International Journal of Advanced Computer Technology (IJACT)

ISSN:2319-7900

A GENERIC & EXTENSIBLE ASSET MODEL FOR A SEMANTIC COLLABORATION FRAMEWORK

Mohammad Amir, School of Engineering & Informatics, University of Bradford, UK; Yim Fun Hu, School of Engineering & Informatics, University of Bradford, UK; Prashant Pillai, School of Engineering & Informatics, University of Bradford, UK

Abstract

Unified data dissemination in the Internet/Web of Things remains an issue of further research. Some focus has been given to this problem in the current literature, but the outreach is still limited to similar, inter-organisation systems. However, to solve the problem of exposing data and knowledge to external agents, cross-vendor collaboration needs to take place. This paper proposes a Service-Oriented Architecture-based integration of semantic technologies within the Web of Things to produce a distributed and semi-autonomous collaboration framework that is capable of offering cross-vendor information exchange and collaboration facilities. By exposing the framework as a web application with a RESTful API and powering it with a semantic engine, the proposed system becomes capable of offering an extensible knowledge management and exchange platform that can handle dynamic and business-oriented applications in the Web of Things. Critical analysis and evaluation of the system prototype is done by testing it in a disaster management application scenario to show that the asset model for the proposed framework is sufficiently capable of meeting the dynamic cross-vendor information exchange and collaboration needs.

Introduction

The Web of Things (WoT) is a concept that focuses on producing, interacting with and consuming web-services offered by internet-enabled "things". These "things" range from simple sensing devices to complex multi-sensor platforms. In essence, WoT envisions devices that can be browsed and interacted with similarly to how we currently browse and interact with the web. The typical application scenarios in this regard range from the casual sensor networks, deployed for example to collect environmental data, to business-centric applications involving management of disasters and deployment of smart environments. As the range and diversity of applications increases, so does the need to effectively collaborate amongst the myriad of involved systems and actors. Analysis of existing literature reveals the growing need to tackle this issue of unified data dissemination, especially in relation to the enablement of cross-vendor collaboration.

Take, for example, a scenario involving a major flood in London, UK. Management of this disaster will not only involve the participation of different emergency departments like the Police, Ambulance Service, Coastguard, Search and Rescue, and thus warrant collaboration amongst these heterogeneous responders; but equally important will be the task of disseminating critical information to the general public of which include affected/likely to be affected people, their relatives and friends, the general public and he media. Thus the problem here is not only of timely and controlled data dissemination amongst the *active* responders tackling to manage the disaster(s) but also of distributing useful information and regular updates to *passive* parties so as to communicate the most correct and up-to-date information. There is also support for this claim of disseminating data effectively and in a unified manner in current literature, for example, in [1]. The preceding problem can be generalized and applied for the whole Web of Things (WoT) domain, for example, in scenarios involving smart homes [2], offices and even entire cities where a multitude of devices and non-linear data loads are common and collaboration outside the remits of the immediate trusted organization remains a pressing issue. In this paper, a Semantically-enriched and semi-Autonomous collaboration framework for the Web of Things (SAW) is proposed to deliver a solution that can integrate private, restricted and non-interoperable information hubs like governmental bodies. The contribution of SAW in the scope of this treatise is the design of a generic and extensible resource-based asset model which sets the foundations for the ensuing cross-vendor collaboration mechanisms for sharing sensing device properties and data semantically.

The rest of this paper is organized as follows: Section II introduces the problem statement and discusses the problem of collaboration and knowledge management, followed by the design formulation of the concept architecture and the asset model in Section III and the presentation of a test case scenario in Section Section IV. Finally, Section V concludes the paper.

Background and Problem Statement

The purpose of a collaboration framework in the context of the Web of Things (WoT) and as defined by this study is

ISSN:2319-7900

to: (1) Capture and represent data, (2) Generate knowledge, and (3) Share and exchange information and knowledge with external human and machine agents. As such, a collaboration framework can be envisioned as having several components as illustrated in Figure 1.

