Toward interoperability for the Internet of Things with meta-hubs

Julien Mineraud and Sasu Tarkoma
Department of Computer Science
University of Helsinki
Finland
Email: firstname.lastname@cs.helsinki.fi

Abstract—The Internet of Things (IoT) envisions that objects may be connected to the Internet, producing and consuming data in real-time. Today, numerous middleware platforms are available to facilitate the communication with these objects. Unfortunately, the interoperability of these platforms is very limited because it requires to “manually” connect the services proposed by each platform.

One key design goal for our contribution is not to build yet another middleware, but rather to augment the functionalities of existing systems via an extension to support their integration into a network of heterogeneous IoT hubs. The extension includes a RESTful API to manipulate the basic component of our extension, the IoT feeds. The IoT feeds allow the platform’s owner to dynamically marshal the IoT features connected to the platform, as well as the data that they produce. Furthermore, the feeds enable the owner to manage and control the data flows before connecting them to his applications. Subsequently, these feeds may also be published to meta-hubs in order to expose them to third parties.

We evaluated an implementation our extension for Android systems to show the feasibility of managing the data flows using the RESTful API on this platform.

I. INTRODUCTION

The Internet of Things (IoT) envisions to combine “smart” objects in our environment into a fully integrated future Internet [1]. Today, plethora of IoT middleware systems, proprietary or open-source, are available for integrating these smart objects into the IoT. The key priority for these platforms is usually to establish communications with a large variety of smart objects, such as sensors and actuators. These platforms also have varying requirements and technological implementations depending on the type of uses of the platform (e.g. domotic, environment monitoring, production line control, etc.). Furthermore, these platforms generally have their own ecosystems and may provide tools for applications or services developers (e.g. libraries, SDK, etc.).

However, IoT systems would benefit from using a generic architecture which provides IoT developers with a common toolkit for the development of IoT services independently of the underlying systems. We selected the following key principles for this architecture:

- Interoperability with other systems
- Ownership of data and device functionalities
- Scoping for managing data and functionality visibility
- Loose coupling and late binding

The first principle is the interoperability of the platform with other systems in order to form networks of heterogeneous but interoperable IoT systems. Moreover, the second principle ensures that the platform user retains full control of his devices and the data that they produce. This would be characterized by private and global spaces. Within the private space, resources are accessed via state-of-the-art access control mechanisms (e.g. OAuth2, etc.), while in the global space, resources can be accessed from within the network of interconnected platforms. This leads to the third principle where scopes are defined to grant permissions to use/view the data and other functionalities that are provided by the platform. Finally, the loose coupling and late binding designs have been selected to ease the manipulation of IoT resources by IoT developers using the common toolkit, in both private and global spaces.

In this paper, we present the IoT Hub architecture that covers these essential characteristics. Our solution is a simple extension of available middleware systems to provide communication between the middleware system and the IoT, as well as tools to control the data flows. The extension includes a RESTful API that supports fine-grained data management while re-attributing the ownership of data and devices to the hub owner. The IoT Hub API defines the concept of IoT feed (loose coupling) which is the basic component that marshals IoT data and features (i.e. sensors, actuators) available within the platform. An IoT feed is composed of its metadata (e.g. time-series data, dependencies to other feeds, scopes, keywords, etc...) as well as the declaration of fields metadata (e.g. type, name, keywords, etc.), and if applicable its data. The fields are not bound by numbers, but potentially by their types. In fact, the IoT feed metadata declaration ensures that fields have compatible types. For instance, a field that access a sensor’s data cannot be included in an IoT feed describing time-series data. The IoT feeds are exposed locally via the IoT Hub API for composition within IoT services (late binding), reserving that the IoT services have sufficient permission to access the feeds (fine-grained data flow control). Moreover, the hub owner has the option of publishing IoT feed descriptions to a special type of IoT hub, the meta-hub. Meta-hubs are the bridging pieces toward interoperability for hub-based middleware systems. The main role of the meta-hub is not to connect smart objects to the platform, but to collect IoT feeds metadata that are published by IoT hubs into
a browsable catalog. Additionally, meta-hubs include catalogs for IoT applications and services, as well as a search engine to extract information from their catalogs.

