Computers in Industry 88 (2017) 35–43

Contents lists available at ScienceDirect

Computers in Industry

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

Data access control for energy-related services in smart public infrastructures

Yohei Kawada[a], Kojin Yano[b], Yoshihiro Mizuno[a], Tatsuhiro Tsuchiya[c,*], Yasumasa Fujisaki[c]

[a] Information and Communication Technology Business Division, Hitachi Ltd., 2-18-1, Konan, Minato-ku, Tokyo 108-8250, Japan
[b] Research & Development Group, Hitachi Ltd., 292, Yoshida-cho, Totsuka-ku, Yokohama-shi, Kanagawa 244-0817, Japan
[c] Osaka University, 1-5 Yamadaoka, Suita-shi, Osaka 565-0871, Japan

ARTICLE INFO

Article history:
Received 14 June 2016
Received in revised form 30 November 2016
Accepted 9 March 2017
Available online xxx

Keywords:
Data access control
Service platform
Energy related data
Smart public infrastructure
Energy service

ABSTRACT

In smart urban infrastructures, access control technology is needed to provide appropriate consumer data to appropriate service providers. In this paper, we analyse the characteristics of and problems with data access in the service platform for smart city public infrastructures to clarify requirements for data access control. Then, we propose a data access control method that satisfies these requirements. The data access control method encompasses a data model for access authorization information that reflects the contracts between consumers and service providers. We develop a prototype system that implements the proposed access control method and experimentally show that the proposed method satisfies performance requirement using the prototype system.

1. Introduction

Recently, the concept of smart cities has attracted much social attention. Proof-of-concept experiments have been conducted in many cities all over the world [1–3]. A smart city aims to "smartize" city's public infrastructures such as energy, water and transportation. Smartization means achieving high resource efficiency while improving the residents' comforts using IT.

The roles for IT in smartized public infrastructures, i.e. smart public infrastructures, are roughly classified as follows.

- Data acquisition

  Obtaining data from devices or equipment in real time.

- Data management

  Storing the collected data and providing them to users.

- Data application

  Utilizing the data in order to provide services to consumers.

A well-accepted information system architecture for smart public infrastructures is in the form of three layers: the sensor layer, the system layer, and the service layer which respectively correspond to the above roles [4,5]. An advanced form of the system layer is a *service platform* that collects the data from a wide variety of devices or equipment in the sensor layer and provides the data to a wide variety of applications in the service layer [4]. A possible future scenario is that this service platform is operated by a data management company, such as an electric power company or DCC (Data Communications Company), approved by the government or local authorities [6].

This paper discusses data access control for the collected data provided by the service platform. Data access control is considered a necessary function for the service platform [3,7,8]. In general, data access control means providing appropriate data to appropriate users on the basis of contracts between the data owners and the users. In this paper we consider data access control over energy-related data collected from consumers' devices and propose an approach to it.

A recent trend in the electric power industry is that the business model has become changing from the traditional two-party model, where consumers and electric companies as suppliers are the only players, to the aggregator model where aggregators play in between the two parties [9]. The aggregators serve the consumers in various ways, such as by visualizing their consumption amount

* Corresponding author.
E-mail addresses: yohei.kawada.tb@hitachi.com (Y. Kawada), t-tutiya@ist.osaka-u.ac.jp (T. Tsuchiya), fujisaki@ist.osaka-u.ac.jp (Y. Fujisaki).