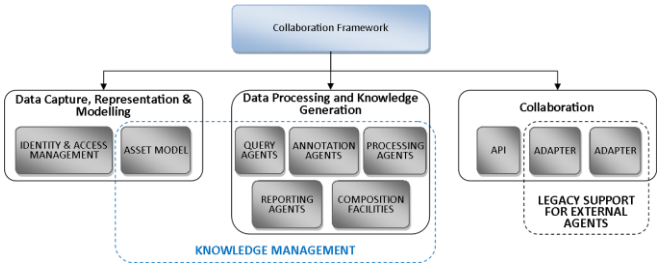

Figure 1: Collaboration framework concept diagram

Data Capture, Representation and Modelling is the first component of the framework, where acquisition of raw data and its modelling in some form of schema takes place. The next component involves Data Processing and Knowledge Representation, where semantic contexts and business rules are applied on the data to convert it into information and actionable knowledge. Finally, Collaboration takes place when the processed knowledge is ready to be exposed and collaborated upon with external agents, either through an Application Programming Interface (API), or via proprietary adapters. The Data Processing and Knowledge Representation component together with the 'Asset model' within the Data Capture, Representation and Modelling component make up the Knowledge Management (KM) framework. This paper is specifically focusing on the Asset Model of the KM framework.

In WoT, there is a strong emphasis on both the amount of data being generated and the ability to understand and derive knowledge from this data effectively and accurately; and also to expose these internal assets to the web [1] [3]. The exposition of sensing device data for cross-vendor collaboration purposes requires the development of a unified collaboration framework which can offer standardised information exchange facilities. A set of preliminary requirements for such a unified collaboration framework are devised as follows:

1. Capability to *acquire*, *model* and *store* large volumes of data over a prolonged period where the data load and processing needs are non-uniform.
2. Capability to *derive* high-level knowledge that is composed of low-level raw data (e.g. the knowledge "It was freezing in the flooded Sunbury, UK, on the 24th March", derived from various sensor data such as temperature reading, water level, location and time of capture).
3. Capability to *expose* private assets (sensing devices and their associated properties and data) to the web.

Existing literature has used terms such as Information/Knowledge Management Systems (IMS/KMS) [3] and Emergency Information Systems (EIS) [4] amongst others to refer to systems that capture, represent and process data and knowledge. Regardless of the terminology, the intent of these systems is to *manage assets*, be it related to the actual collection, processing and analysis of data or the consequent knowledge-derivation to enable business processes. In the literature review section it is shown that existing solutions do not effectively tackle the issue of data dissemination outside the remits of the individual organisations. This restricts the collaboration capabilities of the existing KM systems. This study proposes the SAW framework as an enabler of unified data dissemination to enable cross-vendor collaboration.

Problem of Collaboration

While SAW has been designed as a generic platform, the prototype has been tailored towards the disaster management (DM) application domain to give the framework substance and enable critical evaluation. DM is seen as a suitable candidate not only because of its growing importance in the wake of increasing natural disasters [5] [6], but also because of its widespread affects, the plurality of the involved actors and the heterogeneity of these very actors. In DM, there is the major problem of integration and collaboration simply due to the myriad of involved parties, for example, aid agencies (National Governmental Agencies or NGOs), government personnel, volunteers and businesses. Each actor has their own organisational boundaries, fiscal constraints, working practices and technological capabilities [7] [8]. The differences in cultural and organisational policies as well as conflicting priorities further complicates the collaboration process. [9]. Thus the issue of collaboration and timely data dissemination turns into a complex procedure of "who has what", "where is it" and "who needs it". As no single operational actor enjoys the full authoritative role, there is usually no entity that has the authority, capability and resources to monitor and coordinate the activities of the other participants. Furthermore, there can exist disparities within the IT systems of each organisation, making them incompatible with each other and therefore hindering cross-vendor collaboration. Thus, a top-down centralised approach is ineffective in these situations due to the plurality and heterogeneity of involved parties, their inherent differences, and their trust relationships with each other [10]. On the contrary, a decentralised network might provide more glue to the myriad of actors as suggested by available evidence from academic

ISSN:2319-7900

research [9] [11]. Although the aforementioned research suggests a loosely-coupled social network, the same concepts can be applied to an online electronic network, a "network of networks" which would allow potential actors access to data of interest so long as they are authorised to consume the given data.