In order to execute the services and applications provided by the meta-hubs, the hub architecture includes a javascript engine. The choice of javascript was driven by the fact that most current IoT systems provide web services (RESTful API) and applications are included into a dashboard that is accessed via a web browser. Therefore, these IoT platforms could implement the IoT Hub architecture with only a small overhead.

The contributions of this paper are the following:

- We present a simple yet powerful IoT platform concept, the IoT hub, that interconnects various existing IoT systems. The main novelty stems from the IoT Hub API that exposes both data and control features to third parties.
- The hub follows a data feed design that allows fine-grained and real-time management of flows within a hub and between hubs (i.e. private and global (public) spaces).
- We present a concrete toolchain and implementation of the IoT hub for Android systems and demonstrate the benefits of local data feed processing.

This paper is organized as follows. Section II provides an overview of IoT middleware platforms and solutions toward interoperability for the IoT. This will be followed by Sections III and IV presenting respectively the IoT hub and the meta-hubs. Section V presents our implementation of IoT hub for Android devices and its evaluation will be presented in Section VI. Finally, Section VII concludes this paper and presents the directions for our future work.

II. RELATED WORK

In this section, we will present a number of IoT middleware solutions that could be extended as IoT hubs in the future. This will be followed by a summary of efforts that have been made toward the interoperability for the IoT.

A. Today’s IoT platform landscape

There are numerous IoT platform available today. The following list is not exhaustive but summarizes well the current landscape of IoT solutions.

The EveryAware platform provides an extendable data concept that could be used to enhance the possibilities of sharing and fusing data feeds. The platform is a centralized solution and was the only one focusing on a fine-granularity of data visibility. In our opinion, fine-grained data visibility is essential but is not yet well covered by current IoT solutions. In addition, it provides flexible and extendable data models.

The LinkSmart middleware platform, formerly Hydra, is an open-source service-oriented platform that enables the creation of a network for embedded systems, using semantics to discover the devices connected to the network.

The OpenIoT platform is an open-source platform, fully decentralized, that provides connectivity with constrained devices such as sensors. The platform envisions a billing mechanism for the use of services that would integrated to their solution.

The Thing System is a open-source software using Node.js that enables the discovery of smart things in the home environment. The software does not provide storage functionalities and must be coupled with a PaaS (i.e. Platform-as-a-Service) to enable storage outside the home area.

ThingSpeak is a decentralized, open-source server that may be used to store and retrieve IoT data. It allows opening of the channels to the public but do not provide extensive configuration of the these channels. The platform also provides visualization tools and enables the creation of widgets to visualize the data in a more personified fashion.

The Thing Broker is a centralized platform that provides a Twitter-like abstraction model for things and events to create local ecosystems such as smart homes. All the platforms previously mentioned, apart from OpenIoT, provide a RESTful API to interact with the platform.

B. Toward the interoperability for the Internet of Things

Recent work on distributed services for the IoT have shown the tremendous potential of supporting interoperability amongst IoT devices, platforms and users. For instance, Rachuri et al. [4] proposed a distributed task allocation mechanism from the phone to the local infrastructure to save battery energy of the mobile devices and thus, make the sensing as less intrusive as possible for the end users. Their solution achieved, by offloading sensing task to the local infrastructure, an energy saving of 35% compared to pure sensing. The offloading of sensing depending on the context-awareness have also been achieved with CoSense [5] that enable sharing of GPS location for users using a common transportation (e.g. in a train, bus, tramway or car).

However, a number of challenges, such as service composition, data-points availability, service discovery or data accuracy, have been highlighted in [6]–[8] to create interoperable service-oriented IoT solutions. Unfortunately, these challenges have not been addressed by today’s IoT solutions.

Lea and Blackstock [9], [10] have recently studied the interoperability of IoT platforms. Resulting from the observation of numerous IoT projects within the United Kingdom where most solutions are not interoperable, the authors presented a set of solutions to address this challenge. In particular, the authors introduced a multi-stage solution for interoperable IoT deployments [9].

The first stage consists on enabling IoT platforms to expose their services via RESTful APIs. Currently, most existing IoT platforms provide a RESTful API to enable interactions between the user of the platform and the smart objects, as well as extracting time-series data from the storage. At this point,
IoT service developers can use these services at a high cost of “manually” connecting the services to their applications.