http://dx.doi.org/10.1016/j.compind.2017.03.002
0166-3615/

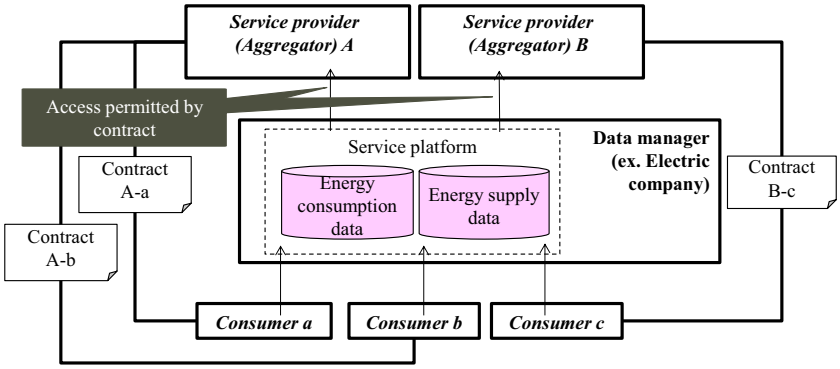

Fig. 1. Data flow among service providers (aggregators), consumers, and the service platform.

of energy or by directly controlling their appliances to save consumption. The consumer contracts with the aggregator individually for receiving the service. When the aggregator accesses the data stored by the service platform, the service platform has to limit the access to only a range of data that is permitted by the contract between the consumer and the aggregator. Fig. 1 shows data flows among these actors.

In the aggregator model, the service platform must support data access control. The problem of access control in the aggregator model is unique in that it requires dealing with energy-related data which can be very large as well as handling various consumer-aggregator relationships regarding access authorization over the large volume of data. However, there has not been enough research on data access control for such platforms. For example, there is no common agreement about how to formally represent the contract between a consumer and a service provider, or how to provide controlled data access based on the contract with practical performance. Although there are a few studies on access control for energy related services, none of them considers the aggregator model or fully addresses these issues.

To address this lack of research, we first clarify the requirements for data access control in the service platform, and then propose and evaluate a data model that represents the contents of contracts and a data access control method using the data model. The contributions of this paper are as follows:

- We present several possible practical services using energy consumption data and clarify data access control required by these services.
- We propose a data model that can represent the contract between a consumer and a service provider. Based on this data model we propose a data access control method.
- We quantitatively evaluate the performance of the proposed method by conducting an experiment using a prototype system.

The remainder of this paper is organized as follows. Section 2 describes the characteristics of data access and the requirements for data access control on a service platform. Section 3 describes the proposed data model which represents the contracts between consumers and service providers. Section 3 also presents the data access control method based on the data model. Section 4 experimentally evaluates the proposed approach using a prototype system with respect to performance. Section 5 concludes the paper.

2. Data model, applications, and access control requirements

2.1. Data model for energy consumption

In this paper, we assume that the service platform stores *energy consumption data*, the data about the amounts of consumed electricity based on the CIM (Common Information Model) object in OpenADE specification [10], which is one of the international standards for automatic demand response. Specifically, we assume that a sensing data is a tuple of numbers or strings that can represent CIM attributes and is appended to the database managed by the service platform every time a measurement is made. Hence the data collected can be represented in a tabular form, as shown in Table 1. This representation style is natural as stated in [11], because tabular format data are popular in industry and can allow standardized access via SQL, a common database language.

Table 1 shows how information is stored by the service platform in a tabular form. In the table, each row represents one sensing datum. Node ID means the unique ID of a device, Class ID the type of the device, and Timestamp the date and time when the measurement was made for the device. Instant consumption means the instant electric power consumption, while Cumulative consumption means the cumulative amount of electric power consumption of the device. The Power field is used for indicating the current on/off status of the device. The italic style symbolically represents concrete ID number. For example, *Device a-1* corresponds to a concrete Node ID, such as 00000801.

2.2. Possible services and data access control

As shown by Fig. 1, the service platform has to enforce appropriate access control over the data on the basis of the contract between the consumer and the service provider. In order to analyse the requirements for access control over energy consumption data, we list possible applications that make use of such data.

Table 1
Energy consumption data. Italic style symbolically represents concrete IDs.

Node ID	Class ID	Timestamp	Instant consumption	Cumulative consumption	Power
Device a-1	Smart meter	2015/5/11 10:00:00	21	1343	
Device a-2	Battery	2015/5/11 11:00:00	3	123	Off
Device b-1	Smart meter	2015/5/11 11:30:00	24	3442	
Device b-2	Heat pump	2015/5/11 12:00:00	4	63	On