Literature Review

Murphy & Jennex [12] highlight the importance of KM and the growing necessity of its effective application in DM. The study states that citizens would often like to contribute but are unable to, not only because they are not inside the physical operations but also because responders themselves are not able to reach out to the community to mine data. Furthermore, the study mentions the growing importance of dynamic and adaptable systems. The KM study presented by Bharosa & Janssen [13] is very comprehensive in this regard as it deals with the issue of information management adaptability, that is, the system's ability to dynamically manage resources in response to external demand and events [13]. The team concluded that overall the information quality was poor in regards to its relevancy (who is it for), consistency (various interpretations), accessibility (lack of contextual information), reliability, correctness and completeness (at the time of viewing). Furthermore, they allude to the fact that existing EIS systems are very close-knit and inflexible solutions that do not permit integration of external assets.

The study in [14] presents a web-based EIS built upon a Role-Based Access Control (RBAC) model and tackles the issue of actor heterogeneity within an EIS environment. It relies on the hypothesis that roles and responsibilities largely remain constant within an organisation and it's the users that change, therefore RBAC offers a convenient and maintainable solution. Whilst this access-based model produces a transparent and auditable data access system, the authors exclude the issue of collaboration within the RBAC model, thereby hindering third-party integration. A more comprehensive model is presented in PMISRS (Personalized Multidisciplinary Information Seeking and Retrieval) [15] where the authors discuss a service-oriented and resource-based architecture that is capable of providing users with personalized services based on their profiles (composed of the user's role and associated tasks within the DM team). However, once again a lack of focus on developing cross-vendor collaboration mechanisms dampens the outreach of their solution.

On a slight tangent, an experimental study in [16] signifies the issue of *trust* in computing technologies that are made *invisible* to hide the underlying complexities. The study evaluates that in order to build *trustable* pervasive systems; the design needs to embody: (1) Flexible interaction modes to enable multiple forms of inspection and (2) Multiple layers of inspection to enable retrospection at different abstractions. This level of transparency can be best achieved by utilising a resource-oriented model. Similarly a very recent experiment by Caragea et al. in [17] highlights the growing importance of social media integration in DM applications and the inherent challenges imposed for machines in learning to analyse and *classify* information posted by the general public. The findings in this study are further augmented by [18] where social media is portrayed as a powerful information dissemination tool that also has the potential of being a disruptive agent if the data is not processed methodically. They argue that ontologies need to be formulated and/or identified for formalising the capture of CR data from social media. This analysis supports this paper's statement that a next-generation semantics-driven collaboration framework for the WoT needs to have the capability to integrate with social media and take steps to ensure that information retrieved through these non-official networks is used, albeit cautiously, to build a more complete model regarding the situation on the ground.

It is important to note that in all the presented studies, very few actually tackle the issue of unified data dissemination. Where this issue has been given some focus, the outreach has been more or less limited to *similar systems* (i.e. cross-instance collaboration) and no particular focus has been applied on the problem of exposing this data or knowledge to third parties (i.e. cross-vendor collaboration). DERMIS in [19] provides the most comprehensive set of principles and guidelines for developing an EIS but promotes a single integrated enterprise type system that spans all the functions of the emergency response from planning through to execution and recovery. However, this goes against the very premise and design principles of modern distributed systems. So while respecting the design principles offered by this study, this paper refutes the single-systems approach as it's incompatible with the modern decentralised and distributed nature of web services. Furthermore, whilst the availability of a single authoritative system might improve data accuracy and consistency, it hinders third-party integration and thereby limits not only the ability of regular users in accessing and making use of the system, but it also dampens the prospects of mining data from disparate sources.

