

A Distributed Open Social Platform for Mobile Devices

Monica S. Lam Giovanni Campagna Jiwon Seo Michael Fischer

Computer Science Department
Stanford University
Stanford, CA 94305

{lam, gcampagn, jiwon, mfischer}@cs.stanford.edu

CCS Concepts

•Human-centered computing → Collaborative and social computing; Ubiquitous and mobile computing;

Keywords

Internet of Things, social platform, personal virtual assistant, messaging

ABSTRACT

This paper presents the architecture of an open social platform for mobile devices. This platform allows users to get access to all their data in web services and IoT devices easily, compute with them, and share them with their friends without losing data ownership to a third party. The key concepts include: (1) *ThingPedia*, an open-source crowd-sourced repository of interfaces and apps, (2) *ThingTalk*, a succinct rule-based language that allows people to share information stored in different web services and IoT devices, (3) *ThingEngine*, personal servers that execute ThingTalk apps on behalf of the users, and (4) *Omlet*, an open chat and messaging platform that does not own users' data.

1. INTRODUCTION

We are at the advent of a new era where billions of IoT devices will be collecting every bit of our daily life. We have fitness devices that count our steps, phones or cars that record our whereabouts, and home devices such as thermostats, smoke alarms, and security cameras that monitor what goes on at home. Also becoming widely available are medical devices, from scales, to blood pressure, electrocardiogram monitors, etc.

Today, consumers are used to the model where social networks, such as Facebook and Snapchat, own the intellectual property of data shared on their systems. Would all the sensitive data collected by IoT devices be following the

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than the author(s) must be honored. Abstracting with credit is permitted. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from permissions@acm.org.

MobileSoft'16, May 16-17 2016, Austin, TX, USA

© 2016 Copyright held by the owner/author(s). Publication rights licensed to ACM. ISBN 978-1-4503-4178-3/16/05...\$15.00

DOI: <http://dx.doi.org/10.1145/2897073.2897075>

same model? Furthermore, our data are now kept in different silos. As more valuable data becomes available, it is important that we can access all our data and share them with whomever easily and confidentially. For example, it is desirable for us to share our medical records, along with all the data collected by a myriad of medical devices, with our doctors. In this way, doctors can provide better health care at a lower cost as they can monitor a large number of patients closely and pay more attention to those who need it.

Recently, we have started seeing cloud services that consolidate our data from a variety of sources. For example, Google Photos helps us find pictures saved across all the different photo web services with the help of its sophisticated face recognition algorithm. The website IFTTT helps us connect all our different accounts, from banking, Facebook, Twitter, to data on our mobile phones [1]. All these data consolidation services require that we give them the credentials to our various accounts. In addition, virtual assistants, such as Google Now, Apple's Siri, Microsoft's Cortana and XiaoBing, Facebook's M, and Amazon's Alexa, are emerging as killer applications that are providing simple, intuitive, personalized natural language interfaces to a wide collection of apps and services.

What does the future hold? Will there be a proprietary monopoly that owns all of our data and manages our data access? Or will there be a couple of non-interoperable systems, like Android and iOS, requiring consumers to adopt one system versus the other. These monopolies or oligopolies get to control the terms of how other companies can operate. If we do not have open competition, innovation will suffer.

2. AN OPEN MOBILE SOCIAL PLATFORM

Mobile devices, being truly personal and constantly in our hands and online, hold the promise of an open alternative. They make possible a distributed system where users can choose who host their data and interact with anybody they wish through direct phone-to-phone communication. We imagine a future where every app on the phone is social. Users can create groups and share easily, without worrying about a third party that tracks all their interactions. They can choose from a large collection of inter-operable apps, websites, or IoT devices. In the meantime, all apps can easily include social features that users can use with any group, not beholden to any social network that owns the users' social network.

To achieve the above goals, we have created a prototype

of an open social platform mobile devices. This platform consists of two components: (1) *ThingEngine*, which helps users access their data across all the different devices and web services, and (2) *ThingPedia*, an open-source, crowd-sourced repository, hosting all the public interfaces to websites, devices, and IoT apps. In this paper, we use the term IoT to refer to all resources from devices to web services.

2.1 Omlet Open Messaging Platform

Our distributed social platform uses Omlet to provide the underlying communication primitives. Omlet is an open chat app that lets users save data in a repository of their choice [2]. It is also a social app platform, as it has open social APIs that let users connect with friends, create a feed, and send/receive data from a feed. Omlet does not own any of the users' data. Omlet keeps users' communication data for only two weeks, users can currently choose to save their data in either Baidu cloud, Box, Dropbox, Google Drive, or Microsoft OneDrive.