The second stage involves agreements of common understanding, such as abstracted data and service models, between interoperable actors. The authors introduced for this latter stage, the HyperCat protocol [10], which aims to provide generic modeling of IoT data and services in order to construct catalogs of IoT services (URI) that are proposed by IoT platforms publicly.

The last stage includes the integration of complex semantics and ontologies to describe the services and things accessible via these platforms. We believe that such staged development for interoperability between IoT platforms, things and services is necessary to take advantage of the possibilities offered by a fully connected future Internet.

However, the catalog server do not incorporate billing and accounting mechanisms to facilitate transactions between IoT hubs, and the design of the search engine is currently based only on filtering. In the next section, we will present a simple yet powerful IoT platform concept that includes the basic functionalities to cope with the challenges inherited from the foreseen properties of the IoT.

III. IoT HUB

Based on our experience with IoT middleware solutions, the heterogeneity of these platforms is considerable (numerous hardware, technologies, requirements and objectives). Unfortunately, current platforms are not able to provide a solution that adapts to the requirements and objectives of all users. For instance on the first hand, The Thing System, which was mentioned in Section II, is designed for home automation and aims to simplify the communication between the system owner and his sensors and actuators (e.g. switch on or off a smart light, reading room temperature, etc.) and offers a nice and easy-to-use interface to the end-users. On the other hand, platforms, such as Axeda[4] provides PaaS for machine-to-machine (m2m) interactions to businesses in order to perform analytics and make proactive actions to replace faulty assets or schedule the recalibration of sensors.

Therefore, as our main objective is to create a network of heterogeneous hubs (depicted in Fig. 3), we propose the IoT Hub architecture (see Fig. 1). It has been designed to be easily implemented on any existing middleware systems. Hence, the architecture is independent of underlying technologies such as database management systems or particular web server implementations.

The IoT hub architecture is generic and includes a common stack of protocols to handle the devices or the data that would be processed by the hub. The hub may be small, if owned by a single individual (e.g. household), or very large (e.g. major company). The hub relies on the existing middleware system to enable the communication with the IoT features and external web service. The underlying system is also responsible of the storage of data[11], as well as the privacy and security mechanisms to access the platform [12], [13].

Depending on the hardware running the hub and the objectives of the IoT solution, several technologies could be used to fulfill these tasks. For example, IoT hubs running on mobile devices are limited in storage capacity, require complex energy management policies and are bound by the operating system to use specific technologies. From another standpoint, an instance of cloud-based IoT hub may have significantly more flexibility. In the particular case of data storage, some of the existing IoT platforms rely on NoSQL databases, such as MongoDB for the storage of time-series of sensor data, while others rely on large SQL databases such as PostgreSQL or Oracle.

The IoT hub is dependent on the underlying platform to provide enablers to instantiate the communication between the smart objects and the RESTful API. In the case of The Thing System, more than 70 “things” are currently supported by the platform, and 30 more are in development stage. We desire that IoT hub implementations benefit from potent efforts on enabling IoT technologies. The enablers also includes bridges to external web services (e.g. google maps API) in order to enrich the local data with external information.

In the IoT hub architecture, these enablers are also responsible of transforming the things to IoT feeds complying to the IoT Hub API. Our architecture favors the loose coupling of things and data by manipulating them via the concept of IoT feed. The IoT feed is the basic component of our architecture to abstract and marshal the properties of the things or the data that they produce. IoT feeds also include a non-empty set of fields that is not bound by size, but potentially by their types to ensure consistency of the fields with respect to the feed properties. As an example, a time-series feed, which may be composed or several data types (e.g. timestamp + temperature + GPS location), does not have the same properties than the atomic feed that accesses the current reading of a sensor or the state of an actuator.

From the IoT hub viewpoint, the things and the data that

http://www.axeda.com/
are handled by the platform are all represented by IoT feeds, which can be manipulated and combined within the private local space of the platform. To be noted that IoT hub feeds declarations are dynamical. A publish/subscribe mechanism is also available to interconnect feeds and generate data flows.