SAW: SEMANTICALLY-ENRICHED & SEMI-AUTONOMOUS COLLABORA-

ISSN:2319-7900

TION FRAMEWORK FOR THE WOT

Analysis of the current literature in the field of DM and collaboration systems reveals the need for a unified and extensible collaboration model. This collaboration model needs to be flexible enough to cater for cross-vendor collaboration so that private assets can be shared readily, whilst at the same time, assets from suitable third-party services can be easily brought in-house and exploited to create advanced mashups. Furthermore, many of the existing systems use RBAC which, though is suitable for a set of uniform organisations with similar roles and hierarchies, is inefficient for representing a generic non-organisation-based asset model. A cross-vendor collaboration framework requires a more comprehensive and decoupled access control mechanism. The SAW framework proposed in this paper is envisioned as an enabler of cross-vendor collaboration by virtue of its decoupled, semantics-enabled, service-oriented and resource-based asset model and the corresponding collaboration mechanisms. The focus of SAW is on developing the actual collaboration mechanisms to achieve this vision which requires first the development of the underlying asset model. However, as SAW is designed to be generic in nature, the focus is not to provide all the functionalities required by a DM application, but rather provide the underlying functionality and the necessary mechanisms to enable the extension of SAW to any WoT-related application. Therefore, the focus of SAW is on tackling the problem of collaboration amongst vendors that ultimately do not trust each other but still want to make use of each other's assets. This paper will present the concept and asset model required to achieve this vision.

Concept Architecture & Data Model

SAW is a combination of three distinct but cooperating systems as shown in Figure 2.

1. Semantics Engine: Enabled by the Apache JENA implementation and running on a Java VM, the semantics engine deals with the semantic annotation of resources on the network as well as semantic reasoning and querying of assets. The semantics engine is exposed to the web through an Apache Tomcat servlet.
2. Webserver: The front-end web application is hosted on an Apache webserver and exposes the underlying functionalities through a RESTful API (Application Programming Interface). Amongst other things, the web application:
    a. Exposes the semantic engine for applications like semantic querying of assets.
    b. Provides a UI for the web app users.
    c. Provides a web-based administration client for the instance administrators.
    d. Exposes a RESTful API.
3. Real-time server: Powered by Node.js, this acts much like the webserver above but has a few additional key functions that enable real-time monitoring and analysis of the network as well as real-time capture and publication of assets.

It can also be seen from the concept architecture that SAW exposes various RESTful endpoints in an extensible manner. In the future, the core framework's functionality may be further increased resulting in extension of the API currently defined. The following APIs would be required for efficient working of the SAW framework:

- Feed, Stream & Point APIs: These correspond to the data hierarchy presented below in Figure 4 and allow devices to publish data on the network.
- Tokens API: Corresponding to the TBAC system presented earlier, this API handles token generation, allocation and management.
- Subscriptions & Publishing API: Participants and observers can subscribe to and receive publications from system feeds, streams and events using these APIs.
- Events API: This API enables creation of custom triggers in response to events (event-based) and/or schedules (time-based).

ISSN:2319-7900

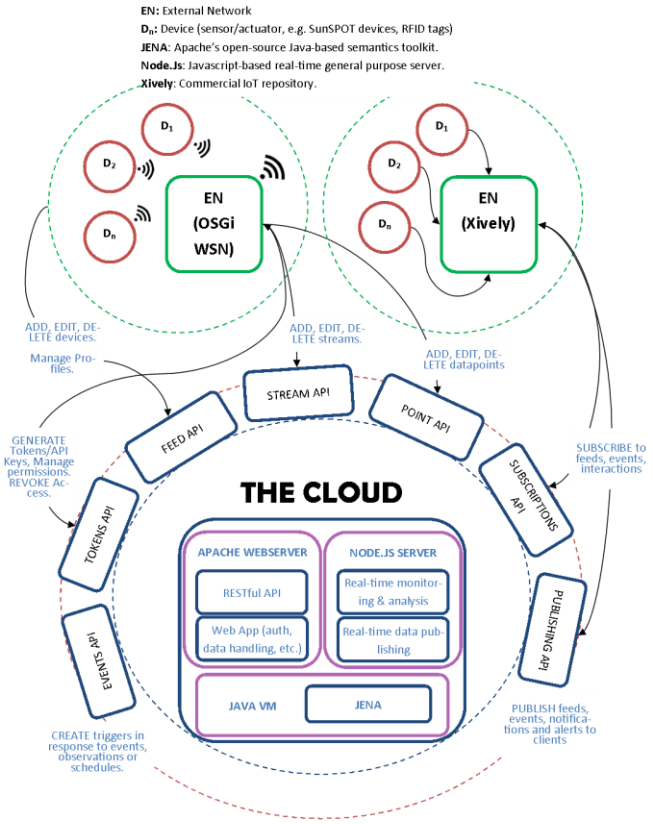

Figure 2: SAW Concept Architecture

In regards to modelling the actual network assets, the proposed SAW framework recognises the following three layers of data in terms of its granularity and expressiveness (Figure 3):

