Future Generation Computer Systems 38 (2014) 13–22

Contents lists available at ScienceDirect

Future Generation Computer Systems

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

Risk driven Smart Home resource management using cloud services

Tom Kirkham, Django Armstrong, Karim Djemame *, Ming Jiang

University of Leeds, Leeds, UK

HIGHLIGHTS

- Cloud computing can be utilized to aid decision making in the Smart Home.
- Risk based integrated management of devices can improve the utilisation of home resources.
- Contextualisation of services in Clouds can be applied to how devices are configured to improve their management.

ARTICLE INFO

Article history:
Received 21 May 2012
Received in revised form
6 February 2013
Accepted 2 August 2013
Available online 21 August 2013

Keywords:
Internet of things
Smart Home
Risk
Web services

ABSTRACT

In order to fully exploit the concept of Smart Home, challenges associated with multiple device management in consumer facing applications have to be addressed. Specific to this is the management of resource usage in the home via the improved utilization of devices, this is achieved by integration with the wider environment they operate in. The traditional model of the isolated device no longer applies, the future home will be connected with services provided by third parties ranging from supermarkets to domestic appliance manufacturers. In order to achieve this risk based integrated device management and contextualization is explored in this paper based on the cloud computing model. We produce an architecture and evaluate risk models to assist in this management of devices from a security, privacy and resource management perspective. We later propose an expansion on the risk based approach to wider data sharing between the home and external services using the key indicators of TREC (Trust, Risk, Eco-efficiency and Cost). The paper contributes to Smart Home research by defining how Cloud service management principles of risk and contextualization for virtual machines can produce solutions to emerging challenges facing a new generation of Smart Home devices.

1. Introduction

In the next decade users will be able to get information through the web from most devices in the home. Embedded web services (internet of things) are set to drastically change how we manage our resources in the home environment from the management of consumable goods to energy consumption. The future home will consist of multiple services linked to physical devices or resource monitors. A natural step in the management of these services is integration along the lines of specific applications or business models. Integration of services in this form aligns the future domain of the Smart Home with current challenges facing the Cloud computing community [1].

Likely applications in the home domain will be focused on the improved use of resources. For example, users will benefit from services to better manage their energy consumption and to improve the use of consumables in the home. The application of smart metering technology shares home data with distributed services in order to monitor energy consumption in order to improve eco-efficiency. The research in this domain is leading to the development of home control panel/dashboard technology for individual users and methods to share home energy data with suppliers and other parties interested in eco-efficiency in communities [2].

To date very little research has been conducted around service based management of home resource utilization. This paper aims to explore the potential of such an approach using risk based integration of home devices in multiple application scenarios linked into a wider Cloud based network of services. The risk assessments are formed by an user input and shape the monitoring and integration of devices in the network aiding Smart Home management for both resource consumption and device control.

The paper structure starts with a background section that describes the concept of the Smart Home and the need for input into the management of services. Moving on, the paper then introduces the use cases and then the risk models for improved resource use. This is followed by an evaluation of the risk models and a discussion section focusing on the initial results of the application of the models and the contextualization of devices. The paper ends with future work and conclusion.

* Corresponding author. Tel.: +44 1133436590; fax: +44 1133435468.
E-mail address: karim@comp.leeds.ac.uk (K. Djemame).

0167-739X/$ – see front matter
http://dx.doi.org/10.1016/j.future.2013.08.006

2. Background

Smart Home is the term given to the application of ubiquitous computing technology into the home environment. The creation of a Smart home environment can embrace a wide range of technologies and is best summarized in research terms within the category of the Internet of Things [3]. The common feature of the Smart Home is the creation of a network of devices that is capable of supporting communication to and from home appliances. Within this domain, research focus can be further separated into device specific categories such as home security, appliance management, digital entertainment, energy management and assistive computing/health care [4].

In terms of research effort the assisted living/health care in the home domain is a well-researched area of work. In this domain the research effort is driven by the cost benefits of remote health provision and constant patient monitoring in the home. However common technologies for assisted living tend to be application specific and the integration of the technologies is often non-standard [5]. This is because many assisted living applications pre-date web services and are designed in vendor specific or application focused environments dominated by specific vendors or procedures set by specific health care providers.