The local management of feeds will provide a rich environment for the IoT hub owner to manipulate data with increased flexibility. Consequently, the IoT hub architecture requires a strong modeling of data and services interoperability with strong type checking (data representation) and well-defined operations that can be applied to feeds (e.g. temperature data can not be aggregated with relative humidity data although they can be both represented by decimals). We envision for the back-end system of an IoT hub, a similar approach to the Yahoo! pipes™ service that transforms RSS feeds (from multiple sources) into new composed RSS feeds. In Yahoo! pipes™, simple operations such as filtering or text search can be applied to RSS feeds to enrich the content of the newly generated feed. Transposed to our IoT approach, IoT feeds could be derivated locally from local and external sources of information to be exposed to third-party services via the RESTful IoT Hub API. Furthermore, IoT services deployed on the platform could trigger operations based on the data they monitor, in a similar fashion than the IFTTT platform[6] or modify the sampling rate of time-series data to either increase accuracy or reduce the need of storage space.

A simplified application of this process with respect to the privacy of the user would be the transformation of the exact location of a hub user (GPS coordinates) into an anonymised location feed that only tells in which city the user is presently. This new feed could then be shared to external services that require GPS location only at a city-level granularity. An example for this third-party service would be a hub owned by a city and collecting weather measurements of individuals currently located in the city. The data flow of this example is shown in Figure 2. Consequently, new fine-grained policies for data exchange could be implemented and give the hub owner full control on the type of information that is shared externally (accessible from the public space).

The last feature of the IoT Hub architecture is an application engine to execute IoT applications that are based on the IoT Hub API. We opted for a javascript engine because most of today’s IoT applications are run from a dashboard in a web browser. Hence the majority of today’s IoT platforms would easily be extendable with no overhead.

In the next section, we will describe a particular type of hub, called meta-hub which provides additional functionalities to support interoperability between heterogeneous hub platforms.

IV. META-HUBS FOR IoT INTEROPERABILITY

Figure 3 depicts the internal components of meta-hubs. Meta-hubs are a variation of regular IoT hubs with a few differences. The role of meta-hubs is not to enable communication between the platform and smart objects, even if this is not mandatory, but rather to store information about IoT hubs and the services that they published. We opted for an IoT Hub URI catalog that is similar to HyperCat[10] which is a repertoire of IoT hub URI that were published by IoT hubs.

Additionally, the meta-hubs would include another catalog for applications and services that are based on the IoT Hub API and can be executed by the javascript engine. This allows the IoT developers to publish and distribute their products to a large number of IoT platforms effortlessly. Moreover, the applications can take advantage of using local feeds while extracting data from remote sources that are available through the meta-hubs. For example, an application could extract temperature from a local sensor feed, and compare the recorded values with the twenty closest temperature sensor feeds from the current location of the user without needing to manually set with which IoT platforms the application has to connect.

To realize these operations, meta-hubs need to incorporate an efficient search engine to browse efficiently through their own IoT feed catalogs, as well as requesting missing infor-
mation from other meta-hubs. Recent work [14] investigated the exploitation of the current web infrastructure to build a search engine dedicated to the IoT. However, we believe that the catalogs of meta-hubs will bridge that gap and the main attributes of the search engine would be to retrieve the best quality of results (e.g. data accuracy, low latency) while avoiding data redundancy.

In addition, components for authentication, billing and accounting could be included to meta-hubs to facilitate transactions between IoT hubs and create potentially novel business and economical models taking advantage of the new opportunities emerging from the IoT. An example is the Windows Azure Data Market[17] which provides catalogs of data which are browsable online, so application developers can easily find the resources necessary to make their application. The marketplace includes different billing schemes (e.g. time-based, quantity-based, free, etc.). The disadvantage of their solution is the need for data producers to build models for data manipulation which require the application developers to learn the data models for every dataset.

Lastly, we would like to elaborate on a possible application and show where the meta-hubs and IoT hub infrastructure would improve existing infrastructures. In a smart city scenario, we foresee that IoT hubs could be owned by individuals in every home. The IoT hub would provide off-the-shelf applications for home automation (i.e. retrieved from the meta-hubs application catalog). Today, home automation middleware systems enable the users to interact with their devices wirelessly, monitor various environmental parameters such as the electric consumption, room temperature and even the content of their fridge. Mostly this information is private, but home owner may be willing to send weekly reports (privatized feeds) about their energy consumption to the building hub. In the meantime, the building hub may build its own weekly report for the city hub, which may be able to analyze the data and deduct if a particular neighborhood would have abnormal energy consumption. The city may in the future understand that this neighborhood may, for instance, have a different isolation material that is inefficient for this location and act accordingly.