1. Data: When used in the context of assets, "data" in SAW refers to the raw, fundamental bits of information that does not convey any meaning without a given context. For example, "-2", "delivery arrived". This is raw data that needs to be contextualised to hold a particular meaning. Data, by itself, can only be used and understood by the system where it originates from.
2. Information: When raw data is contextualised, information is produced. For example, adding the context "temperature" to "-2" gives us a "temperature value of -2". Further contexts, for example, "°C", can be added to refine the meaning further. Contextualisation is the process of adding semantic metadata conforming to a common ontology understood by all participating networks. Unlike data, information can be used by other networks providing they understand the contexts.
3. Knowledge: Knowledge is a high-level representation of a set or sets of information and involves the use of semantic concepts such as inferencing. For example, "very cold in flooded areas of Sunbury", derived from the information "-2 degrees Celsius" , "location is Sunbury" and "water level: overflowing". As humans, we are mostly interested in knowledge. For example, we want to find out "parking space available in xyz?" as opposed to "no. of proximity sensors in xyz that have a reading below …".

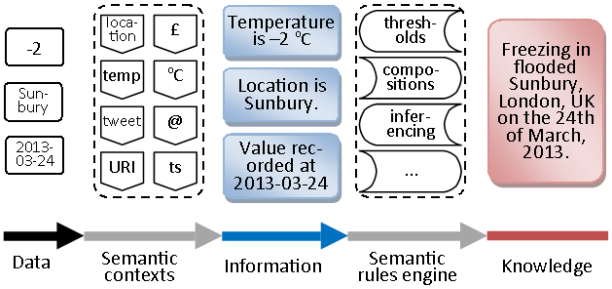

Figure 3: Data expressiveness in SAW

The structure depicted in Figure 3 makes it possible to break down high-level knowledge into the underlying information and even down to the very fundamental raw pieces of data which is useful for introspection of assets.

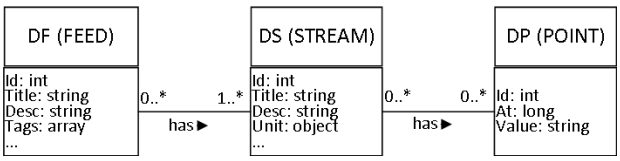

Figure 4: Data hierarchy

The proposed SAW framework has a simple but extensible data hierarchy as illustrated in (Figure 4). A *datafeed* (DF or *feed*) implements a generic device template which can be used to model and represent any kind of physical or virtual device. For example, an Arduino board or a twitter user respectively. A *feed* has 1 or more *datastreams* (DS or *stream*) that describe a particular sensor or actuator asset of the *feed*. For example, a light sensor on an Arduino board or a twitter user's tweet stream. Finally a *stream* can have 0 or more *datapoints* (DP or *point*), where each *point* references a particular value at a given instance in time, E.g., a time-stamped light sensor value or a particular tweet from the stream of a twitter user. The generic templates for data *feeds*, *streams* and *points* are:

1. Extensible so that more fields can be added as and when needed,

ISSN:2319-7900

2. Semantically annotated so all the participating networks have a common understanding regarding the meaning of a particular field, and
3. Transport independent so that they can be represented in any data transport technology (XML, JSON, etc.).

As mentioned earlier, the *points* by themselves convey no meaning to other networks and systems, but when modelled through the semantics contained in the *stream* and *device* definitions, a set of information is formed which can be understood and acted upon by participating networks, thus creating the foundations for a generic and extensible collaboration model.

Token-Based Access Control (TBAC)

In related literature the use of RBAC is very common. RBAC relies on the hypothesis that roles largely remain constant within an organisation so role-based access offers a convenient and maintainable solution. However, RBAC is unsuitable for modelling access control where roles are hard to define and/or unsuitable to use. For example, RBAC would not be suitable in a typical WoT scenario where hundreds of devices are being connected daily such that multitudes of streams are being added to the network and thousands of datapoints are being published. Defining the roles of each user for each device for each stream in this case becomes a huge problematic issue making this mechanism not scalable. It is both illogical and unfeasible to define roles in this setting, especially when the ability to control access right down to individual streams of data is needed. Instead, this paper proposes that a token-based system is more suited for such a scenario. In this proposed mechanism, a set of tokens are generated automatically for each feed to represent a common set of read/write permissions and further tokens can be generated by users for refining access to feeds and streams.