The adoption of wider standards in terms of the Smart Home as in many other domains is linked to the emergence of standards based networking technology and the internet. A good example can be seen in research and applications of Radio Frequency Identification (RFID) technology with the expansion of wireless networks [6]. The integration of home devices depends on the direct adoption of open standards or integration of legacy systems to gateways or services that support open standards such as available in the web services community [7]. Web services not only present standards for local integration but also allow distributed services to integrate with web service enabled devices present on the internet.

Enablement of Web Services at device level is directly linked to the ongoing increase of power in embedded processors driven by demand in devices such as Mobile Phones. Improved processing at device level and the development of standards and technology to aid Mobile device integration with the internet is significant for the Smart Home. Web Service toolkits and groupings of standards such as the Devices Profile for Web Services (DPWS), enable web services to be present on more powerful embedded devices [8]. Direct integration with devices via web services is significant as it removes the need for gateways to bridge technologies allowing direct communication with devices, this also enables standards based integration with web based applications outside of the domain of the home [9]. Thus no local hubs or servers are needed with devices connected directly over the internet. Future applications for the web integration of Smart Home devices range from ideas linked to social network integration of home appliances to the intelligent remote management of devices within Smart Grids [10,11]. In effect the devices in the home become services in wider Smart Home clouds. This remote integration is cited to have the potential to create a new domain of consumer facing computing applications and associated services. But, initial attempts at the compulsory adoption of home based devices have created problems in particularly with respect to data privacy. A good example of such issues can be seen in the domain for Smart Metering. In the Netherlands the government intended to make a compulsory roll out of meters as part of a national energy reduction plan, but this was curbed when privacy issues were raised [12]. The scheme is now voluntary and the issues of recording of device level data in the home can be seen to raise other privacy and trust risks for consumers [13].

The potential of device level services to leverage Smart Home integration with third party services depends on the level of support and protection offered to users. To help solve this problem the user needs to be presented with application processes and data sharing risks that they can understand. One approach to this is via the use of user defined risk assessment based service integration. This approach can be both linked to user preferences and embedded in the data sharing that embraces the Smart Home applications.

3. Use case

The use case is concerned with how a user can better use resources in his or her home. Typical improvements would deliver lower costs by improved energy and resource consumption in the home. The use case also includes the scenario where an organization is responsible for the management of multiple homes. This could be in the case of smart meters provided by an energy company, or in the case of domestic appliances the party could be a property maintenance company. To demonstrate how resource can be improved in the context of a single or multiple homes we demonstrate this by focusing on the use of resources by one common appliance. The appliance chosen is a washing machine. This choice was made because large amounts of test data exist for this type of appliance and the process of washing clothes involves multiple resources from energy, water and washing powder.

The key characteristics of a washing machine are broken into six assessment categories of energy consumption, appliance reliability, water usage, noise, usability and cost. Using these categories the user performs a risk assessment based on his or her preferences in terms of category weighting. The results of this helps the user choose the appropriate machine.

Once the machine is chosen monitored device contextualization can take place to deploy specific service types on the machine to suit different application environments. When the machine is being used data transmission takes place using this embedded web service device to send data in to external monitoring services. The user sets preferences for the management of the machine in terms of the wider home including:

- Terms on which to automatically reorder stocks of washing powder linked to best cost efficiency. Linked to supermarket costs and offer fluctuation.
- Energy management of resources such as water and electricity, linked to external costs of resources and energy consumption thresholds.
- Appliance maintenance in terms of when specific items need a deep clean or mechanical service. Linked to usage data.
- Management of the application is linked to requirements set by the user.
- Wider settings in relation to data security and privacy.

Risk management underpins the device, service and user relationships. Risk is associated with all data sharing transactions and agreements reached with third parties to share data, in all cases the security and privacy requirements of the user are taken into account. Risk is calculated from the user requirements set at the beginning of the process and also includes real time need from the environment (for example running low on washing powder). This risk then forms the basis on which third parties are engaged within the application requirements.

Fig. 1 illustrates the types of services provided by third parties that we expect to interact with our home data summarized into Energy, Appliances and Grocery data. Working clockwise from the top the energy company (windmill) would be interested in the energy consumption data for billing; the factory would receive information about appliance usage in order to add knowledge to the monitoring of devices to prevent failure. The metering of resource