The key communication abstraction in Omlet is a *feed*, a timeline of data and events that is shared by a group of users. Messages can be sent to a feed for distribution, and users can subscribe to feeds to receive new data. In Omlet proper, a feed corresponds to a group chat, but feeds can be used also for shared documents. Omlet handles identity authentication and management, as well as notification and delivery of the messages across users' devices and designated cloud services.

2.2 ThingEngine

ThingEngine is a personal server that runs applications on behalf of the user. It executes the IoT apps, logs users into the various resources, and keeps track of credentials to the various web services. It also keeps a catalog of all the IoT devices that a user can access, allowing users to refer to their devices based on their attributes. The ThingEngine can interface with the user via a personalized natural language assistant, named Sabrina, in an Omlet feed. The ThingEngine is open-source and can be run as a cloud service, in a home server, or even on a phone. For convenience, we also host a cloud service, and this cloud service has no ownership rights to any of the users' data.

2.3 ThingPedia

ThingPedia is an open-source, crowd-sourced repository of public interfaces and apps using these interfaces. Unlike IFTTT, all the information is open-sourced and the interfaces or apps can be executed anywhere. We expect de facto standards to emerge as certain devices become popular in each domain. The interfaces include authentication codes, which need to be invoked only once, by the ThingManager, when a user connects with an external service or device. The apps are written in ThingTalk, described below.

3. EASE OF PROGRAMMING AND USE

Distributed systems are notorious for being hard to program and hard to use. To address the complexity in programming, we have created *ThingTalk*, an IoT language that makes it easy to write privacy-preserving distributed applications in just a few lines of code.

ThingTalk programs consist of a set of rules; whenever the trigger on the left-hand-side fires, the action on the right-hand-side is taken. For example, we can say "if the weather

channel predicts rain tomorrow, send me an email message" in a one-line ThingTalk program. The triggers and actions may refer to public interfaces in ThingPedia. They may also refer to variables and computations; whenever the values of variables on the left hand side change, the right hand side is activated.

To facilitate data exchange between users in a feed, ThingTalk has feed-accessible variables. Communication can be achieved simply by writing to these variables; the updated results are pushed to everyone in the feed. By implementing on top of the Omlet messenger, ThingTalk enables a group of friends to exchange information without giving up data ownership to a third party. For example, a couple of lines of ThingTalk will enable a group of friends to share their locations in real time as they travel to their gathering, or attendees of a conference to exchange business profiles in their LinkedIn accounts among themselves.

The open mobile platform is also designed to be easy to use. A user can choose from a large collection of ThingTalk apps from the ThingPedia website. By default, results are returned in the user's feed with Sabrina, the virtual assistant. For group apps, users can simply invoke the app on the feed of interest. If any of the external services or devices require authentication, the user needs to only provide the credential once. The credentials are saved in the user's personal ThingEngine.

4. CONCLUSIONS

An open platform that encourages open competition, fosters inter-operability, and gives users the ability to access and share confidentially all their data will open up opportunities for many new applications. By making apps easy to write with ThingTalk and providing a crowd-sourced and open-source Thingpedia to collect interfaces and apps, we can potentially create better apps than those provided by closed proprietary systems.

The ThingEngine provides a safe haven where all our data can be accessed and shared, without the worry of losing privacy. This enables the creation of a new category of software that knows everything about us. For example, we have found that browsers and search engines, built with the full knowledge of our email history and social media we subscribe to, performed significantly better than tools we have today [3, 4]. This platform can also provide users with the ease of mind when installing privacy-sensitive devices such as cameras to monitor the well being of the elderly and children. Finally, confidential data sharing is critical to many important domains including education, finance and medicine.

5. REFERENCES

- [1] If-This-Then-That. <http://ifttt.com>.
- [2] Omlet chat. <http://omlet.me>.
- [3] S. Hangal, A. Nagpal, and M. Lam. Effective browsing and serendipitous discovery with an experience-infused browser. In *Proceedings of the 2012 ACM international conference on Intelligent User Interfaces*, pages 149–158. ACM, 2012.
- [4] A. Nagpal, S. Hangal, R. R. Joyee, and M. S. Lam. Friends, romans, countrymen: lend me your urls. using social chatter to personalize web search. In *Proceedings of the ACM 2012 conference on Computer Supported Cooperative Work*, pages 461–470. ACM, 2012.