Tokens in the proposed mechanism effectively enable the modelling of multi-faceted (controlling of multiple actions) and cascading (applying to different levels and abstractions of sensing devices) sets of permissions for accessing resources on the network. In SAW's implementation of TBAC, the 1st step is to define two top-level visibility controls for resources:

1. Public access: These resources can be searched and viewed by everyone.
2. Private access: These resources can only be accessed if a token with the necessary permissions is used. Child resources of a private visibility resource are always private.

The next step is to categorise actions as either of the following:

1. Read actions: Identified by the GET HTTP verb, these actions view resource information.
2. Modify/write actions: Any action that uses the remaining HTTP verbs (PUT, POST, DELETE) has the potential to modify resources on the network. Regardless of the visibility of a resource, a token with the necessary permissions is required to carry out these actions.

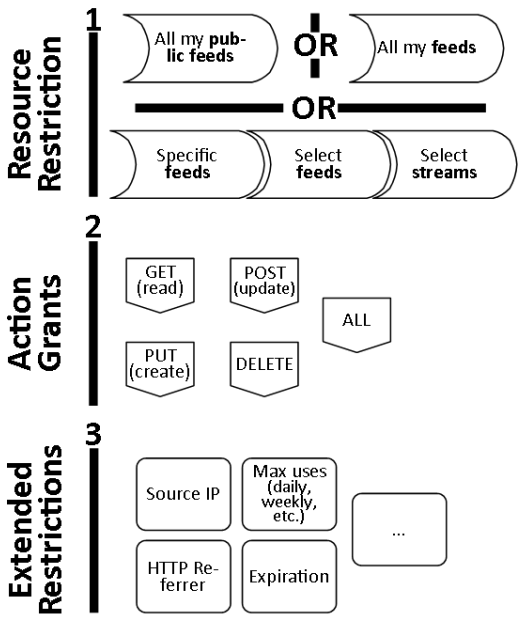

Figure 4: TBAC model showing token construction process

The general process for creating tokens is shown in(Figure 5). In the beginning there is the option of restricting the token scope to particular feeds for a given user (and subsequently, selected streams). In the next step, actions that are permitted on the selected resources can be chosen and finally, due to the extensible nature of SAW's architecture, additional restrictions can be defined to further refine the scope of the token. Furthermore, each token can have multiple sets of permissions in a cascading fashion to enable more fine-grained access control. Finally, the tokens can be used to audit resource access as each request is logged. This TBAC model presents a comprehensive and extensible access control mechanism for the network's resource-based asset model and allows users to easily provision and audit access to private resources.

ISSN:2319-7900

Exposition through RESTful API

The resource-based asset model in SAW is implemented by a service-oriented programming architecture and thus easily exposed through a RESTful API. Basic CRUD (Create, Read, Update, Delete) operations on resources are enabled through the use of the corresponding HTTP verbs: PUT for creating, GET for reading, POST for updating, and DELETE for deleting resources. All *write* actions will require the client to specify a token with the appropriate permissions in the request (either as an HTTP header key like: *X-APIKey: API_KEY*, as a query string in the URL like: http://api.saw.com/feeds?key=API_KEY, or as a request parameter). Additional configuration parameters can be specified through HTTP headers.

Resources can be created by submitting a PUT request to one of the resource endpoints as follows:

```
PUT http://saw.local/api/v1/[ feeds | streams | points ]
```

This will create a new resource according to the payload of the request body. The payload can be presented in XML or JSON. When creating a stream or point for a feed, the feed and/or stream IDs will need to be provided in the payload. Since the API is resource-based, the endpoints for interacting with streams and points of feeds are inclusive of the feed ID. An example is shown below:

```
POST http://api.saw.com/feeds/123/streams/lightSensor
```

This will update a stream with the ID "lightSensor", which belongs to a feed with the ID "123", according to the payload specified in the request body. Below is an example of a JSON "key:value" pair can that can be specified in the request body to update the stream's title:

```
{
        "Title": "New Device Title"
}
```

Application in DM

A case scenario is presented in this section to demonstrate how the proposed asset model can relate to real-life DM applications. A feed labelled "Sunbury" (a town in Surrey, UK) is taken as an example to explain the aforementioned principles. This feed is taken in the context of a flood that might occur as the water level in the neighbouring river Thames raises. This feed will have many streams as it will be measuring the water level (amongst other things) around areas with potential risk of flooding. For this example, two streams are considered and both are radar-based water level monitoring sensors: R1 and R2.

