Pervasive and Mobile Computing 43 (2018) 20–26

Contents lists available at ScienceDirect

Pervasive and Mobile Computing

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

Consume: A privacy-preserving authorisation and authentication service for connecting with health and wellbeing APIs

Mart Wetzels [a,*], Idowu Ayoola [a], Sander Bogers [b], Peter Peters [a], Wei Chen [c,d], Loe Feijs [a]

[a] *Designed Intelligence Group, Department of Industrial Design, Eindhoven University of Technology, Eindhoven, LaPlace 32, 5612AZ, Netherlands*

[b] *Designing Quality in Interaction Group, Department of Industrial Design, Eindhoven University of Technology, Eindhoven, LaPlace 32, 5612AZ, Netherlands*

[c] *Center for Intelligent Medical Electronics, Department of Electronic Engineering, School of Information Science and Technology, Fudan University, Shanghai, China*

[d] *Shanghai Key Laboratory of Medical Imaging Computing and Computer Assisted Intervention, Shanghai, China*

ARTICLE INFO

Article history:
Available online 15 November 2017

MSC:
00-01
99-00

Keywords:
Data acquisition systems
Authentication
Privacy
Healthcare
eHealth

ABSTRACT

The growth of the Internet of Things (IoT) application within the health- and wellbeing domain enables individuals to monitor their health. Acquired data can be used privately, contribute to clinical databases, or for research. The amount of health and wellbeing tracking devices introduces complexity in data aggregation and scattered overviews. Few services exist to aggregate health data. Current services raise privacy concerns. *Consume* is a service for aggregating authentication and authorisation for Application Programming Interfaces (APIs). *Consume* aims at research and allows to add existing and custom APIs on-the-fly without restarting services.

Introduction

Publicly accessible health APIs are increasing as companies are releasing new health trackers. In most cases, a single API will enable data extraction from a range of devices from the same vendor [1]. Bluetooth- and WiFi-enabled devices often provide a dedicated smartphone application for communication of data and a dashboard for the user to create insight on their behaviour. The increase in the type of trackers – activity, sleep, heart rate, respiratory – results in various applications being installed on the smartphone and resulting in a scattered overview of the consumer's data. Health Mashups integrate multiple data sources into a uniform interface and possibly create new insights with data fusion [2]. Related commercial Health Mashups and services are Apple HealthKit, Microsoft Health, GoogleFit, QoasiModo, Shimmer, Fitabase, and HumanAPI. HumanAPI targets companies, medical institutions, and other platforms   instead of directly to end-users.

Within the domain of pervasive healthcare, privacy is an important value [3]. The use of these services and individual devices raises the following issues concerning the user's or participant's privacy. Firstly, ownership of data often remains at the vendor, or they reserve the right to use and commercially exploit or share with affiliated partners [4]. Secondly, the

[*] Corresponding author.
E-mail addresses: m.h.wetzels@tue.nl (M. Wetzels), w_chen@fudan.edu.cn (W. Chen).

https://doi.org/10.1016/j.pmcj.2017.11.002

location of data stored from European Union (EU) citizens is becoming more regulated [5]; restricting storage in the US in some cases. Thirdly, commercial data aggregation services also hold the right to use the data as the individual vendors. The latter causes an increased privacy risk for consumers because the service holds data from various input streams; enabling a richer knowledge on the consumer's behaviour.

Consume facilitates the combination of ease of integration and preserving of privacy through pseudonymization to existing research that requires data aggregation through health and wellbeing APIs. Ease of integration is achieved by enabling expansion of supported APIs on a live system by prioritising universal logistics not bound by a single API. *Consume* lowers the threshold for researchers to experiment with a range of data sources and data generating devices. Preservation of privacy is achieved by the pseudonymization of Personally Identifiable Information (PPI) and by separating the concerns of authorisation/authentication and aggregation of data.

Personalised healthcare systems

The self-monitoring of weight using a scale is one of the oldest self-tracking devices adopted by the general public. Nowadays, the range of measurable body metrics has increased beyond weight and activity but the data extraction of these new devices are not always accurate, and different trackers show a divergence between measuring the same actions and behaviour [6]. A validation study on the accuracy of the Fitbit One (Fitbit) [7] concludes the device to be reliable for measuring step-count but warns about the accuracy of calculated distance travelled. Geolocation, collected by the Moves(ProtoGeo Oy) [8] application, can be used to complement the accelerometer-based step-detection from a wearable device. The iOS-application Gyroscope(Gyroscope Innovations Inc.) is a recent example of a system that uses sensor data from different devices to provide a richer overview of health- and wellbeing data.

Personal Healthcare Systems often focus on maintaining or increasing the user's health by providing insights and persuading them to be more active. The *Principe of Tailoring* [9] describes that contextual information, in combination with personal information, can increase the personalisation of tailoring technology for an effective persuasion strategy. For example, a running application that provides motivational support can take into account the weather, in relation to the user's performance, to determine the type of motivation that is required. Data acquisition systems need to be able connect to other APIs that can provide contextual information to enrich the personal information obtained from trackers. *Consume* enables researchers to access other APIs, following OAuth2 protocol, in addition to popular health and wellbeing APIs.

In addition to fitness and activity trackers, research is done on new applications within tracking of health. *Smart Cup* allows patients with fluid retention to measure their water intake [10] to prevent over-hydration. *SocialHue* utilises the HUE-lights (Philips) to increase social connectivity between elderly and their caregivers [11]. The last example uses the Philips HUE API to change the ambience in a living environment. *Consume* supports researchers to utilise these APIs for new development in personalised healthcare system. New devices and contextual information services, with their APIs, will be developed more rapidly than before. These developments emphasise the need for data validation models [12,13] to ensure the validity of aggregated data.

System

Consume uses Node.js (Node.js Foundation, 2016), an event-driven I/O server-side Javascript environment based on Google V8-engine, and utilises several popular dependency listed in Table 1; minor dependencies are not listed.

Fig. 1 illustrates the system architecture of *Consume*. In production environment *Consume* redirects to an encrypted connection between client and server when an SSL-certificate is provided. Authentication- and user-related data is stored in MongoDB collections named *users* and *usertokens*. API configurations are stored in the collection named *apis*. All collections have a Schema defined using Mongoose. The current version of *Consume* provides an interface, using Twitter's Bootstrap, for participants to register and link accounts. Other efforts addressed in this paper will include the removal of user interface, leaving the back-end, in a separate version of *Consume*. This version can be used for integration in existing systems.

Architecture

Figs. 2, 3, and 4 depict the Data Flow Diagrams (DFDs) of different data acquisition systems. The DFDs separate external and internal services. External services include the APIs where data is to be fetched, external systems, and possible databases. Internal services include the system for fetching data and local database. Fig. 2 represents a system with several APIs where each API requires dedicated code within the system to authorise with an API. Fig. 3 represents a service that aggregates APIs externally and enables internal services to acquire the data. Fig. 4 represent the *Consume* service where universal code is used to aggregate from different APIs within the internal service.

The benefit of using a data aggregation system, Fig. 3, over a custom data collection system, Fig. 2, is the reduction of complexity in the internal services.

The privacy issues raised by data aggregation services are caused by the aforementioned *right to use* and *ownership* of data by external services. These services are not transparent in how they (re-)use data. For the individuals sharing data it is not communicated what happens to their data and what other parties have access.