Consequently, to achieve this type of scenario, a large dissemination of heterogeneous IoT hubs and meta-hubs would be necessary. Hence, we present in the next section an implementation of the IoT hub for Android systems.

V. IoT HUB FOR ANDROID

We implemented a version of the IoT hub for Android (aHub) because the majority of IoT platforms for mobile phones are rather limited and that mobile phone users represents a potentially large volume of IoT users for the IoT hub architecture to sustain (i.e. ecosystems of IoT hubs).

The IoT hub for Android uses the NanoHttpd[15] lightweight web server to answer HTTP requests as defined by the RESTful IoT Hub API. The application includes two activities: (i) a WebVi

To evaluate the IoT hub platform and demonstrate the feasibility of managing the data flows using the IoT Hub API, we designed a simple application. The application first checks for the availability of two types of atomic feeds: (i) a feed giving access to accelerometer data and (ii) a feed to a switch (data modeling of an actuator with only ON/OFF states). In our scenario, this will be the camera flash of the Android smartphone. If the feeds are available, the application becomes usable and can be started by clicking a button on the dashboard. The application will then periodically retrieve the accelerometer data and compare it to the previous measurements in order to detect a “shake” gesture. When the shake gesture is identified, the application will toggle the state of the ON/OFF feed and stops the measurements.
for 2 seconds. We have used this application to evaluate our platform with respect to feasibility of managing the data flows using the IoT Hub API.

An example of the comparison between the native (developed with the Android SDK on a Samsung Galaxy S3 mini) and the javascript applications is shown in Fig. 4. In this experiment, the user shook his phone, after starting the applications (starting the javascript application automatically launches the native application), repeatedly at various frequencies. In Fig. 4, the force represents the absolute difference between the aggregated $x$, $y$ and $z$ of the accelerometer of two consecutive measurements (every $200\text{ms}$). The experiment included three stages: (i) the phone was shook every $30\text{s}$, (ii) the phone was resting on a table and (iii) the phone was shook at high frequency.

During the experiment, the javascript application is expressing very similar behavior to the native applications. However, some delays can be observed during the last stage of the experiment. These are due to the time required to access the phone’s camera (the native application did not have it implemented to avoid concurrent use of the camera). This resulted in the javascript application to miss some of the shake gestures observed by the native application. The experiment was repeated 20 times and has always shown identical patterns.

Thus, this demonstrates that it is feasible to manage the data flows using the IoT Hub API. Moreover, these applications are available for all hub-based platforms and can be distributed to a wide audience via the meta-hubs.

VII. CONCLUSIONS & FUTURE WORK

In this paper, we presented the generic IoT Hub architecture to enable interoperability between IoT solutions. The key component of the architecture is the IoT feed that provides loose coupling of the data and assets managed by the platform. The platform owner is able to regain the ownership of the data and the devices functionalities by dynamically managing the IoT feeds properties via the IoT Hub API. Additionally, the IoT feeds may be exposed to third-parties services by publishing their description to meta-hubs. Hence, meta-hubs are the cornerstones of networks of interoperable hubs with added functionalities to distribute applications and services based on the IoT Hub API. We demonstrated the feasibility of controlling data flows with the IoT Hub API as native and hub-based applications expressed similar behaviors.

We envision for future work to use an IoT-dedicated DSL for the development of complex applications such as distributed analytics on a network of hubs. The applications will include the composition of numerous data flows, sensor data corrections, data aggregation and fusion in a distributed fashion on heterogeneous middleware systems.