Scenario 1: The feed is set as *private* which necessitates that both the streams are also set as *private*. In this case, a set of tokens will be required to read and modify the feed and the streams. These tokens can be supplied to anyone who needs to monitor or take action to events in response to the readings (by setting up custom alerts). Tokens with extended *write* permissions can be supplied to other parties by the collaboration platform operators if there is a need to distribute administration capabilities. This demonstrates two things:

- Access to private assets can be granted to others without forfeiting authority which solves the *trust* issue in cross-vendor collaboration thereby making it more feasible. The issue of trust is solved because organisations have precise control over the resources they wish to share and with whom they want to share. The issued grants can be revoked at any time.
- Assets can be reused and output increased via intuitive distribution of responsibilities which improves effectiveness of the overall operation.

Scenario 2: The feed and the R1 stream are set as *public* and the R2 stream as *private*. Everyone will be able to view the R1 stream and setup custom events and alerts in response to the published data as it arrives or meets a certain condition. However, tokens will be required to modify the R1 stream and to read or modify the R2 stream. At any given moment in time, permissions to any of the streams can be revoked by either changing the visibility of the streams or by revoking or changing the permission sets on the distributed tokens. Again this shows how SAW is able to provision fine-grained access control for sensitive network assets whilst making it easy to share and act upon streams of data that might be needed by other actors partaking in the operation.

Conclusions

Looking at the current state of the web and the growing need for open distributed systems, this paper proposes that a semantics-driven, service-oriented and resource-based data model would be ideal for creating a decoupled and extensible framework that can be customised for a variety of applications ranging from DM and relief work to monitoring and interacting with next-generation WoT applications (e.g. smart cities). The proposed SAW framework acts as an enabler of the above vision and a concept architecture and asset model describing how such a system may be designed and implemented is presented.

ISSN:2319-7900

The semantics-based modelling of assets and the distributed SoA-based design of the system enables SAW to easily communicate with and collaborate amongst not only other instances of itself, but also other commercial and public IoT solutions like Xively and Thingspeak with the help of adapters. By extensively focusing on the problem of collaboration and tasking itself with the design and creation of a decentralised, RESTful and semantics-enabled system, SAW has the potential to offer and enable effective collaboration amongst WoT applications, especially since it is generic in nature and extensible in design. The architecture and model pertaining to the semantic annotation and querying of assets as well as the eventing and data publishing mechanisms of the framework will be presented in a future publication.

References

[1] S. Vieweg, A. L. Hughes, K. Starbird and L. Palen, "Microblogging during two natural hazards events: What twitter may contribute to situational awareness," in SIGCHI Conference on Human Factors in Computing Systems, New York, 2010.

[2] A. F. Vilas, R. P. D. Redondo, J. J. P. Arias, M. R. Cabrer, A. G. Solla and J. G. Duque, An AmI-Enabled OSGi Platform Based on Socio-Semantic Technologies, M. A. Al-Qutayri, Ed., InTech, 2010.

[3] M. Dorasamy, M. Raman and M. Kaliannan, "Knowledge management systems in support of disasters management: A two decade review," Technological Forecasting & Social Change, 2013.

[4] M. Jennex, "Emergency response systems: lessons from utilities and Y2K," in Tenth Americas Conference on Information, New York, 2004.

[5] S. Jennings, "Time's Bitter Flood - Trends in the number of reported natural disasters," OXFAM, 2011.

[6] P. Peduzzi, "Is climate change increasing the frequency of hazardous events?," in Environment & Poverty Times, Kobe, 2005.

[7] H. R. Rao, V. S. Jacob and F. Lin, "Hemispheric Specialization, Cognitive Differences, and Their Implications for the Design of Decision Support Systems," MIS Quarterly, vol. 16, no. 2, pp. 145-151 , 1992.

