://doi.org/10.1016/j.comnet.2018.07.019
1389-1286/

forcement of privacy preferences able to work locally at smart object level.

Acknowledging that embedding the enforcement mechanism into smart objects might imply some overhead, we have extensively tested the proposed framework. In doing the experiments, we have considered several scenarios, by varying the complexity of the privacy preferences, smart object networks, and evaluated queries. The experiments allow us to asses the feasibility of the proposed approach in a variety of application domains.

The remainder of this paper is organized as follows. Section 2 discusses related work. Section 3 describes the system model and design assumptions of the proposed privacy preserving framework. Section 4 introduces the privacy preference model. Section 5 presents the proposed enforcement mechanism. Experimental results are illustrated in Section 6, whereas Section 7 concludes the paper.

2. Related work

In recent years, security and privacy in the IoT domain have been deeply investigated, with the results that various approaches have been proposed for dealing with different aspects of security as well as of privacy. In this section, we provide an overview of those proposals that are more related to the proposed framework. In particular, we focus on those approaches that enforce, in some ways, users' privacy. However, we also have to note that literature offers several interesting proposals that, like our framework, deal with the problem of decentralized policy enforcement. All these efforts have been done in domains different from IoT, but they deserve to be cited and compared to our solution. In the following, we summarized work in these two directions.

2.1. Enforcement of users' privacy in the IoT domain

So far different access control models have been exploited in the IoT domain: role based access control (RBAC) (e.g., [4,7]); capability based access control (CapBAC) (e.g., [2]); attribute based access control (ABAC) (e.g., [3,8]), and access control models based on semantic rules (e.g., [9]). Although these proposals are instrumental to control how users' personal data are used, and thus, in some sense, to protect users' privacy, they do not make users able to provide their own preferences on how their data have to be used and distributed. In contrast, our proposal makes user able to have a full control on how data have to be processed (e.g., accessed, aggregated, released).

User's privacy preferences have been considered in [10], which proposes a framework avoiding inference of personal data due to data fusion. Users specify their privacy preferences in terms of a level of confidentiality associated with each data. The proposed framework consists of a central unit, called Personal Data Manager (PDM), that manages personal data collected by different devices, playing thus the role of a gateway between users and third party applications. A further module, called Adaptive Interface Discovery Service (AID-S), computes the risk of inference associated with a data disclosure, via probabilistic models and learning algorithms (e.g., RST, KNN, Bayes Filter, HMM etc.). Based on this risk value, AID-S recommends optimal privacy settings to users to reduce the privacy risks. Similar to our proposal, also this approach considers user's perspective, but only in stating the confidentiality level of personal data, whereas our privacy model considers several dimensions of a privacy preference. Additionally, we enforce privacy of the user against data inferences in a decentralized setting, being able to pose more limitations on possible data fusions.

Compliance of user's privacy preferences with third party's privacy policies have been considered in [11]. Here, it has been proposed an application for mobile phones that supports customers in making privacy decisions. Privacy preferences are automatically generated according to the result of a questionnaire filled by users. The application informs the user whether his/her privacy preferences complies with the corporate's privacy policies. In contrast, we handle privacy in a bigger application scenario, that is, we enforce user privacy preferences in a decentralized IoT scenario, where different smart objects may apply their own queries over data and other parties may get involved in data processing.

Similar to our approach, other proposals have targeted smart environments (e.g., smart home and smart city systems) with the aim of protecting users' privacy. In [12], authors address the security and privacy problems of IoT smart home at the network level, that is, by monitoring network activities of IoT devices to detect suspicious behaviors. An external entity, called Security Management Provider (SMP) has been proposed. SMP can add access control rules to protect specific IoT devices or can apply dynamic policies to change access control rules depending on the context (e.g., the family members being present or absent from the house). This proposals aims at protecting privacy of the user by limiting access on data through an external entity, i.e., SMP, with the use of context information. In contrast, in our approach, we enforce user-defined privacy preferences to protect users' privacy in a decentralized scenario.

In [13], a two layered architecture is proposed for protecting users' privacy in smart city applications. A trusted layer is designed to store real identities of individuals that can be processed only by the platform's components, without disclosing the identities to the outside world. In contrast, an untrusted second layer only makes generic, unidentifiable and identity-independent information available to external applications. Even if this proposal protects personal data, this is enforced only inside the trusted layer, without considering future operations that may be done on the released data to infer new sensitive information. Moreover, users are not able to set and enforce their own privacy preferences.

2.2. Decentralized policy enforcement

A notable example of decentralized privacy management is represented by the sticky policy approach [18]. According to this approach user privacy preferences are strictly associated (sticky) with users' data. Pearson and Casassa-Mont et al. [18] describe the core mechanisms required for managing sticky policies, along with Public Key Infrastructure (PKI) and encryption methodologies to attach sticky policies with data as well as to enforce them. Brown and Blough et al. [19] present a distributed enforcement approach for sticky policies that permits data to be disseminated across heterogeneous hardware and software environments without pre-existing trust relationships. Also, Sicari et al. [14] present a sticky policy approach to manage the access to IoT resources by allowing users to set and manage access control policies on their own data. In this approach, sticky policies allow to define: owner of the data; purposes for which the data can be used; a timestamp that points out the validity; and constraints which represent the rules for filtering the data with obligations and restrictions.

Our solution has some similarities with the sticky policy approach, as we share the same goal, that is, decentralized enforcement of user privacy preferences. However, in our proposal we go beyond the traditional privacy preference model, where constrains are posed mainly on purpose, retention time, and third party usage by proposing a mechanism to derive privacy preferences for newly generated data. Additionally, sticky policy approaches use encryption mechanisms to enhance privacy, whereas in our approach encryption is just used to secure communication. Indeed, encryption mechanisms add extra level of complexity and demand higher resources from the devices.