REFERENCES

[1] L. Atzori, A. Iera, and G. Morabito, “The internet of things: A survey,” Computer Networks, vol. 54, no. 15, pp. 2787–2805, 2010. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1389128610001568
[2] M. Becker, J. Mueller, A. Hotho, and G. Stumme, “A generic platform for ubiquitous and subjectve computing,” in Proceedings of the 2013 ACM conference on Pervasive and ubiquitous computing adjunct publication, ser. UbiComp ’13 Adjunct. New York, NY, USA: ACM, 2013, pp. 1175–1182. [Online]. Available: http://doi.acm.org/10.1145/2494091.2497570
[3] R. A. Perez de Almeida, M. Blackstock, R. Lea, R. Calderon, A. F. do Prado, and H. C. Guardia, “Thing broker: a twitter for things,” in Proceedings of the 2013 ACM conference on Pervasive and ubiquitous computing adjunct publication, ser. UbiComp ’13 Adjunct. New York, NY, USA: ACM, 2013, pp. 1545–1554. [Online]. Available: http://doi.acm.org/10.1145/2494091.2497588
[4] K. K. Rachuri, C. Efstratious, I. Leonidatis, C. Mascolo, and P. J. Rentfrow, “Metis: Exploring mobile phone sensing offloading for efficiently supporting social sensing applications,” 2013 IEEE International Conference on Pervasive Computing and Communications (PerCom), vol. 0, pp. 85–93, 2013.
[5] S. Hemminki, K. Zhao, A. Y. Ding, M. Rannanpärvi, S. Tarkoma, and P. Nurmia, “Cosense: A collaborative sensing platform for mobile devices,” in Proceedings of the 11th ACM Conference on Embedded Networked Sensor Systems, ser. SenSys ‘13. New York, NY, USA: ACM, 2013, pp. 34:1–34:2. [Online]. Available: http://doi.acm.org/10.1145/2517351.2517402
[6] T. Teixeira, S. Hachem, V. Issarny, and N. Georgantas, “Service oriented middleware for the internet of things: A perspective,” in Proceedings of the 4th European Conference on Towards a Service-based Internet, ser. ServiceWave’11. Berlin, Heidelberg: Springer-Verlag, 2011, pp. 220–229. [Online]. Available: http://dl.acm.org/citation.cfm?id=2050669.2050893
[7] S. Cherrier, Y. Ghani-Doudane, S. Louhier, and G. Roussel, “Salt: A simple application logic description using transducers for internet of things,” in IEEE International Conference on Communications (ICC), June 2013, pp. 3006–3011.
[8] G. Xiao, J. Guo, L. D. Xu, and Z. Gong, “User interoperability with heterogeneous iot devices through transformation,” IEEE Transactions on Industrial Informatics, vol. 10, no. 2, pp. 1486–1496, May 2014.
[9] M. Blackstock and R. Lea, “Toward interoperability in a web of things,” in Proceedings of the 2013 ACM conference on Pervasive and ubiquitous computing adjunct publication, ser. UbiComp ’13 Adjunct. New York, NY, USA: ACM, 2013, pp. 1565–1574. [Online]. Available: http://doi.acm.org/10.1145/2494091.2497591
[10] R. Lea, “Hypercat: an iot interoperability specification,” IoT ecosystem demonstrator interoperability working group, Tech. Rep., April 2014. [Online]. Available: http://eprints.lancs.ac.uk/2517402
[11] R. Roman, P. Najera, and J. Lopez, “Securing the Internet of Things,” Computer, vol. 44, no. 9, pp. 51–58, 2011.
[12] M. Ma, P. Wang, and C.-H. Chu, “Data management for internet of things: Challenges, approaches and opportunities,” in Green Computing and Communications (GreenCom), August 2013, pp. 1144–1151.
[13] X. Wang, J. Zhang, E. M. Schooler, and M. Ion, “Performance evaluation of attribute-based encryption: Toward data privacy in the iot,” in IEEE International Conference on Communications (ICC), June 2014, pp. 725–730.
[14] B. Ostermaier, K. Röer, F. Mattern, M. Fahrmair, and W. Kellerer, “A real-time search engine for the web of things,” in Internet of Things (IOT), 2010, pp. 1–8.

[15] J. Vouillon and V. Balat, “From bytecode to javascript : The js_of_ocaml compiler,” Software: Practice and Experience, 2013. [Online]. Available: http://www.pps.univ-paris-diderot.fr/~balat/publications/vouillon_balat-js_of_ocaml.pdf