[8] S. Celik and S. Corbacioglu, "Role of information in collective action in dynamic disaster environments," Disasters, vol. 34, no. 1, p. 137–154, 2010.

[9] B. Balcik, B. M. Beamon, C. C. Krejci, K. M. Muramatsu and M. Ramirez, "Coordination in humanitarian relief chains: Practices, challenges and opportunities," International Journal of Production Economics, vol. 126, no. 1, pp. 22-34, 2010.

[10] J. Max Stephenson, "Making humanitarian relief networks more effective: operational coordination, trust and sense making," Disasters, vol. 29, no. 4, pp. 337-350, 2005.

[11] M. S. Jr. and M. H. Schnitzer, "Inter-Organizational Trust, Boundary Spanning and Humanitarian Relief Coordination," Nonprofit Management and Leadership, vol. 17, no. 2, pp. 211-232, 2006.

[12] T. Murphy and M. E. Jennex, "Knowledge Management, Emergency Response, and Hurricane Katrina," International Journal of Intelligent Control and Systems, vol. 11, no. 4, pp. 199-208, 2006.

[13] N. Bharosa and M. Janssen, "Extracting principles for information management adaptability during crisis response: A dynamic capability view," in Proceedings of the 43rd Hawaii International Conference on System Sciences, Hawaii, USA, 2010.

[14] I. Aedo, P. Díaz and D. Sanz, "An RBAC model-based approach to specify the access policies of Web-based emergency information systems," International Journal of Intelligent Control and Systems, vol. 11, no. 4, pp. 272-283 , 2006.

[15] N. Chen and A. Dahanayake, "Role-based Situation-aware Information Seeking and Retrieval for Crisis Response," Internation Journal of Intelligent Control and Systems, vol. 12, no. 2, pp. 186-197, 2007.

[16] M. Büscher, P. H. Mogensen and M. Kristensen, "When and how (not) to trust it? Supporting virtual emergency teamwork," International Journal of Information Systems for Crisis Response and Management (IJISCRAM), vol. 1, no. 2, pp. 1-15, 2009.

[17] C. Caragea, N. McNeese, A. Jaiswal, G. Traylor, H.-W. Kim, P. Mitra, D. Wu, A. H. Tapia, L. Giles, B. J. Jansen and J. Yen, "Classifying Text Messages for the Haiti Earthquake," in Proceedings of the 8th International ISCRAM Conference, Lisbon, Portugal, 2011.

[18] H. G. Bressler, E. M. Jennex and G. E. Frost, "Exercise 24: Using social media for crisis response," International Journal of Information Systems for Crisis Response and Management (IJISCRAM), vol. 3, no. 4, pp. 36-54, 2011.

[19] M. Turoff, M. Chumer, B. Van De Walle and X. Yao, "The design of a dynamic emergency response management information system (DERMIS)," Journal of

ISSN:2319-7900

Information Technology Theory and Application, vol. 5, no. 4, pp. 1-35, 2004.

Biographies

MR MOHAMMAD AMIR is currently a PhD candidate at the University of Bradford, UK. He received a 1st Class BEng Honours degree in Electronics, Telecommunications & Internet Engineering (ETIE) from the same university. His research interests include web services, semantic web and the web of things. Mr Amir may be reached at ma-mir1@student.bradford.ac.uk.

DR PRASHANT PILLAI is a Senior Lecturer at the School of Engineering, Design and Technology at the University of Bradford. He has over 10 years of research experience in areas of Mobile/wireless networks like 2G/3G, WLAN/WiMax and Bluetooth and Satellite based networks (DVB, BGAN), looking into the wireless and network control, System architecture design, protocol development and design of security architectures. He is a member of IET and IEEE and a fellow of the HEA. Dr Pillai may be reached at p.pillai@bradford.ac.uk.

PROF YIM FUN HU is Professor of Wireless Communications Engineering in the School of Engineering, Design and Technology in the University of Bradford since 2005, where she is the Head of the Future Ubiquitous Networks (FUN) Research Group. Research activities of the FUN Group encompass mobile and wireless networking, Internet of Things and Cloud computing. She was awarded the Yorkshire Forward Chair in Wireless Communications by the regional development agency for her contributions to wireless communications knowledge transfer activities in 2007. Prof Hu may be reached at Y.F.Hu@bradford.ac.uk.